UNIVERSITY OF ALASKA ANCHORAGE

CSCE 470

CAPSTONE PROJECT

Mobile P2P Telehealth

Author:

Bruno Lopes

Supervisor:

Prof. Adriano Cavalcanti, PhD

Anchorage AK, May 2015.

UAA Computer Science &
Engineering Department
UNIVERSITY *of* ALASKA ANCHORAGE

bruno.lopes@alaska.edu

Version 2.9

"Less is more”

Abstract

The target of this project is to provide health providers with a secure tool that enables direct interaction with clients independent of a centralized institutional infrastructure. The proposed prototype implements a peer-to-peer environment where in addition to real time sessions providers are able to remotely access biometric sensorial data extracted from remote patient readings. This interface was designed for real time access to patient readings, allowing patients to exchange real time sensorial data (body temperature, pressure, heart beat, etc) live or offline. The idea is to provide a platform where providers and clients can interact independently from institutions, decreasing the cost associated with commuting and overall hospital (or any institution) bureaucracy. The concept also protects confidentiality with patient sensitive data along with biometrics to prevent any violations or fraud.

The role of Telemedicine continuous to grow as technology evolves, health professionals enjoy the idea of remote contact with patients but lack an ideal intuitive e-health solution implemented with simplicity, usability and legality to be used as an accountable tool. The main issue faced by health professionals is the solution surrounds legality, health insurance organizations claim the possibility of fraud when remote sessions are established between patient and doctor without a 3rd party authority validating the session, similar to showing proof of identification at a hospital front desk. By adopting biometric access control along with other device sensors we can validate who, where, when and how the session was stablished. Insurance corporations currently rely solely in the health institution to provide authentication, only after a client is validated insurance companies will agree to provide financial assistance predetermined on contract. This bureaucratic process model is similar to a capital oriented open market negotiation, far from having clients and providers needs as a main priority. This capital oriented business practice decrease quality on level care and only protects the relationship between the institution and health insurance corporations, shifting the priority from health professional and patient to insurance and hospital. This project focus in reverting focus back to health professional and patient.

Contents

Chapter 1

Introduction

1.1 Scenario

This project aims to bring health providers even closer to their patients by connecting them remotely and independently of hospital or institutional infrastructure. The Telemedicine concept is not new, it is used worldwide with a high success rate. In United States insurance bureaucracy prevents proper practice of concierge medicine due to large infrastructure requirements. European countries adopted this model in the universal health care practice as a way to reduce long term cost along with an increase of preventive care **[1]**, this practice can be observed in places where the Health field is adopted as patient oriented care, opposed to a capital oriented model.

There are different applications that can benefit from remote professional care, for both ongoing type of treatment or basic diagnosis. Alaska's population groups are disperse, distant from large cities, the extreme winter temperatures, high cost of commuting and lack of infrastructure at times force individuals to stay at home and self-medicate when immediate assistance might be required.

With the increasing usage of new technologies modern society has facilitated the access and distribution of information. Today's health industry pushes technology to allow better access control per individual. As society we continue to better utilize authentication methods that are capable of identifying a user and to adequate its experience. As we praise the fundamental principles of public data and sharing content we also understand the important principle of privacy and anonymity. Authentication is a fundamental where information technology is used to provide unique access to content, a more unique experience has the potential to gather relevant data, and consequently maximize system usability **[2]**.

To legally (following required regulations) connect providers and patients biometric access control technologies act as an interdisciplinary solution, integrating physical and logical realms for patient logical authentication. This automated validation can be extended to any kind of direct patient care that could benefit from patient interaction, from Mental Health to Family Medicine. The Telehealth concept is not new but it is still under development in United States, in the map below from the National Conference of State Legislatures we can observe the current state coverage for Telehealth services.

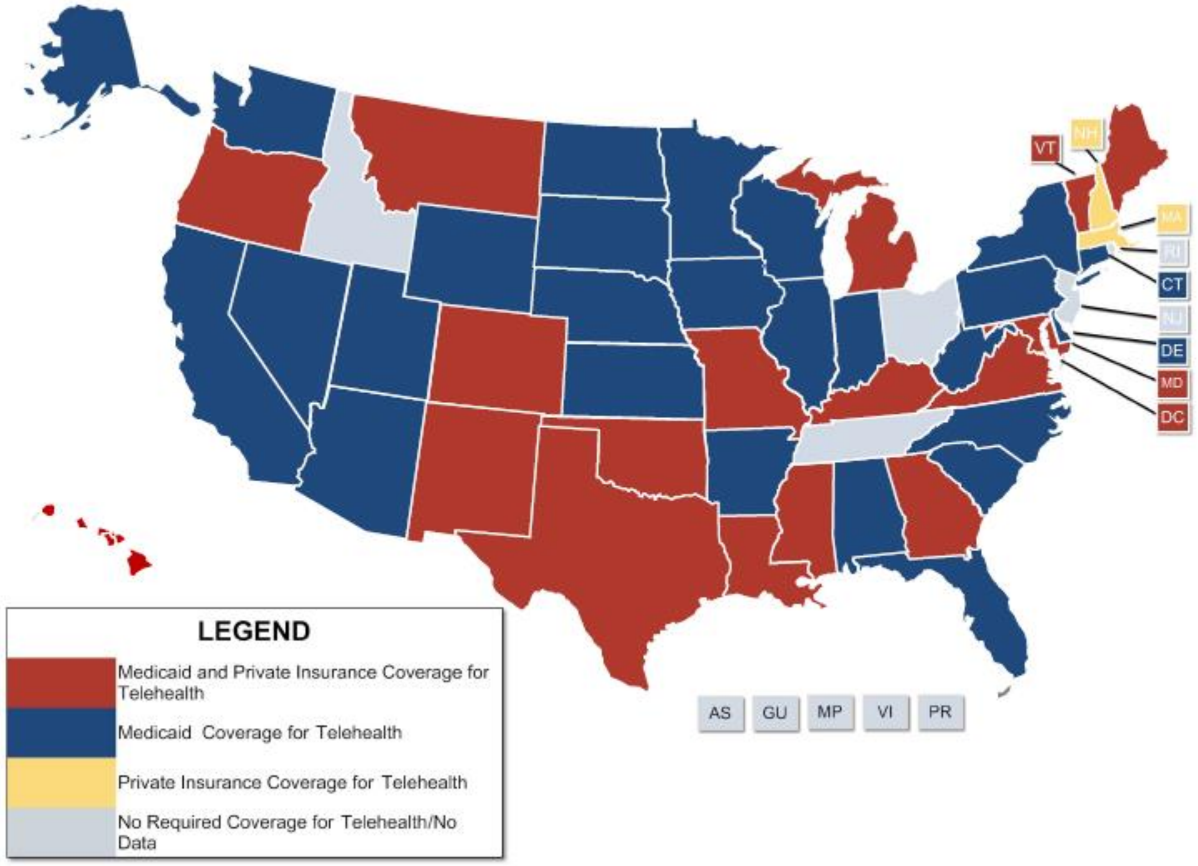

VT
NH
MA
RI
CT
NJ
DE
MD
DC
AS
GU
MP
VI
PR
LEGEND
Medicaid and Private Insurance Coverage for Telehealth
Medicaid Coverage for Telehealth
Private Insurance Coverage for Telehealth
No Required Coverage for Telehealth/No Data

Figure 1.1: States with Coverage for Telehealth Services **[3]**

Biometric sensors combined with other devices to assure simple secure authentication, it ensures patient secure access, provides access control and logs all relevant information from involved participants. When paired with a location sensor (GPS), it is capable to register the physical location of both provider and patient while in session. This combination is beneficial for both insurance companies and health providers. Insurance companies can use the secure data extracted from biometric authentication and location sensors to validate who and where. Health providers can make use of patient’s home environment to account on diagnosis important information such as local temperature, humidity, air pollution, pollen count and etc.

1.2 Application

Project development will focus on implementing the solution presented, as an attempt to join different technologies and disciplines to provide a Telehealth session that includes a remote form of interaction between patient and provider. The proposed solution will cover the fundamentals of Telemedicine along with the required security by using biometric authentication, establishing a secure transmission channel and exchanging data. There are several details that are intentionally not being covered in this project, my purpose is to provide the interaction described above following the guidelines of HIPAA, CFR, CMS and AMA CPT. The topology map below illustrates the strategy adopted for the implementation:

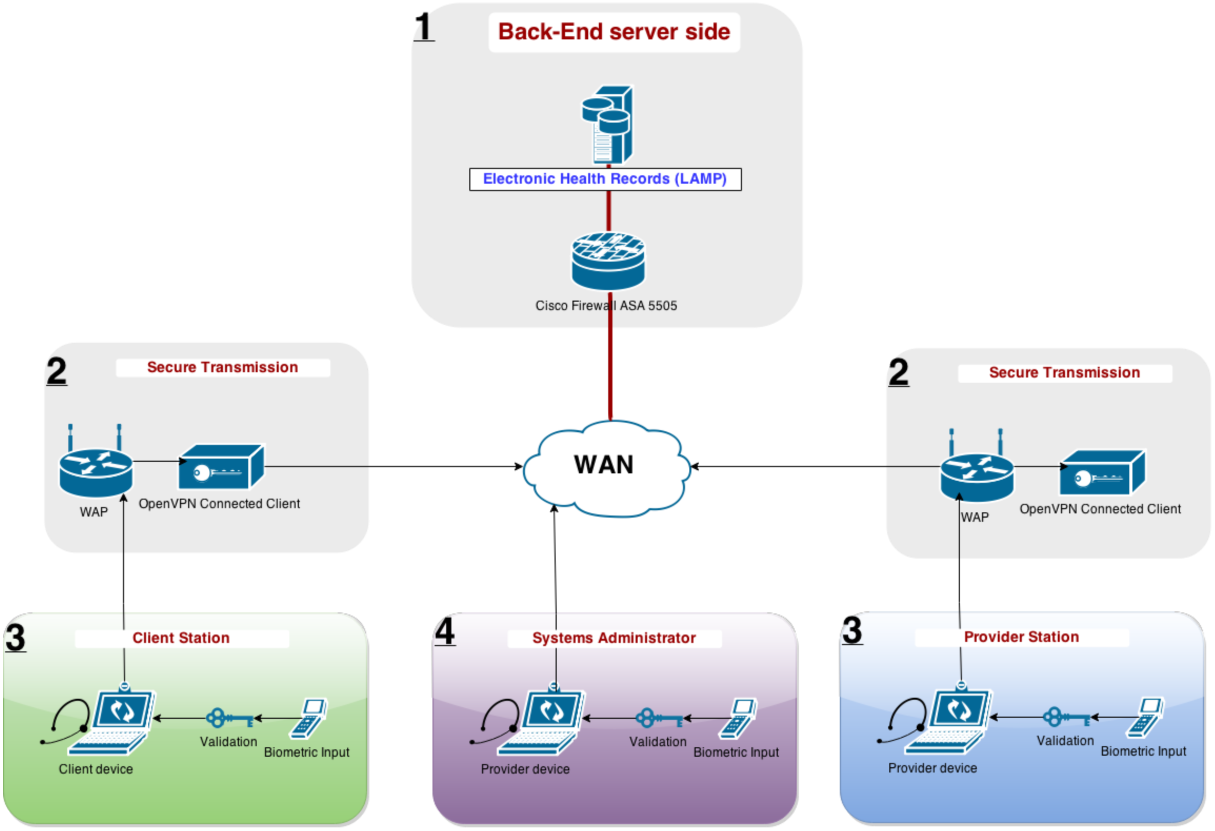


Figure 1.2: Proposed topology diagram

The **Provider Station** hardware constitutes of an Android 4.0 Nexus 7 tablet connected via USB2.0 to a Galileo Gen2 controller that is connected to a biometric fingerprint scanner. The Android device communicates with the Galileo (Arduino based) board using the Amarino toolkit library, the Galileo board receives serial signal from the biometric sensor and outputs the validation and quality of input to the Android application. The **Provider Station** is capable of authenticating or registering a new user, if registering a new user is selected the provider follows the UI to collect demographic information about the patient along with the patient's fingerprints. The Android application receives the validation response from the Galileo controller and if positive toggles the wireless 802.11g interface inside the Android device to the ON position, connecting the **Provider/Client Station** to the **Secure Transmission** section.

The **Client Station** acts similarly to the **Provider Station**, but its back end functionality lacks the ability to register new patients and to read different patient records.

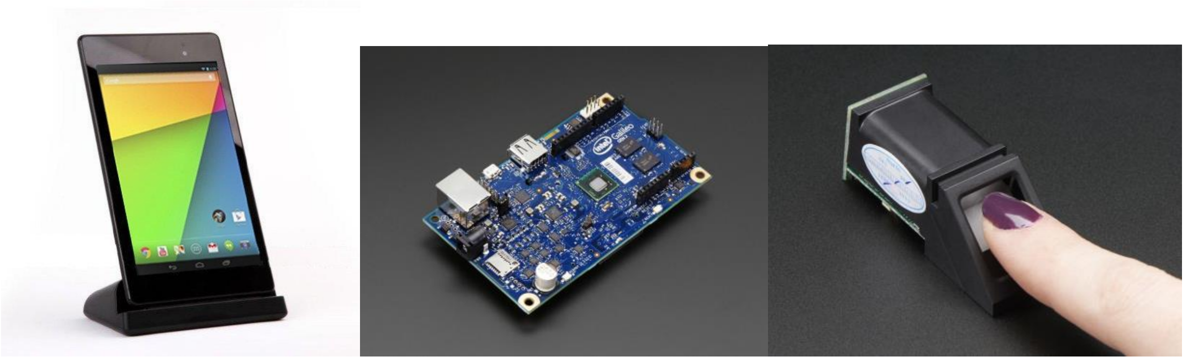


Figure 1.3: Front End devices

The **Secure Transmission** segment takes care of the secure transport of information by encapsulating and encrypting data using SSL/TLS for key exchange. This wireless access point functions as an always VPN connected router, connecting the **Client and Provider Stations** to the **Management and Core Servers.** The system constitutes of a Raspberry Pi running a customized version of Raspbian (modified version of Debian for the Raspberry Pi) configured to have an always connected VPN tunnel to the **Management and Core Servers** router - firewall. This routes are static and this access point only receives incoming requests from pre-configured devices that passed the biometric validation.

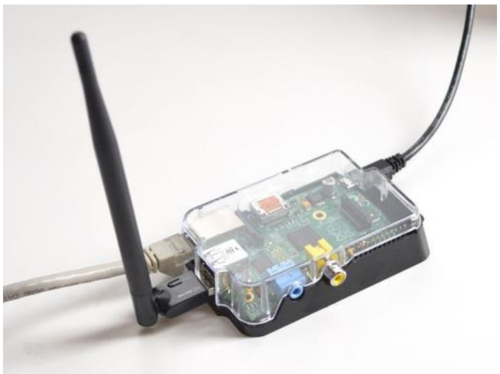


Figure 1.4: Secured Debian Wireless router

The **Management and Core Servers** form the Electronic Health Records system that combine database, access control, packet filtering and central system monitoring. The database constitutes of a LAMP (Linux, Apache, MySQL and PHP) server running on a Raspberry Pi accepting connection from authenticated sessions. The monitoring, access control and packet filtering are managed by the Cisco Adaptive Security Appliance ASA 5505, acting as a gateway firewall accepting incoming connections from authenticated clients.

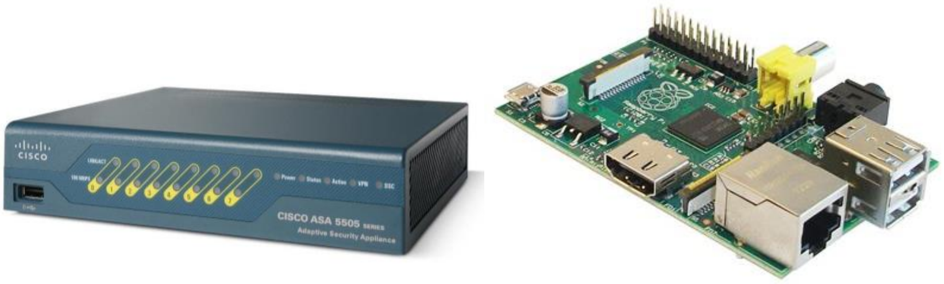


Figure 1.5: Back End components, Gateway firewall and LAMP server

The prototypes are to be built by interconnecting devices directly, the security protocols, encryption, encapsulation and details regarding data transmission on 802.X will be disclose on later stages of development. A breadboard is required to connect the Arduino microcontroller to the biometric fingerprint scanner, the current and voltage discrepancy require the use of resistors for proper wiring.

This implementation integrates different platforms prioritizing security and usability for both patient and provider, the user experience is of importance and led to some of the important system design decisions. The patient segment will write to the database and the provider will be able to read its entries. The back end infrastructure will be managed by a Systems Administrator, which should remain as an invisible actor, able to provide direct support and maintenance to all systems if necessary.

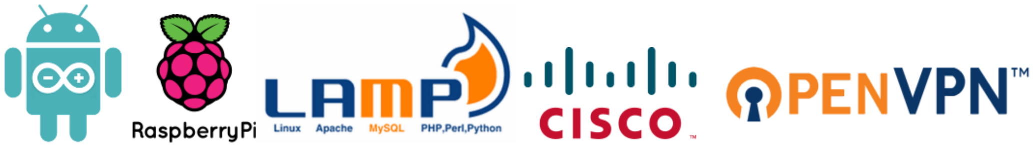


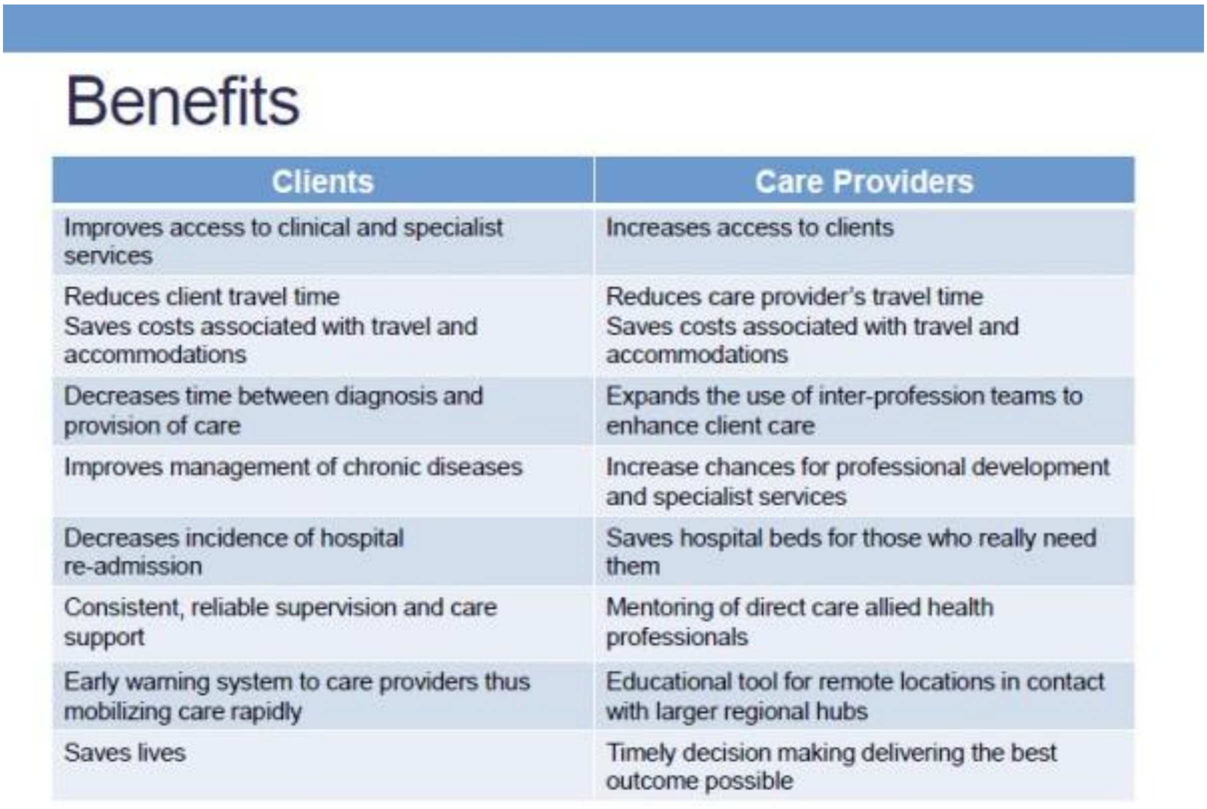
Figure 1.5: Technologies in use

Medical practices might vary depending on state, provider or licensing institution, the purpose of this project is to provide a customizable prototype that could adequate type of practice. This practices are not to be settle by the technology however the technology in place should accommodate any special requests. The system carries a base operational procedure in order to protect its integrity, for example access to the application can only be granted for authenticated users. The system is also protected from malicious attack originated from individuals with direct physical access, complex sequences for passwords, encryption and convergence protect the system from a threat, if any segment is compromised its branch become inoperable and it can only return to production once a redundant backup is restored.

The prototype intended audience could be extended from the clinical family doctor proposed in the solution. The term Telehealth is intentionally used in order to broad usage within the health field. From Mental Health applications to clinical ongoing treatment such as chemotherapy the proposed prototype securely connects two nodes using a secure line and biometric authentication in order to follow mandatory health insurance and practice regulation required to legitimate the session. By stablishing a secure connection between provider and client the 3rd party insurance can validate the session and respond with financial assistance that would benefit both client and provider. In order to attribute value to all involved parties (insurance, professional and client), the proposed solution uses a robust secured system to implement an enterprise level Telemedicine infrastructure but with a fraction of the cost. By utilizing Android tablets as interface and microcontrollers as array of sensor the project simplify institutional complexity and promotes patient-provider interaction.

1.3 Motivation

The motivation for this senior project is a combination of previous experience and multidiscipline and content learned through the Computer Systems Engineering bachelors program. The purpose relates to the health industry in United States, which face several challenges in bringing the infrastructure to a converged stage. In the year of 2009 the recent elected president made a firm commitment to improve institutions infrastructure and handling of private patient data, with the goal of reducing extra costs in health care by eliminating bureaucracy during his mandate. I believe that Telehealth can be an important component to make this a reality, this project aims to benefit patients from rural Alaska **[4]**, patients that have issues with transportation and providers that want to increase patient ongoing care.



Benefits

Clients	Care Providers
Improves access to clinical and specialist services	Increases access to clients
Reduces client travel time Saves costs associated with travel and accommodations	Reduces care provider's travel time Saves costs associated with travel and accommodations
Decreases time between diagnosis and provision of care	Expands the use of inter-profession teams to enhance client care
Improves management of chronic diseases	Increase chances for professional development and specialist services
Decreases incidence of hospital re-admission	Saves hospital beds for those who really need them
Consistent, reliable supervision and care support	Mentoring of direct care allied health professionals
Early warning system to care providers thus mobilizing care rapidly	Educational tool for remote locations in contact with larger regional hubs
Saves lives	Timely decision making delivering the best outcome possible

Table1: Benefits for Clients and Providers

The project purpose is not to exclude the fundamental in person interaction between patient and provider, but to increase preventive and ongoing care connecting both sides more often and more directly. My professional background reflects on a set of skills required to accomplish this project, having worked before as Systems Administrator for a health organization I understand the institutional demands as well the front/back end technologies required to accomplish effective primary care.

Figure 1.7: Remote patient care assistance

The multidisciplinary context in this project is rich and of my interest, all resources are readily available and it involves useful usage of hardware and software combined to solve the issue of legal independent interaction between provider and patient. This motivates me to apply in practice what I have learned during my Computer Systems Engineer bachelor program at University of Alaska Anchorage. The front end will be equipped with mobile platforms and development in Android (Java), along with the Arduino based Intel Galileo controller (C/C++) modulating a serial signal from the fingerprint scanner. The secure socket transmission will involve networking and security protocols, along with access control, packet filtering and other transmission strategies to ensure security and integrity with all patient data. Back End services will be provided thanks to a private MySQL database scheme to store and protect all patient data. This system perform Telemedicine equivalent to a hospital facility infrastructure, but at much lower scale and cost.

I believe that technology will continue to assist human development by empowering individuals, this then self-aware individuals will be capable of building a better world independently from institutions or environment placement. This principle lies behind my senior project and motivation, providing an alternative to a bureaucratic health institutions.

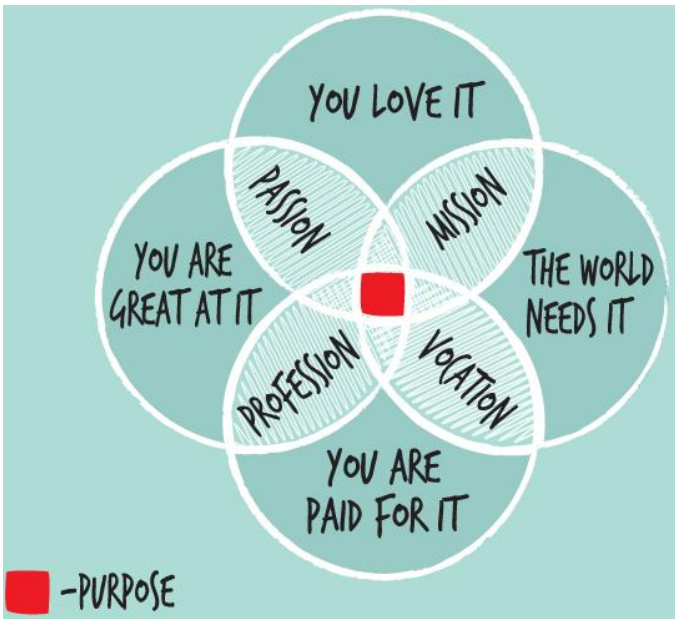


Figure 1.8 motivation ***[7]***

1.4 Recent Developments

Although private sector research and technology advancements drive development in the Telehealth field, government regularization and licensing are the driving factor for al innovation in the field. Public demand and awareness are secondary in relation to practices and norms adopted, providers work close to the private sector to implement functional solutions that are legally covered, recognized by the American Hospital Association and the American Health Care Professionals network. With direct government support, funding is increased as new solutions are more likely to reach general public **[5]**.

Telehealth industry most recent developments shows an increasing concern on integration with Content Management Systems along with systems that provide Medicare and Medicaid reimbursement. New patient demands are followed by concurrent Healthcare reforms and types of treatment, the cost of high speed broadband web access has significantly lowered in the past few years and remote access technology is being explored in places driven by innovation. Advancements on mobile computing along with the evolution of medical devices and adaptive network infrastructure delivery models are pushing the implementation forward and faster. In United States medical practice is also capital oriented, the *consumerization* of patients pushes competition further and consumer’s expectations rely on the usability of integrated product models resulting in the use of Telehealth to provide more patient engagement services to patients. **[6]**

Figure 1.9: Trends on Mobile implementations of Electronic Health Records System and monitoring

Chapter 2

2.1 Methodology

The proposed implementation is based in the Agile **[11]** software development methodology splinted in 3 mutually exclusive segments in order to facilitate final integration:

1. Front End
2. Transport
3. Back End

On each segment iterations will be based on units model following the Gantt Chart proposed, this unit system is important in the Agile methodology and it assists to measure progress over time. Each small increment includes a developing and testing phase prior to delivery, following the Agile methodology tasks were divided in small chunks containing a relative units of effort estimative. One unit consists of a 4-hour journey and it is expected to take an average of a day to be concluded, this estimative can be compared to 1 unit per working day. Most tasks are expected 1 to 2 units to be completed and critical points can be observed on complex tasks that can take 3 or 4 units to finish.

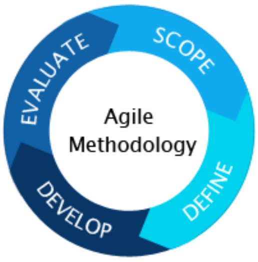


Figure 2.1: Agile Methodology primitives

Following the Agile based project Scope and proposed estimation (total **33 units):**

1. Front End Development: **14 units**
    - **2 units:** Integrate Android device to Arduino platform
    - **2 units:** Design User Interface
    - **2 units:** Design access control via Arduino validation and wireless toggle
    - **4 units:** Transmit data to remote host over the network
    - **4 units:** Remotely read (provider) and write (patient) data to and from MySQL database
2. Transport and Routing: **10 units**
    - **2 units:** Setup and configuration of both (client/provider) Debian platform routers
    - **1 unit:** Research compatible secure protocol between firewall and routers
    - **3 units:** Configuring gateway Cisco ASA firewall
    - **1 unit:** Configuring and testing traffic on public address space
    - **1 unit:** Securing devices and defining access control policies
    - **2 units:** Converging network and integrating devices
3. Back End Development: **9 units**
    - **1 unit:** LAMP server installation and configuration
    - **1 unit:** Securing Linux OS + redundant backup
    - **1 unit:** Securing Apache Server
    - **3 units:** Configuring MySQL database
    - **1 unit:** Establishing remote database access from Android device
    - **2 units:** Configuring Python

2.2 System Integration & Modeling

2.2.1 Front End Development: Android + Arduino

System design and implementation between both platforms, communication strategy between the Android application intent and the fingerprint sensor serial communication.

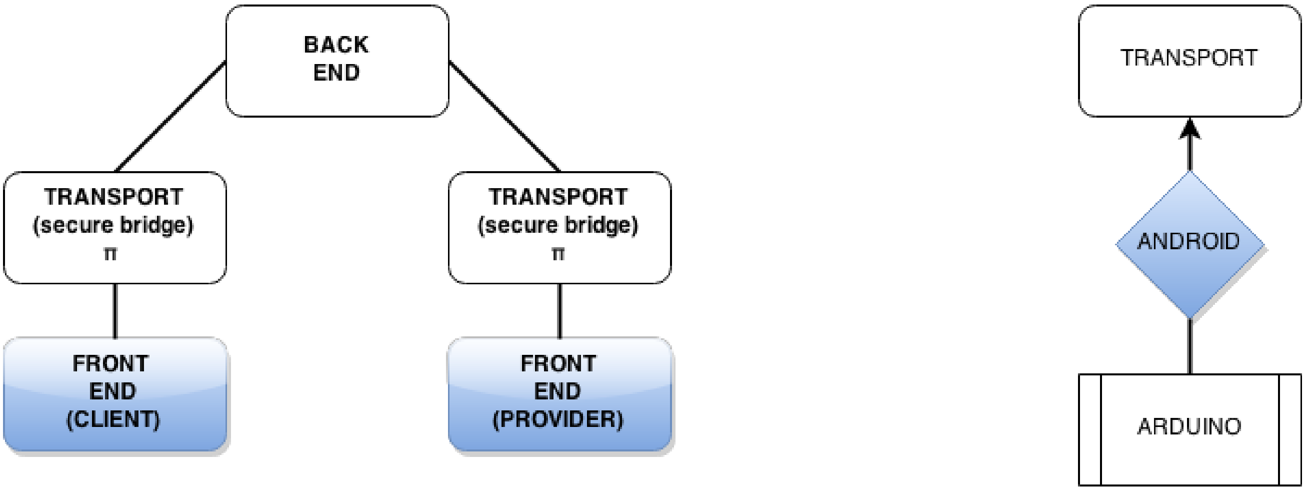


Figure 2.2: Front End physical & logical diagrams

Requirements

Software platform and developer resources

- ❑ Android Studio IDE
- ❑ Eclipse IDE
- ❑ Arduino IDE
- ❑ Amarino library

Hardware Components

- ❑ **[2x]** Nexus 7 Android tablet
- ❑ **[2x]** Intel Galileo Gen2 board
- ❑ **[2x]** Biometric fingerprint sensor
- ❑ **[2x]** RS232 temperature sensors
- ❑ **[1x]** RS232 body sensor

Technology

The fingerprint sensor connected to the Intel (Arduino based) board provides authentication to validate user access. The Android Host USB library connects the Android (Java) and Arduino (C/C++) platforms, the user interface is built on XML (Android) and the remote access to the MySQL database is done using secure sockets for data transmission.

2.2.2 Transport: Secure Transmission

Secure data transmission happens by a combination of hardware (Cisco Firewall) and software (AES encryption via Virtual Private Network) technologies to insure confidential data integrity and security. Local access to secured routers is provided by "up on validation access", controlled access to routers relies on biometric authentication within the Front End Android Application, the system carries a 5 minute timeout policy to enforce access control.

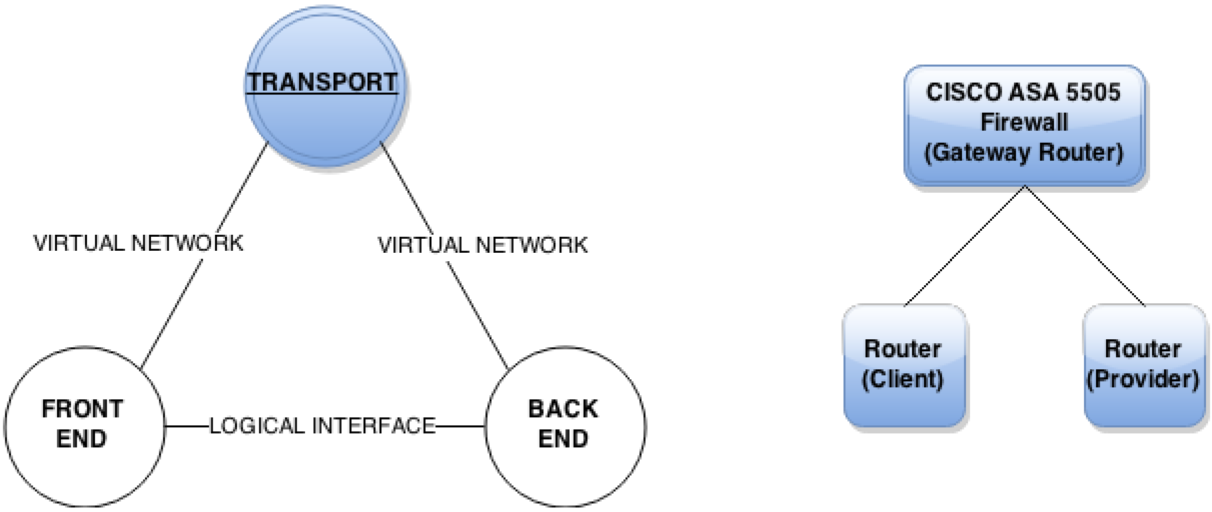


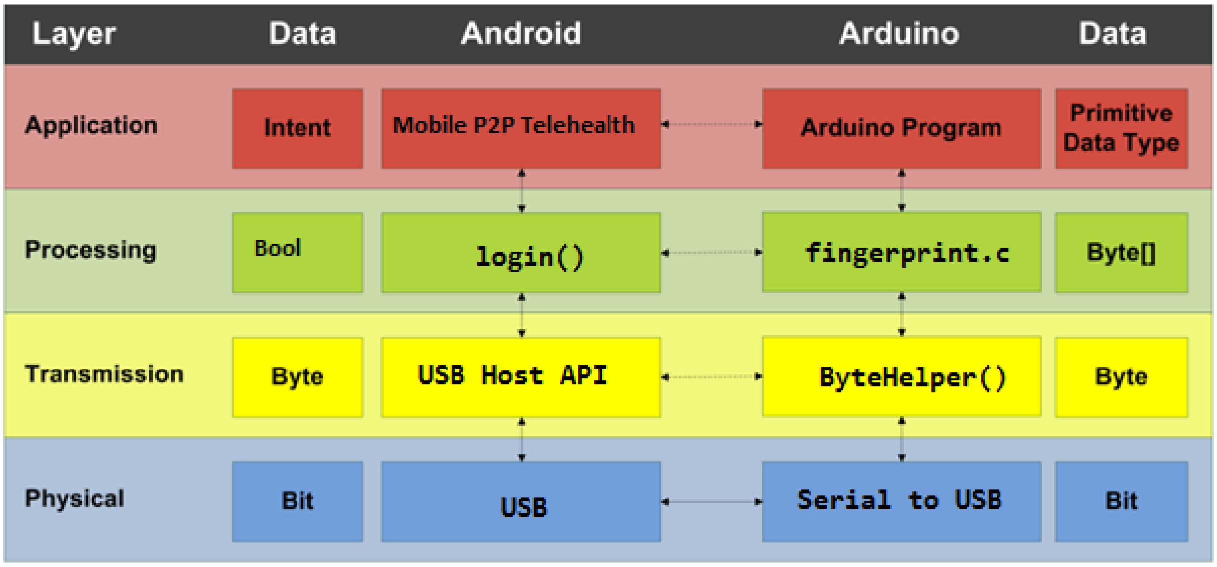
Figure 2.3: Transmission physical & logical diagrams

System

The Cisco ASA 5505 Router Firewall creates the virtual private network that connects to remote routers, using AES or 3DES hardware encryption for Application, Session, Transport, Network and Data Link layers from the OSI Model.

The usage of high security implementation follows the same standards adopted in Health Institutions**[8]**, complying with the American Medical Association, US Department of Health and Human Services Code of Federal Regulations 45/46, HIPAA integrity and confidentiality **[9]** along with the recent Health Information Technology for Economic and Clinical Health provision signed in 2009**[10]**.

The Debian based routers are configured to once turned on automatically create a VPN tunnel directly to the firewall, all configurations are protected and the system is robust. Due to regulations the encryption of all traffic is expected, the external router segments transport from input allowing the front end client and provider to only access this secure connection after a positive biometric validation. This method maximizes security as the router's connection to the back end infrastructure is independently separated from the front end interface.



Layer	Data	Android	Arduino	Data
Application	Intent	Mobile P2P Telehealth	Arduino Program	Primitive Data Type
Processing	Bool	login()	fingerprint.c	Byte[]
Transmission	Byte	USB Host API	ByteHelper()	Byte
Physical	Bit	USB	Serial to USB	Bit

Table 2: System Interface list

Technology

The potential to implement extra security strategy is considerably increase due to the technology inherited on Android. VPN encrypt data transmission and can be combined with the Internet Protocol Security (IPsec), router tables can be maintained by OSPF along MAC address filtering. The proposed implementation include a hardware firewall appliance, this system controls inbound/outbound packet filtering and logging ensures that connections to the Gateway Firewall are secure.

2.2.3 Back End Processing: Linux, Apache, MySQL and Python

The function of the LAMP server is to store, manage and control access to confidential data stored from Front End nodes. It also assists access control by centralizing fingerprints data to be distributed among connected devices, although not completely implemented one of the purposes for the prototype is to mock the fundamental functionality of an Electronic Health Records system.

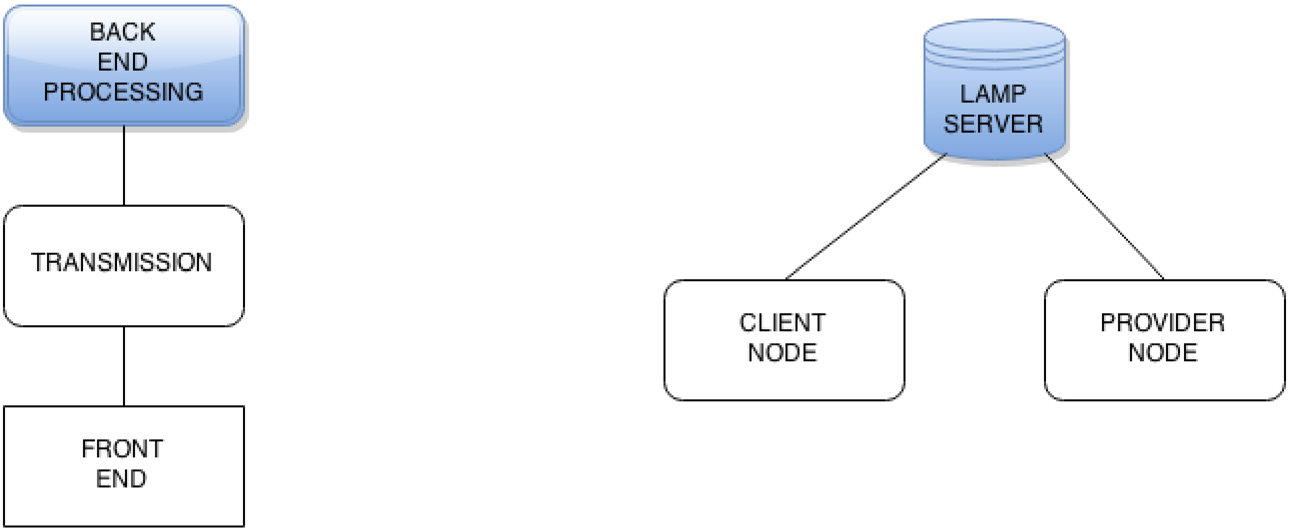


Figure 2.4: Back End physical & logical diagrams

The L.A.M.P. Server

Connected directly to the Gateway Firewall the server includes:

- Linux Debian OS (custom Raspbian distribution for Raspberry Pi)
- Apache Web Server
- MySQL database
- Python

Technology

This system **[12]** is responsible for storing data from client and provider devices, along with logging information about the whole infrastructure including routers and Gateway Firewall. The data received from each client is stored and used to build a patient electronic health record chart, this chart can be accessed by the provider in other to review patient relevant information or to organize current data stored. The relationship to the database can be summarized by clients writing to the database and providers reading from it, this is the fundamental type of interaction that is proposed to be simulated in this prototype, any extra type of access or interaction with the client records can exist in a later stage.

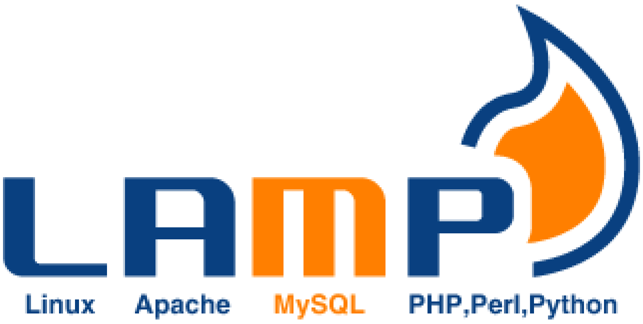
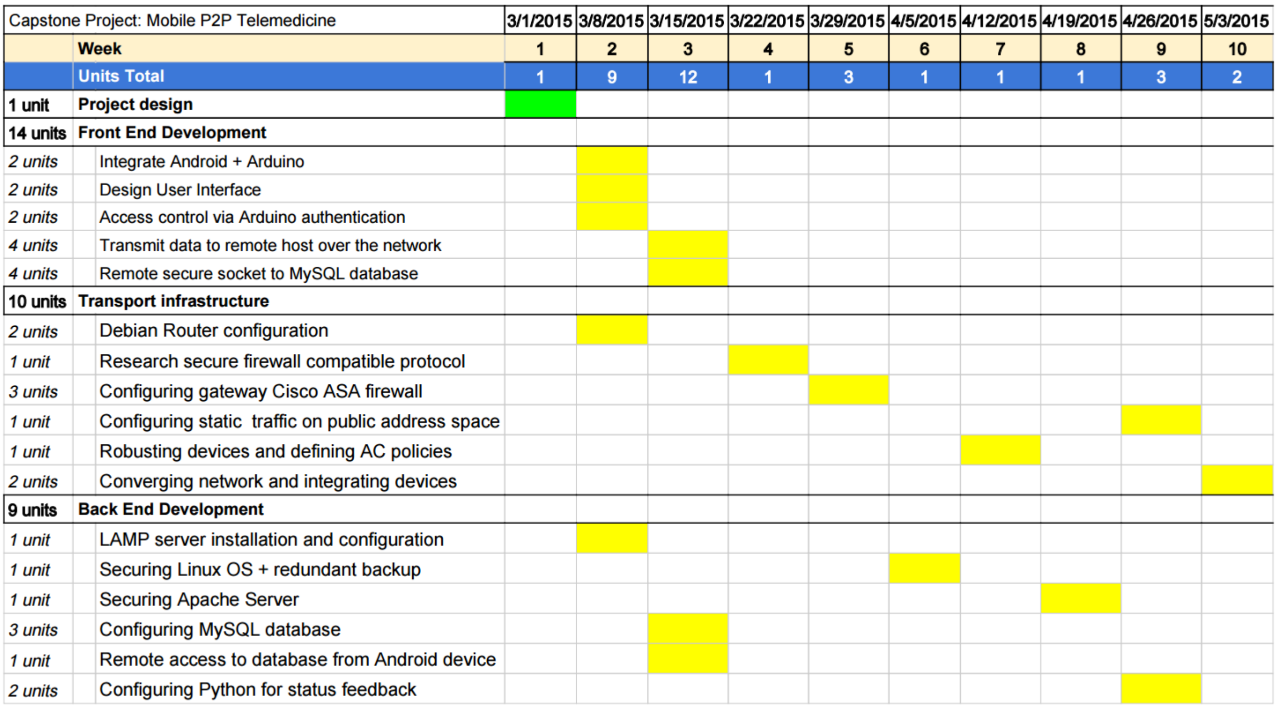


Figure 2.5: LAMP server works as the system Electronic Health Records System

2.3 Gantt Chart

The proposed timeline for this project surround time and availability given within a senior year college semester. I divided tasks based on complexity and length of time estimations, few tasks are dependent from one another and this dependencies are demonstrated on the Gantt chart above. Each unit is an equivalent of a 4 hour journey and it is expected to be completed within a day worth of work, this is a best approach effort and is subject to change depending on task and/or time availability.



Capstone Project: Mobile P2P Telemedicine		3/1/2015	3/8/2015	3/15/2015	3/22/2015	3/29/2015	4/5/2015	4/12/2015	4/19/2015	4/26/2015	5/3/2015
	Week	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
	Units Total	**1**	**9**	**12**	**1**	**3**	**1**	**1**	**1**	**3**	**2**
1 unit	**Project design**	🟩									
14 units	**Front End Development**										
2 units	Integrate Android + Arduino		🟨								
2 units	Design User Interface		🟨								
2 units	Access control via Arduino authentication		🟨								
4 units	Transmit data to remote host over the network			🟨							
4 units	Remote secure socket to MySQL database			🟨							
10 units	**Transport infrastructure**										
2 units	Debian Router configuration		🟨								
1 unit	Research secure firewall compatible protocol				🟨						
3 units	Configuring gateway Cisco ASA firewall					🟨					
1 unit	Configuring static traffic on public address space									🟨	
1 unit	Robusting devices and defining AC policies							🟨			
2 units	Converging network and integrating devices										🟨
9 units	**Back End Development**										
1 unit	LAMP server installation and configuration		🟨								
1 unit	Securing Linux OS + redundant backup						🟨				
1 unit	Securing Apache Server								🟨		
3 units	Configuring MySQL database			🟨							
1 unit	Remote access to database from Android device			🟨							
2 units	Configuring Python for status feedback									🟨	

Figure 2.6: Current Proposed project Gantt Chart

The most complex tasks are around an average of a working week (4 days) and the simpler tasks can be completed within a day. The initial priority is the Android application, routers and server to be setup and configured so the infrastructure can follow. After this initial main section of the project is taken care of, remote functionality and the ability to integrate devices comes next and in the final stages I will be working on testing and to robust the system security with policies for access control, redundant backups and accessibility.

Chapter 3

3.1 Front End Design

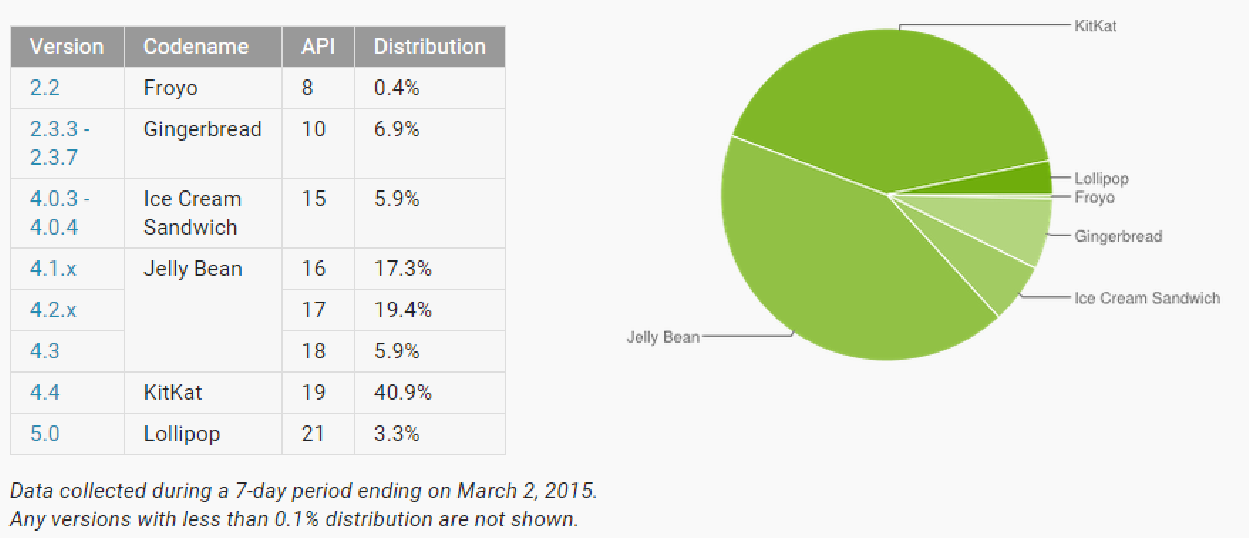
The system constitutes of 3 main segments (Front End, Transport and Back End), Front End is responsible for Graphical User Interface along with unit testing to Transport and Back End. The Application Design main focus is to provide a familiar interface for both Provider and Client, where information from each can be accessed and interacted from the Back End database to the Android environment. The Android Application color scheme, visual design **[15]**, information architecture **[16]** and content strategy **[17]** are based on usability principles commonly adopted in web design **[18]**.

3.1.1 Current Platform Considerations

Among other devices and systems a mobile platform was chosen because of its portability and wide realm of sensors already included on smartphones and tablets (Asus Nexus 7). Android was chosen as an open source platform which facilitates research, strong emphasis on accessibility with freely available development environment and low complexity

	Open Source	Accessibility	Low Complexity
Android	🟩	🟩	🟩
iOS	🟥	🟥	🟥
Windows Mobile	🟥	🟩	🟩

Table 3: Front End Platform comparison



Version	Codename	API	Distribution
2.2	Froyo	8	0.4%
2.3.3 - 2.3.7	Gingerbread	10	6.9%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	5.9%
4.1.x	Jelly Bean	16	17.3%
4.2.x		17	19.4%
4.3		18	5.9%
4.4	KitKat	19	40.9%
5.0	Lollipop	21	3.3%

Data collected during a 7-day period ending on March 2, 2015.
Any versions with less than 0.1% distribution are not shown.

Figure 3.1: Google Android API distribution ***[19]***

3.1.2 System Components

The Android USB Host API introduced on Android 3.1 allows the Android device to behave as an USB host without the need for Android Accessory Development Kit, this hardware support communication allows Android to communicate with accessories directly via USB.

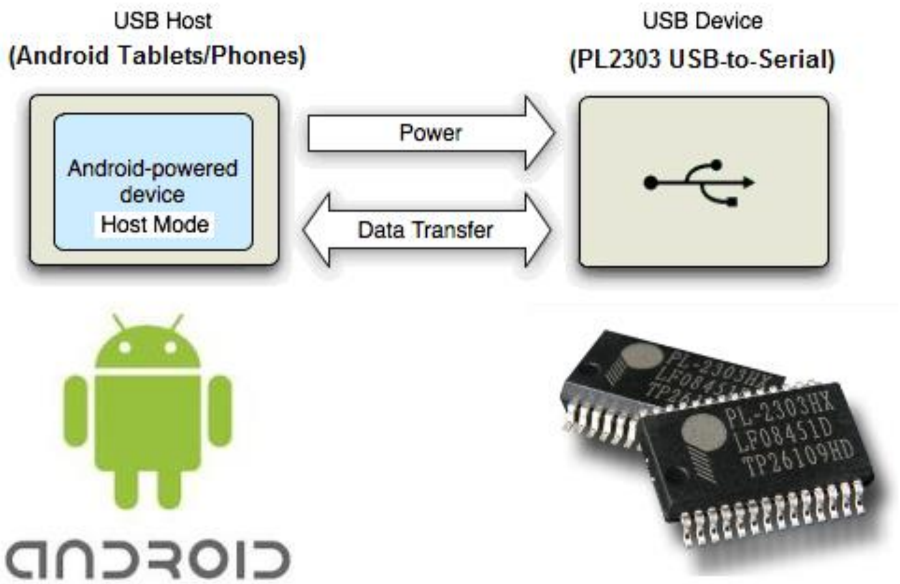


Figure 3.2: Android USB Host API ***[20]***

The simple approach for an effective secured communication between the Android API and the Arduino SPI uses the Android device as an USB Host. The Android USB Host interface powers the bus and enumerate connected USB devices **[21],** allowing the Android device to communicate with the Arduino microcontroller using a serial-to-usb firmware bridge driver on both Android and Arduino devices.

In order to properly secure access to device configuration and to protect the prototype system from alteration, the activity lifecycle strategy adopted includes an “always running” activity running on full screen.

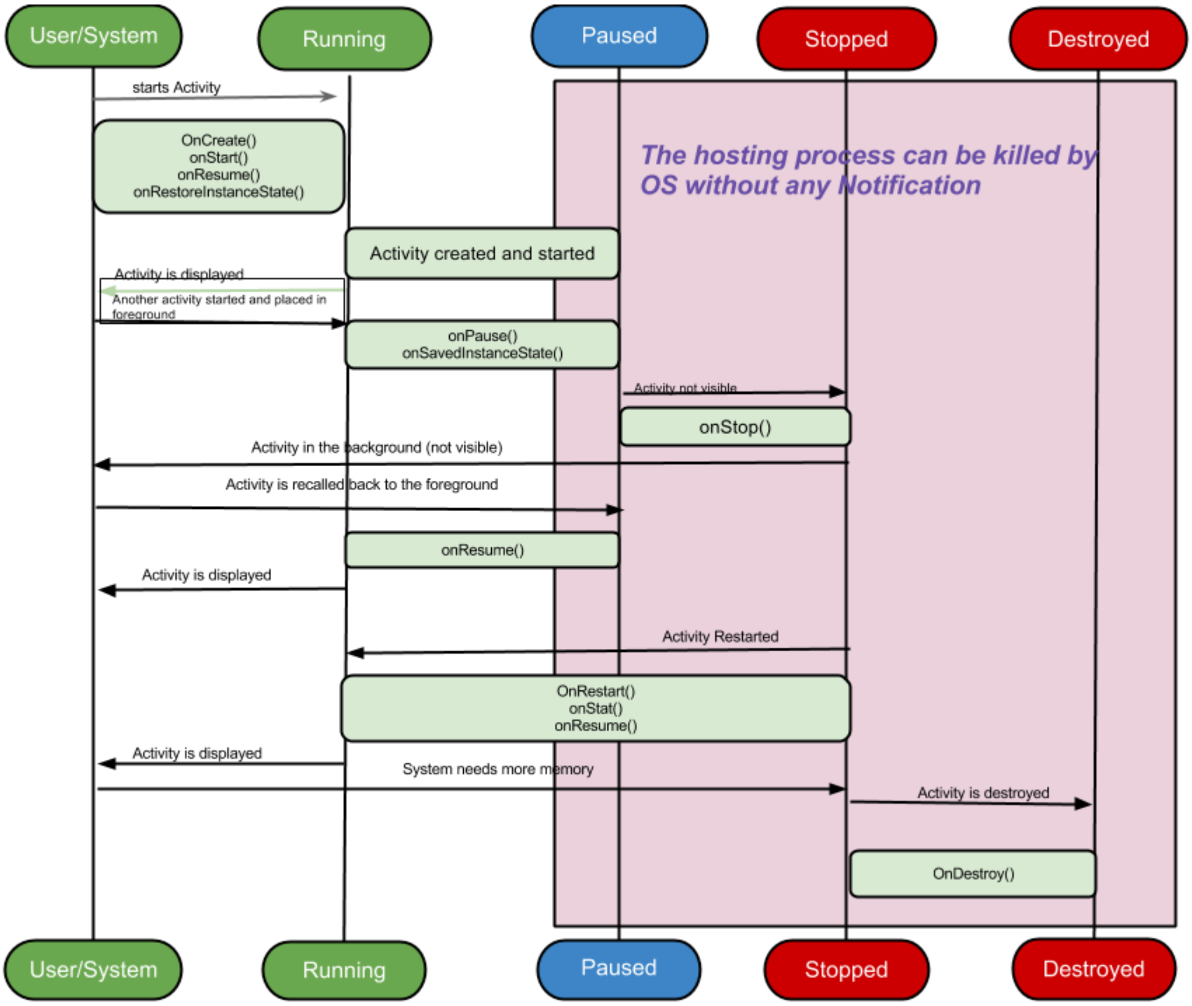


*Figure 3.3: Android activity lifecycle **[21]***

The Arduino microcontroller runs a custom made firmware to validate the user and allow access to the system, the Arduino firmware converts the analog serial signal received from sensors to USB acting as a simple pulse width modulation driver. All data is converted using the AT Mega SOC sending and receiving data across the Arduino USART port.

The Arduino interface choice as the microcontroller allows possible future integration to other open hardware external devices and sensors that utilize the serial bus method of communication. The choice of sensors and devices can be customized based on possible client treatment needs.

The Arduino interface choice as the microcontroller allows possible future integration to other open hardware external devices and sensors that utilize the serial bus method of communication. The choice of sensors and devices can be customized based on possible client treatment needs.

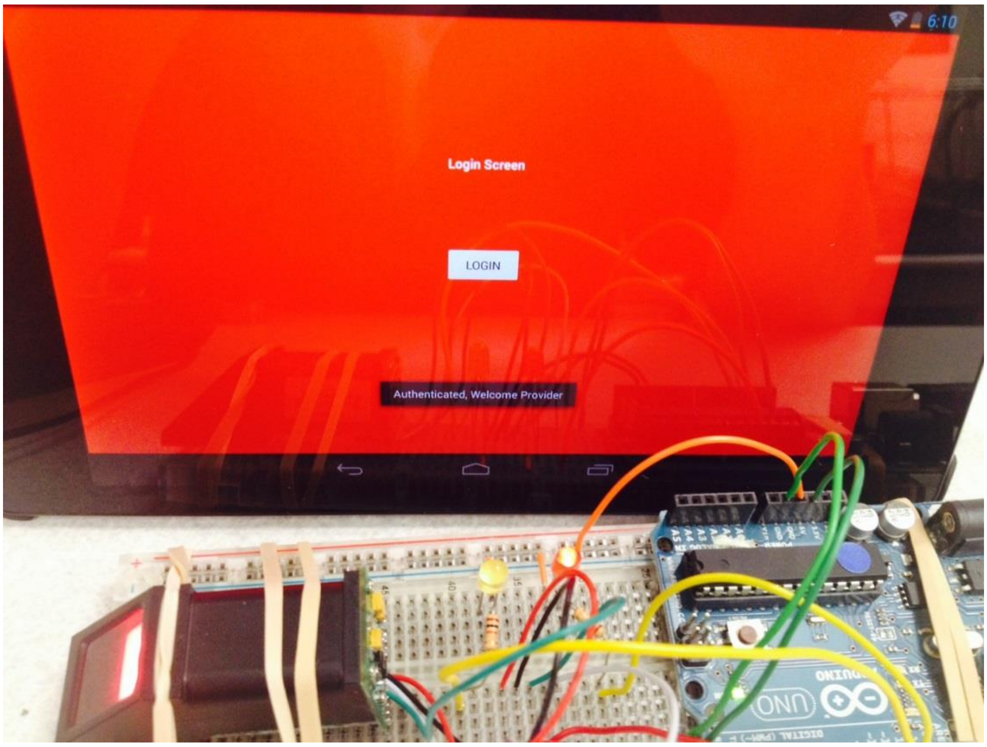


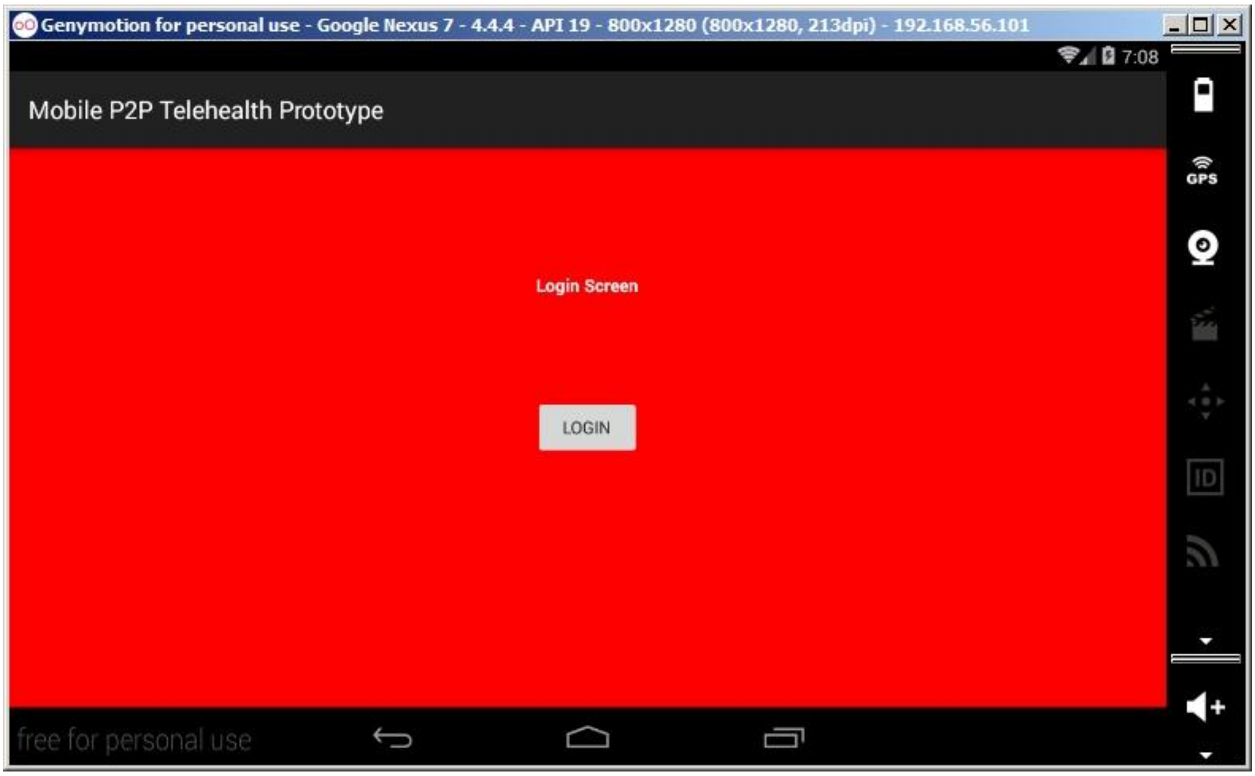
Figure 2: Android to Arduino OTG USB connection ***[22]***

3.1.3 User Interface

The Front End application was intentionally developed to run on full screen at all times, in order to properly secure the system both Providers and Clients must only have access to the application interface. Both Provider and Client can interact with the system using the same interface, the difference is the level of access each account carries from the initial enrollment parameters. Overall the Provider account can "read" contents previously stored on the database while the Client account allows the Client to "write" data from sensors directly to the database.

The exceptions follows prototype implementation, the environment in practice for this project relates the interaction between a doctor and a remote patient, where the doctor eventually will need write permission to add notes to the patient's chart.

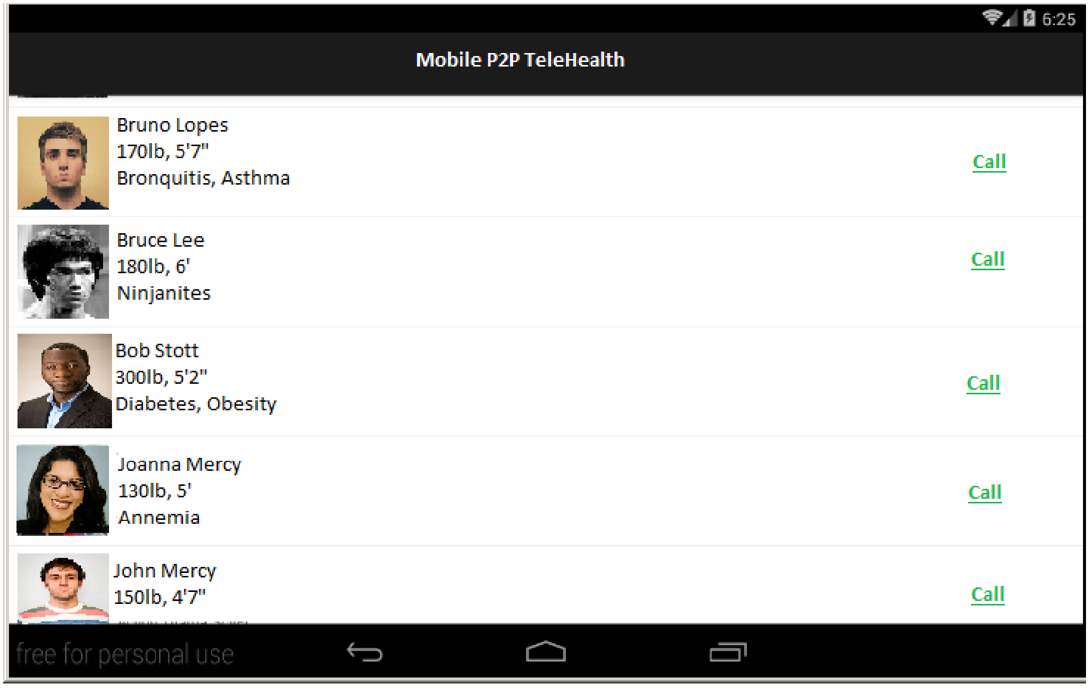
Initial Login Screen



Genymotion for personal use - Google Nexus 7 - 4.4.4 - API 19 - 800x1280 (800x1280, 213dpi) - 192.168.56.101

Figure 3.5: Prototype initial Login screen

Client || Provider List



Bruno Lopes
170lb, 5'7"
Bronquitis, Asthma

Bruce Lee
180lb, 6'
Ninjanites

Bob Stott
300lb, 5'2"
Diabetes, Obesity

Joanna Mercy
130lb, 5'
Annemia

John Mercy
150lb, 4'7"

Figure 3: GUI Prototype of Provider's client list

Calling Screen

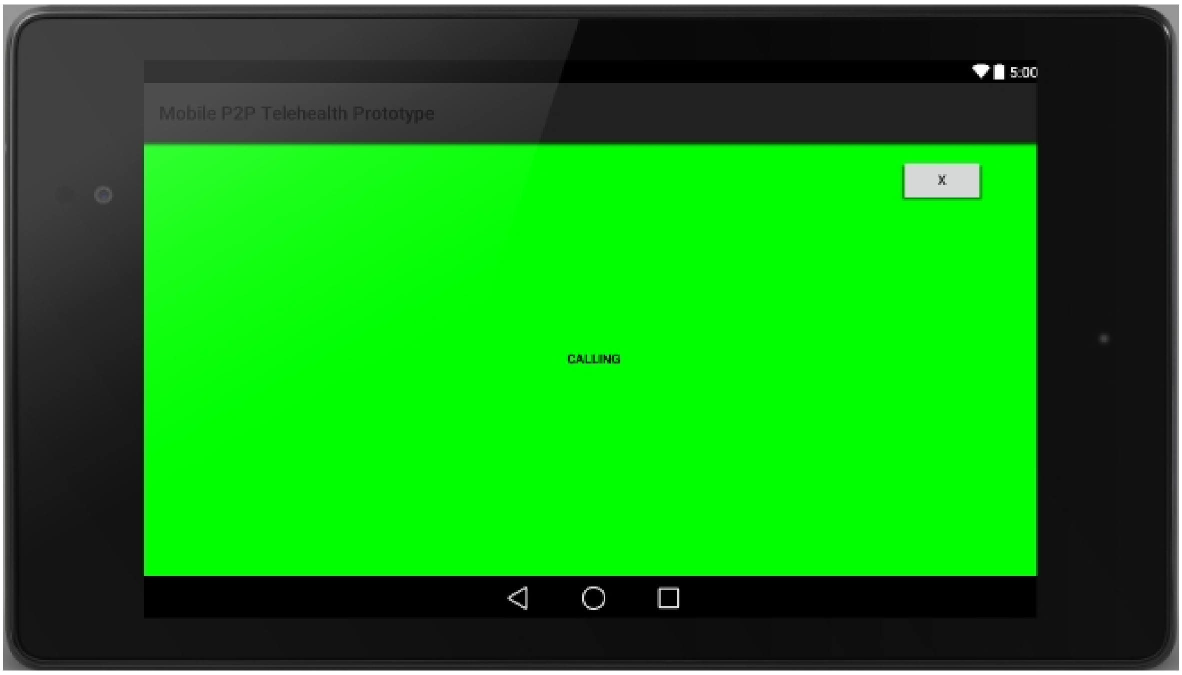


Figure 4:GUI Prototype of calling screen for both Client and Provider

3.2 Testing

Continuous unit testing is planned on any software change or implementation. The Gantt Chart iterations were segmented onto testable sections, due to the complexity of this project testing strategies are different depending on which layer interaction is occurring.

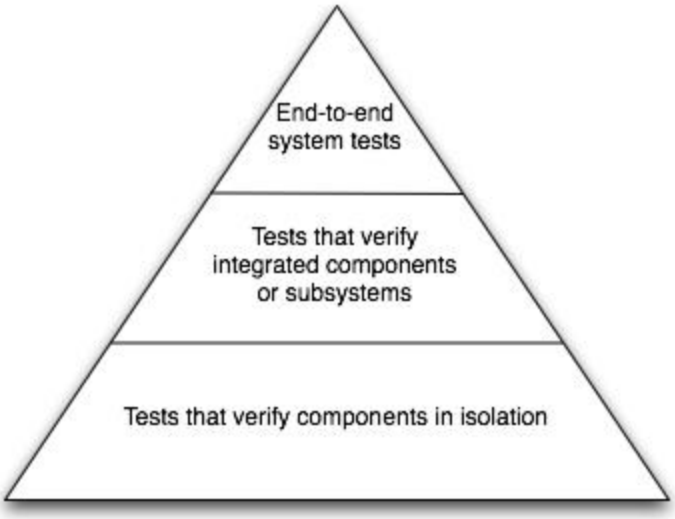

End-to-end system tests
Tests that verify integrated components or subsystems
Tests that verify components in isolation

Figure 5: Overall system testing hierarchy

3.2.1 Unit testing tasks

Front End: General UI, fingerprint validation, network connectivity

Transmission: Connection between nodes, security protocols, benchmark efficiency

Back End: Database access control, read and write access, monitoring tools

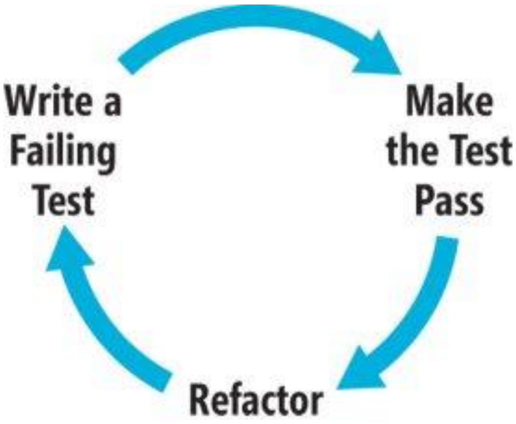


Figure 6: Development testing strategy

Chapter 4

4.1 Results

In order to properly quantify reached results we must satisfy the base principle proposed in this project prototype: “Provide a secure infrastructure to connect remote clients to health providers using a low cost efficient infrastructure”. This secure environment must follow current USA health care informatics regulation and guidelines to be considered applicable for health clinics and health insurance companies. The proposed model brings all the base functionality and expansion capabilities expected on a Telemedicine device, but at a fraction of the cost. The closest industry implementation model to the Mobile P2P Telehealth would be the AFHCAN Cart **[13]**, used by many tribal villages in the interior of Alaska.

Comparing to current health industry implementations, the measured success from the prototype must fulfil the following criteria:

- ✓ Secured biometric access control to Front-End
- ✓ Secured transmission stablished on Debian router
- ✓ Cisco Firewall VPN tunnel stablished between Front-End and Back-End
- ✓ Health records access control policy
- ✓ Secured access to system Electronic Health Records (database)
- ✓ Exchange of data between Client (write) and Provider (read) nodes
- ✓ Secure logoff and timeout policy

4.1.1 Segmented Results

Direct access to application can only be granted via biometric authentication, the fingerprint validation is provided by an Arduino microcontroller connected to the Android tablet via USB. Although this project does not cover patient/provider initial registration nor any clinical procedure, it is important to note that such policies must be adopted outside the developing environment. The following image demonstrates the result of a successful biometric validation, authenticating the user to proceed with the system.

- ✓ Secured biometric access control to Front-End interface:

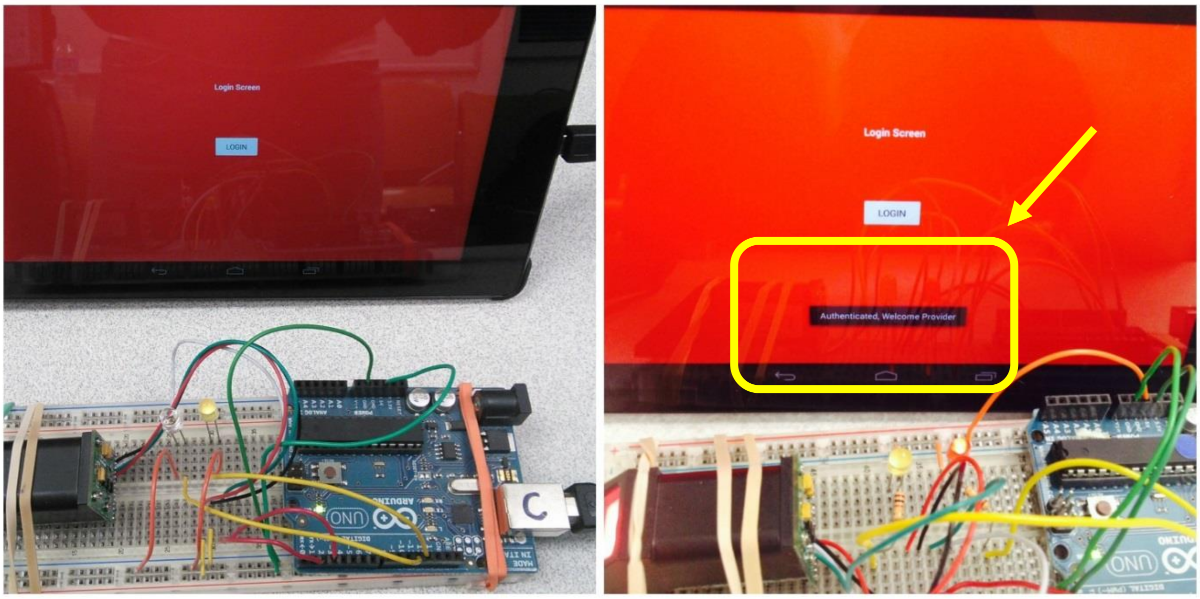
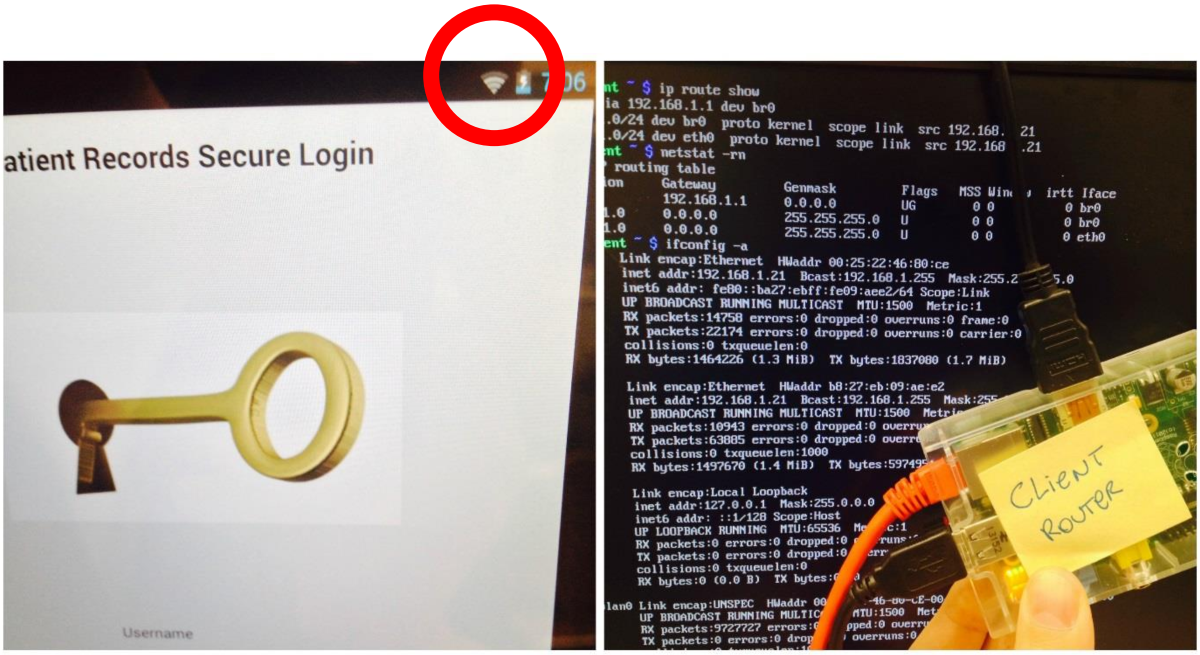


Figure 13: Front-End biometric authentication process

After the Client or Provider successfully authenticate to the Front-End application, the application toggles the wireless to the “ON” position, which is preconfigure to access the device’s unique Access Point.

- ✓ Secured transmission stablished on Debian router:

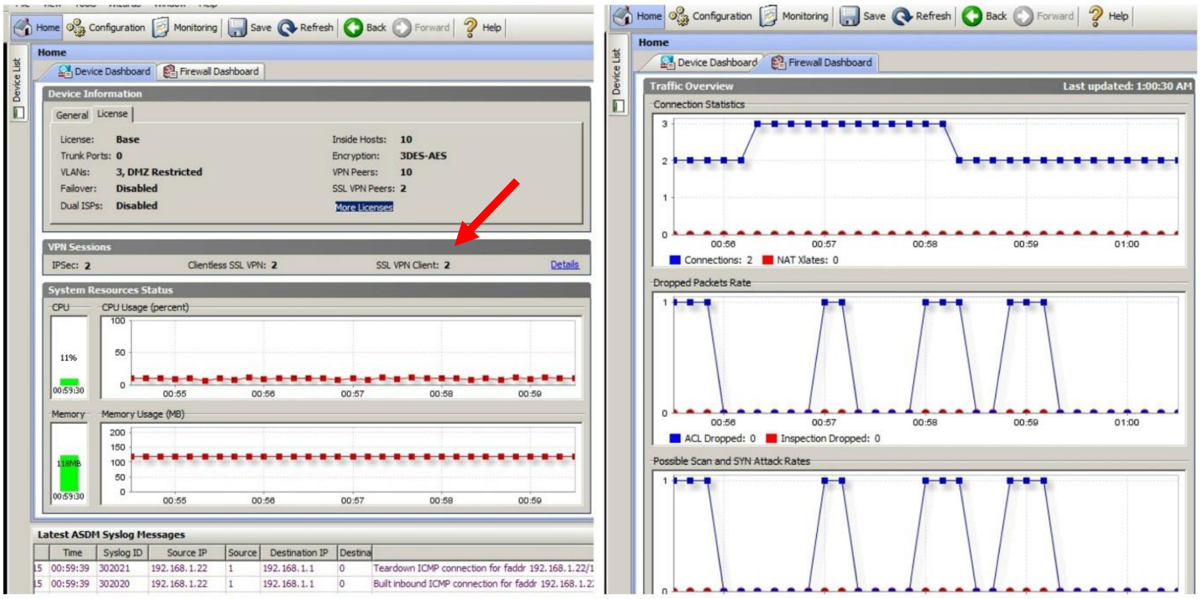


```
nt ~ $ ip route show
ia 192.168.1.1 dev br0
.0/24 dev br0  proto kernel  scope link  src 192.168.  21
.0/24 dev eth0  proto kernel  scope link  src 192.168  .21
nt ~ $ netstat -rn
 routing table
ion      Gateway          Genmask          Flags   MSS Win   irtt Iface
         192.168.1.1      0.0.0.0          UG        0 0          0 br0
1.0      0.0.0.0          255.255.255.0    U         0 0          0 br0
1.0      0.0.0.0          255.255.255.0    U         0 0          0 eth0
ent ~ $ ifconfig -a
  Link encap:Ethernet  HWaddr 00:25:22:46:80:ce
  inet addr:192.168.1.21  Bcast:192.168.1.255  Mask:255.2   5.0
  inet6 addr: fe80::ba27:ebff:fe09:aee2/64 Scope:Link
  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
  RX packets:14758 errors:0 dropped:0 overruns:0 frame:0
  TX packets:22174 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:1464226 (1.3 MiB)  TX bytes:1837080 (1.7 MiB)

  Link encap:Ethernet  HWaddr b8:27:eb:09:ae:e2
  inet addr:192.168.1.21  Bcast:192.168.1.255  Mask:255
  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metri
  RX packets:10943 errors:0 dropped:0 overru
  TX packets:63885 errors:0 dropped:0 overr
  collisions:0 txqueuelen:1000
  RX bytes:1497670 (1.4 MiB)  TX bytes:597495

  Link encap:Local Loopback
  inet addr:127.0.0.1  Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING  MTU:65536  Me   c:1
  RX packets:0 errors:0 dropped:0    runs
  TX packets:0 errors:0 dropped:0    err
  collisions:0 txqueuelen:0
  RX bytes:0 (0.0 B)  TX bytes:

lan0 Link encap:UNSPEC  HWaddr 00     -46-80-CE-00
  UP BROADCAST RUNNING MULTIC     MTU:1500  Met
  RX packets:9727727 errors:   pped:0 overru
  TX packets:0 errors:0 drop    overruns:0
```

Figure 14: Secured connection between Debian WAP router and Front-End application

Once the Front-End application validate the user, the connection to the Debian router grants the secure VPN transmission of sensitive data within the tunnel. Note that all data transport is independent from node environment, as required by HITECH guidelines **[14].**

- ✓ Firewall VPN Session stablished between the Debian routers and Back-End server



License: **Base**
Trunk Ports: **0**
VLANs: **3, DMZ Restricted**
Failover: **Disabled**
Dual ISPs: **Disabled**
Inside Hosts: **10**
Encryption: **3DES-AES**
VPN Peers: **10**
SSL VPN Peers: **2**
More Licenses

IPSec: **2**
Clientless SSL VPN: **2**
SSL VPN Client: **2**
Details

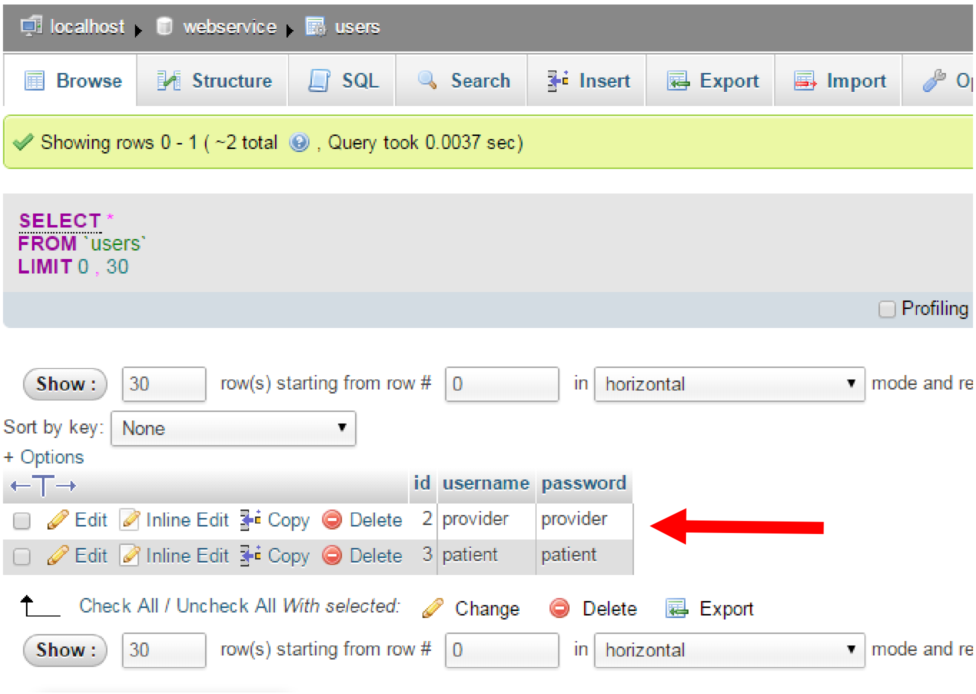
	Time	Syslog ID	Source IP	Source	Destination IP	Destina	
15	00:59:39	302021	192.168.1.22	1	192.168.1.1	0	Teardown ICMP connection for faddr 192.168.1.22/1
15	00:59:39	302020	192.168.1.22	1	192.168.1.1	0	Built inbound ICMP connection for faddr 192.168.1.2

🟦 Connections: 2 🟥 NAT Xlates: 0

Figure 15: Secured connection between Debian WAP router and Front-End application

Access to the database is then granted, both client and provider are able to exchange data. Security measures were adopted to ensure that access to database is restricted and sensitive client data requires appropriate access control. There are 3 different layers of security, including access to the system (biometric authentication), secure data transmission (VPN tunnel 3DES-AES encryption), and secure login to the database (EHR equivalent).

✓ Health records access control policy



✓ Showing rows 0 - 1 (~2 total , Query took 0.0037 sec)

```
SELECT *
FROM `users`
LIMIT 0 , 30
```

Show : 30 row(s) starting from row # 0 in horizontal mode and re

Sort by key: None

+ Options

id	username	password
2	provider	provider
3	patient	patient

Check All / Uncheck All *With selected:* Change Delete Export

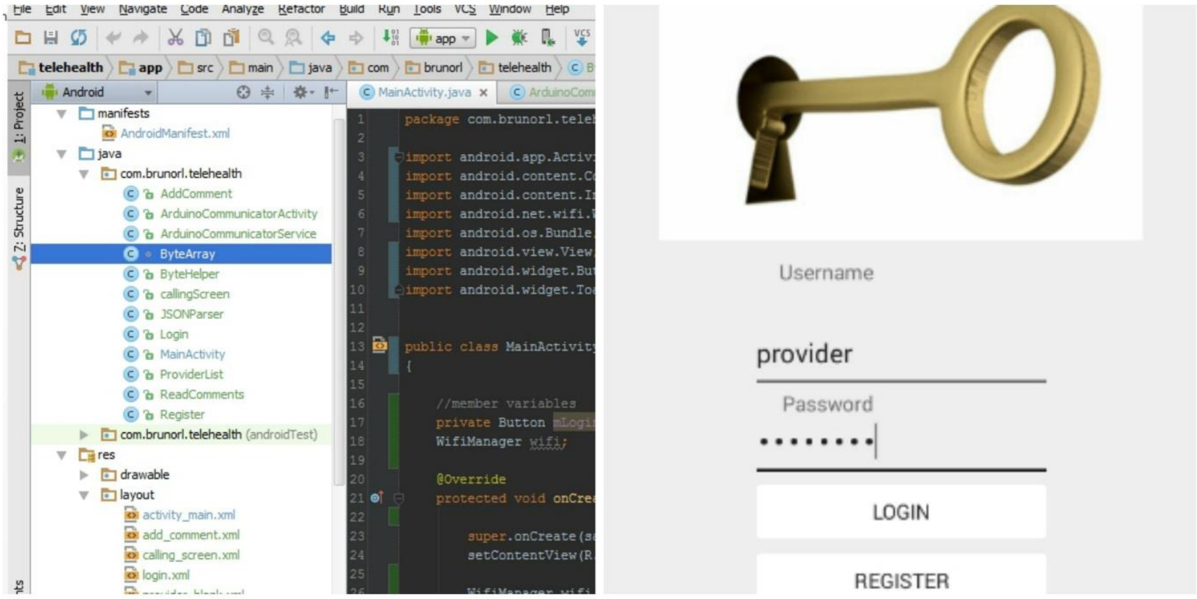
Show : 30 row(s) starting from row # 0 in horizontal mode and re

Figure 17: Database access control list, equivalent to an EHR access

Future implementation could include live video stream, and real time interaction with connected sensors. The design pattern implemented suggests the adoption of SIP for the VoIP protocol and h.232 for the video stream.

Following the Back-End design, the system implemented followed proposed scope:

✓ Secured access to system Electronic Health Records (database)



```
package com.brunorl.telel

import android.app.Activ
import android.content.C
import android.content.I
import android.net.wifi.
import android.os.Bundle
import android.view.View
import android.widget.Bu
import android.widget.To


public class MainActivit
{

    //member variables
    private Button mLogi
    WifiManager wifi;

    @Override
    protected void onCre

        super.onCreate(s
        setContentView(R
```

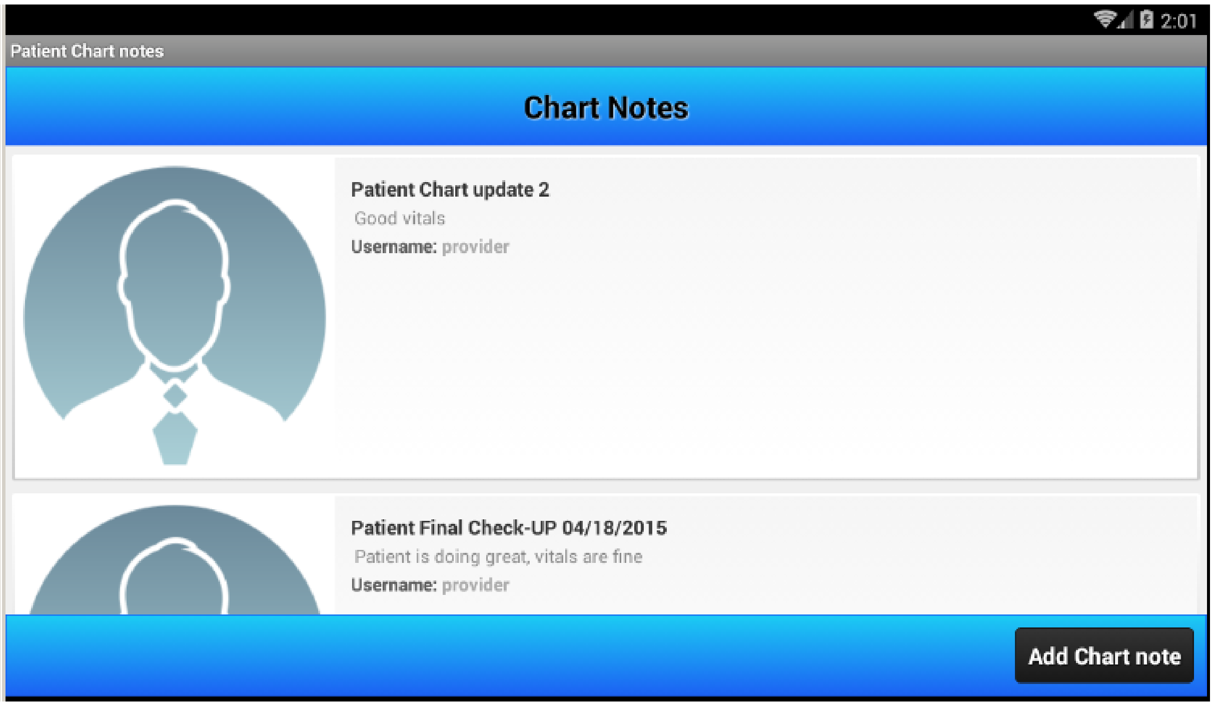
Username: provider

Password: ••••••••

Figure 17: Project design structure ready for expansion and database access via PHP script

After authentication, access to patient records are provided from the EHR database concluding the successfully secured controlled access to patient records.

- ✓ Exchange of data between Client (write) and Provider (read) nodes
- ✓ Secure logoff and timeout policy



Patient Chart update 2
Good vitals
Username: provider

Patient Final Check-UP 04/18/2015
Patient is doing great, vitals are fine
Username: provider

Figure 17: Project design structure ready for expansion and database access via PHP script

4.2 Discussion

In this section I will be discussing a few issues and detours taken along the project implementation. During the initial phase an overall idea for the final solution was to have a centralized back end server database managing all data among nodes, including data from microcontrollers and the ever changing key pairs for the Debian routers connection. Due to the time given, some of this additional features that would increase feasibility and security were pushed out of main scope, resulting on a functional yet not optimal prototype implementation. Another aspect relevant to note is that the Arduino board is currently storing the finger-print data points file in cache locally to each node, and currently requiring a 3rd role (System Administrator) and a different device to register and associate the finger print to a potential user (Client/Provider). The time constraint also impacted the design presented in the GUI, the possibility of building a custom hardware enclosure and the development of live stream of audio and video between client and provider. Although the system structure support future enhancements due to the lack of time the main priority was based on project scope. The biggest challenges presented in this project were not system complexity nor lack of research, the biggest challenge was time constraint.

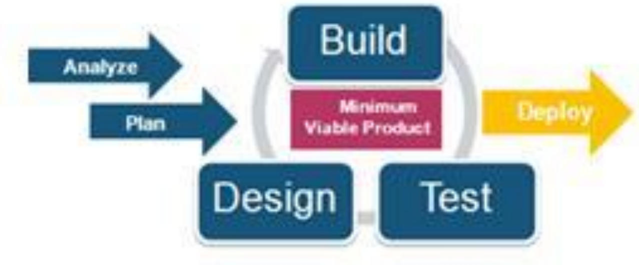


Figure 17: Final Project implementation strategy

Time management played a big role in this project, on each iteration documentation and testing were required, this was however a great practice for software development using the Agile methodology.

Chapter 5

5.1 Summary

The final project structure changed from the original proposed strategy, due to some difficulties using the serial fingerprint API new account enrollment requires the System Administrator role to register and configure new users.

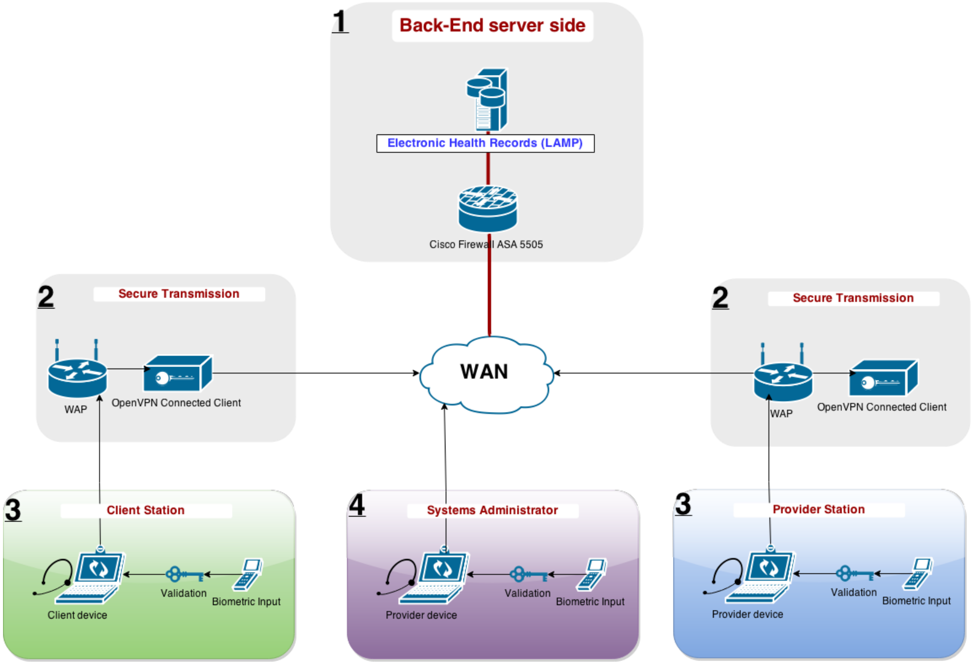


Figure 17: Final Project implementation strategy

The Systems Administrator role now includes account registration in addition to system support, additional requirements might vary depending on implementation adopted. The purpose of this prototype implementation is to adapt solution to level of care proposed, in an environment where a clinic require remote providers to register new patients remotely such accommodations could be developed.

In order to push this solution into a production environment the adoption of different biometric sensors is desirable regarding the level of care adopted from the health professional. It is important to note that the prototype microcontroller interface development was built to support the usage of different sensors, but along with further software customization new database tables should follow new forms of input.

5.2 Implications

The use of a distributed peer to peer platform can also generate a few issues regarding data retention, data ownership, access control policies and centralized system control. Note that the very purpose of this project is to empower the health professional so this professional can provide better service. The level of care reflects on guidelines and organizational structure adopted by health professional. The solution strategy focus the approach in the professional itself, that interacts with clients and have an infrastructure working with him/her. This proposed strategy aims to improve the quality of the level of care provided, this must follows general clinical practices but is capable of accommodating future customization and expansion. In a nutshell the presented prototype offers a base system for professionals to provide health services on a secure and billable manner, further expansion and customization are possible and required.

5.3 Recommendations

As a prototype a lot of features were missing from this project to be suited for a production environment and adequate adoption within the health industry. With given time I would consider enhancing the user interface to provide a better user experience; hardware design for an enclosure that fits front-end devices together was one of the initial concepts pushed out of scope due to scarcity of time; implement more health sensors and robust the system adopting proper design patterns and algorithms to facilitate future expansion.

5.4 Conclusion

The main purpose of this project was to integrate different technologies I was exposed to while during my time on academia and previous professional experience, in order to design and build a prototype solution to a common problem. My perspective about Telehealth and the Health industry in general finds that a lot of new technologies do emerge and serve a single purpose in isolated cases and environments, but we do lack on a final solution that fits all needs. Currently in Alaska we have both scenarios, an implementation of Telehealth using AFCHAN Carts which works on small clinics but not offered as an individual per patient solution, and the need of Telemedicine on isolated native communities with scarce resources and difficulty access. I believe that this project demonstrated that we can develop a bridge to connect both worlds. By having a device at home patients can communicate directly with their doctors independently of a clinic or hospital to intermediate the connection. This kind of treatment improve the relationship between client and provider, approaching both ends on a more human interactivity, this type of interaction is highly valuable for example in Mental Health services and all that is required is electricity and web access in both ends. I believe that this project has the potential to change the level of care provided by professionals not only in Alaska but in any remote community in need. This main goal was achieve under heavy Health industry guidelines, protecting client sensitive data and at the same type providing a convenient method of interaction for both parties. I believe that it would take just as much work it took on design and develop a final solution to a production implementation, but with a base built and this goal in mind Alaska provides the ideal environment to pilot and pioneer an aggregated Telemedicine solution.

References

[1] Tracy A. Lustig, Rapporteur. Board on Health Care Services. The role of Telehealth in an evolving healthcare environment, Institute of Medicine of the National Academies Vol. 1, pp. 17-32, 2012.

[2] US Department of Health and Human Services, Health Resources and Services Administration, http://www.hrsa.gov/publichealth/guidelines/BehavioralHealth/behavioralhealthcareaccess.pdf, 2013.

[3] Joshua Ewing State coverage for TeleHealth Services. National Conference of State Legislators, http://www.ncsl.org/research/health/state-coverage-for-telehealth-services.aspx, 2014.

[4] University of Alaska Statewide Health Programs University of Alaska Anchorage Center for Human Development. Evolution & Summative Evaluation of the Alaska Federal Health Care Access Network Telemedicine Project. http://www.hrsa.gov/ruralhealth/about/telehealth/evolution.pdf, 2004.

[5] John R Graham. Top Health Trend For 2014: Telehealth To Grow Over 50%. What Role For Regulation?. Forbes, 2013.

[6] Rajesh Vargheese. 10 Trends why TeleHealth adoption will take off. Cisco Healthcare, 2014.

[7] Motivation by Hustle & Grind, http://goo.gl/rukj8V

[8] AMA CPT, http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/cpt.page

[9] HIPAA Regulation, http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/

[10] HITECH Provision, http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

[11] Agile development, http://en.wikipedia.org/wiki/Agile_software_development

[12] LAMP web server, http://en.wikipedia.org/wiki/LAMP_%28software_bundle%29

[13] AFCHAN Cart, http://www.afhcan.org/

[14] HITECH Guidelines, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/guidance_breachnotice.html

[15] Usability design, http://www.usability.gov/what-and-why/visual-design.html

[16] UX Matters, http://www.uxmatters.com/mt/archives/2012/06/ux-design-defined.php

[17] Content Strategy, http://boxesandarrows.com/content-strategy-the-philosophy-of-data/

[18] Content Worth, http://alistapart.com/article/a-checklist-for-content-work

[19] Android Dashboards, https://developer.android.com/about/dashboards/index.html