

Florida International University
Knight Foundation School of Computing and Information Sciences

Software Engineering Focus

Final Deliverable

Medical IoT Security

Team Members: Rebecca Devariste, Sherman Collins, Jarren Guinto, Yashasvini Kattelu, Ariel Echevarria

Product Owner(s): Sherman Collins

Mentor(s): Masoud Sadjadi

Instructor: Masoud Sadjadi

The MIT License (MIT)
Copyright (c) 2016 *Florida International University*

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Abstract

This document presents the information necessary to gain a good understanding of Medical IoT Security. The use of wireless technology to connect medical devices and apps to improve patient safety. The use of medical IoT focuses on end users. Remote patient monitoring is the most common application of IoT devices for healthcare. The IoT promises many benefits to enhancing and streamlining healthcare delivery to proactively administer to patients. IoT can provide incredible benefits to physicians, nurse practitioners, surgeons, and nurses.

Table of Contents

INTRODUCTION	5
CURRENT SYSTEM	5
PURPOSE OF NEW SYSTEM	5
USER STORIES	
IMPLEMENTED USER STORIES	7
PENDING USER STORIES	10
PROJECT PLAN	
HARDWARE AND SOFTWARE RESOURCES	12
SPRINTS PLAN	13
<i>Sprint 1</i>	13
<i>Sprint 2</i>	13
<i>Sprint 3</i>	14
<i>Sprint 4</i>	15
<i>Sprint 5</i>	16
<i>Sprint 6</i>	17
<i>Sprint 7</i>	18
SYSTEM DESIGN	
ARCHITECTURAL PATTERNS	20
SYSTEM AND SUBSYSTEM DECOMPOSITION	21
DEPLOYMENT DIAGRAM	22
DESIGN PATTERNS	22
SYSTEM VALIDATION	23
GLOSSARY	37
APPENDIX	38
APPENDIX A - UML DIAGRAMS	38
<i>Static UML Diagrams</i>	38
<i>Dynamic UML Diagrams</i>	40
APPENDIX B - USER INTERFACE DESIGN	52
APPENDIX C - SPRINT REVIEW REPORTS	69
APPENDIX D - USER MANUALS, INSTALLATION/MAINTENANCE DOCUMENT, SHORTCOMINGS/WISHLIST DOCUMENT AND OTHER DOCUMENTS	74
REFERENCES	80

INTRODUCTION

We focused on understanding our roles as a team and exploring the concept of Medical IoT (Internet of Things). This involved deep research into the security challenges of Medical IoT and brainstorming potential implementations to address these issues. One of our primary objectives was to solve the critical problem of safeguarding medical devices within hospital networks from cyber threats. These devices play a vital role in transmitting sensitive patient data and ensuring their secure and accurate operation was at the forefront of our efforts.

Current System

To start we did not have any system in place yet. We were discussing what contributions we could add to the Medical IoT development process. After our research we decided that we were going to incorporate a little bit of cybersecurity to fulfill our security goals.

Purpose of New System

The use of medical IoT Security it to implement ways to detect disease and thoroughly monitor the healthcare system. We wanted to create something that provided customized attention to patients that they would be able to benefit from. The scale of medical devices create large and sometimes complex attack surfaces. Securing medical devices and assets in the healthcare industry against cyberattacks is crucial. Our system was created to eliminate medical device blind spots across any IT infrastructure with built-in integrations.

USER STORIES

The project progressed through several phases, each with distinct objectives. Initially, the team focused on understanding group roles and researching Medical IoT, particularly its security aspects, to develop practical implementations. Efforts then shifted to addressing the challenge of protecting hospital medical devices from cyber threats, ensuring secure and accurate data transmission.

As development continued, the team explored and designed key features, including firewalls, and systems for EKG, MRI, and EEG devices. Toward the final stages, they collaborated to finalize individual projects, integrate findings, and plan how to combine results effectively. The concluding efforts involved consolidating work from different platforms into a unified system, ensuring all functions were seamlessly integrated into the website and final product.

Implemented User Stories

The team collaborated to develop specific medical devices, such as EKG and MRI machines, while configuring firewalls and establishing connectivity processes. They focused on securely connecting the devices to the network, ensuring accurate data tracking and transmission, and implementing additional security measures, including encryption, to protect sensitive patient information.

Pending User Stories

There are no more pending User Stories

PROJECT PLAN

The project began with no system in place as the team discussed potential contributions to the Medical IoT development process. After conducting research, the focus shifted to integrating cybersecurity measures to meet security goals. The system design centered on creating a secure network with firewalls to protect data, ensuring medical devices could share information securely. Plans included implementing encryption and security checks to restrict data access to authorized personnel. Key requirements included setting up firewalls and configuring various medical devices to connect securely within the system.

Hardware and Software Resources

- <https://www.paloaltonetworks.com/network-security/medical-iot-security>
- <https://asimily.com/blog/iot-device-security-top-4-ways-to-secure-your-healthcare-iot-devices/>
- <https://www.paloaltonetworks.com/cybersecurity-perspectives/iot-adoption-in-healthcare>
- https://ordr.net/solutions/healthcare?utm_medium=cpc&utm_source=google&utm_campaign=%7Bcampaignname%7D&utm_content=690706826158&utm_term=cyber%20security%20for%20healthcare&rm_ci=11308918528&rm_gid=114806177030&rm_kw=cyber%20security%20for%20healthcare&rm_mt=p&rm_n=g&rm_cr=690706826158&gad_source=1&gbraid=0AAAAAC1NsX9-c8ZO1Nrzf12hxEaTaXgJ&gclid=CjwKCAiA0rW6BhAcEiwAQH28Iti_lfYPQ9MHfvLoZXpIU-T81RMoQRLElTdo1YF5olBJxIzZSH89GBoCsboQAvD_BwE
- <https://www.nist.gov/cyberframework>
- <https://everhour.com/blog/what-is-github/#:~:text=Further%2C%20GitHub%20allows%20developers%20to,scratch%2C%20thanks%20to%20simple%20actions.>
- <https://www.somar.co.nz/blog/collaborative-web-development/#:~:text=Why%20is%20collaboration%20important%20in,fosters%20a%20client%2Dcentric%20approach.>

Sprints Plan

Sprint 1

The plan for this sprint was to focus on research, gaining a thorough understanding of Medical IoT and its challenges. The insights gained were intended to guide the initial phases of system development, setting a strong foundation for the project.

Sprint 2

The goal was to design and build a secure system for medical devices in hospital networks. This included planning for firewalls, testing device connectivity, and ensuring the system would meet both safety and functionality requirements for efficient and secure patient monitoring.

Sprint 3

This sprint was centered around early development and research for the final product. The plan involved identifying new devices to integrate into the system and strategizing how to begin assembling core components.

Sprint 4

The team aimed to finalize individual tasks and start consolidating research and findings into a cohesive plan, preparing for the next phase of integration and implementation.

Sprint 5

This sprint focused on wrapping up individual projects and initiating the process of compiling all findings and developments into a structured framework for the website.

Sprint 6

The plan for this sprint was to streamline workflows and organize all team contributions into a unified structure. This involved aligning team efforts to ensure consistency in how components and findings would be presented on the website.

Sprint 7

Sprint Seven:

This final sprint focused on refining the website and polishing the final product. The team planned to test the overall system, verify functionality, and ensure the website showcased all findings and implementations in a professional and cohesive manner.

40

SYSTEM DESIGN

Regarding the system's design we wanted our dashboard to be seamless. We understood that it would be crucial for a network security officer in a hospital to be able to have a system that isn't hard to understand. The user interface consists of a welcome page that explains the purpose and evolution of medical IoT security.

Furthermore, our medical devices were designed similarly to the way that they would operate and look in a hospital. We integrated network security connection via the network and the medical devices so that they would be connected to the network.

Architectural Patterns

Medical IoT Security incorporated several architectural patterns that assured a seamless use process. The interface integrations were created to simplify, scale, and secure all of the medical IoT devices.

The key design patterns we included were data encryption both at rest and in transit, network segmentation, firmware updates with integrity checks, anomalous detection and behavioral monitoring, and lastly, our security management centralized system.

SYSTEM VALIDATION

The system validation for medical IoT was a rigorous process. We evaluated and tested all our security features, the firewalls, and the system to ensure that all the data was protected. We identified security gaps and risks for anything that had outdated information on our end. We implemented strict authentication as well as access controls and assured us that the multi-factor authentication mechanisms were robust.

GLOSSARY

Medical IoT Security:
[Learn more](#)



Medical IoT, or the Internet of Medical Things (IoMT), is a network of medical devices, applications, and hardware that are connected to the internet. IoMT devices are designed to improve healthcare by using automation, sensors, and machine learning to reduce the need for human intervention.

Appendix A - User Interface Design

The user interface for medical IoT Security presented an overview of connected medical devices, the security status, and any type of abnormal behavior or potential threats. The user interface design was executed to include key features such as anomaly detection, device visibility, and risk assessment dashboards.

Appendix B - Sprint Review Reports

Week 1:

Features/functions that were tested thoroughly and worked as expected without any errors/issues.

■ Each user story went well as we discussed research and learned more about IOT devices in the medical field.

- As well the creation of our Github and drive folder went fine with no issue.
- Research about existing medical IOT devices went as planned. ○ Features/functions that were tested thoroughly and did NOT work as expected. Here is the list of issues/errors observed.
- There were no issues whatsoever ○ These are features/functions that were tested thoroughly and would benefit from some improvement/enhancement. Here is the list of suggested enhancements/improvements.
- The functions that were tested thoroughly and would benefit some enhancement would be: - the machine's ability to detect organs, bones, muscles, and blood vessels to identify abnormalities - improving tissue detection accuracy and enhancing image clarity. - enhancing image resolution for blood vessels.
- Features/functions that were tested thoroughly and worked as expected without any errors/issues.
- EEG: Features were tested repetitively to develop a perfect execution to further acknowledge that there was no error or issues in the feature.
- ■ ■ Features/functions that were tested thoroughly and did NOT work as expected. Here is the list of issues/errors observed.
- Firewall: After further research on how firewalls worked I learned more about the security aspect of them. As well I tested some vmware on virtual machines for routers to start implementing them on a router itself. The main problem being how difficult it may be to implement a "firewall" itself into our final product itself.

EKG: some of the features in this user story were developed but there wasn't enough time in this sprint to test it and x any bugs/issues or potential problems. Therefore, I'm not very sure if all the features work without any problems.

- All of the new additions, updates, and features were implemented completely well. ■ • Added features that would be able to detect minor and major

- abnormalities but more specically minor abnormalities for advanced prevention. ■ •An additional feature to make it more cohesive to most, if not all of the organs.

- Succeeded with the development of advanced prevention so that all abnormalities were caught before spreading and aecting the patient significantly.

- ■ These are features/functions that were tested thoroughly and would benet from some improvement/enhancement. Here is the list of suggested enhancements/improvements.

- Features/functions that were tested thoroughly and worked as expected without any errors/issues.

- Rebecca: I was able to complete everything from the sprint and review my previous tasks from weeks before. I have made sure that all of my work syncs with one another.

- Yashasvini: worked on developing a user story that improves the security of the patient's data and collaborated with team members to put together a nal product

- Jarren:I developed a feature where remote management helps troubleshoot connectivity issues faster and maintain device security.

- Sherman: Each user story went well. I did more research about how rewall security mainly works for medical devices. The team will be meeting to start working on the nal product.

- Ariel: I worked on features that involve seeing which devices are on and o throughout the hospital. Everything went well during my research.

- Features/functions that were tested thoroughly and worked as expected without any errors/issues.

- Rebecca: I was able to collaborate with my peers and work on github on our presentation.

- Yashasvini: collaborated with teammates to put together all of our work for the nal presentation

- Jarren: I am helping lead development of the website for features etc.

- Sherman: Lead development of the website for our product there just needs to be more features and information added.

- Ariel: ■ Started to put together all my of my research with the teammates and begin the website

Appendix C - User Manuals, Installation/Maintenance Document, Shortcomings/Wishlist Document and other documents

User Manual / Maintenance Guide Reference:

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/iot/iot-security-admin/iot-security-admin.pdf

Shortcomings/ Wishlist:

- **Patient-Centric Features:** Adding features like **remote monitoring**, **health tracking**, or the ability for patients to communicate directly with their healthcare providers.
- **Mobile Accessibility:** Ensure that the dashboard is mobile-friendly or has a companion app for easy access by medical staff on the go.
- **Data Visualization:** Consider using advanced visualizations such as **heat maps**, **trends over time**, or **predictive modeling** to help clinicians interpret complex data more effectively.

REFERENCES

- <https://docs.paloaltonetworks.com/iot/iot-security-admin/medical-iot-utilization/utilization-dashboard>
- <https://docs.paloaltonetworks.com/iot/iot-security-admin/medical-iot-utilization>
- <https://docs.paloaltonetworks.com/iot/iot-security-admin/medical-iot-utilization/biomed-dashboard#ide7158244-2e2f-4f39-9f1c-baaba72b70ee>
- <https://docs.paloaltonetworks.com/iot/iot-security-admin/medical-iot-utilization/utilization-information-panels#idd0826234-780e-488b-a095-2bb6ddd18d27>
- <https://docs.paloaltonetworks.com/iot/iot-security-admin/iot-security-overview/iot-security-portal>
- <https://www.paloaltonetworks.com/resources/techbriefs/healthcare-iot-solution-brief>
- https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/healthcare-iot-solution-brief
- <https://www.youtube.com/watch?v=JgCwl7iBalo&list=PLWGxHWZa19Z0vxG3eNuoSB3fT6kp5Q6A5>
- <https://asimily.com/blog/iot-device-security-top-4-ways-to-secure-your-healthcare-iot-devices/>

- <https://cylera.com/>
- <https://www.cynerio.com/blog/cynerio-launches-data-security-and-protection-toolkit-dashboard-for-nhs-trusts>
- <https://www.nozominetworks.com/industries/healthcare-cybersecurity>
- <https://claroty.com/blog/healthcare-iot-101-guide-to-the-internet-of-things>
- <https://klasresearch.com/compare/healthcare-iot-security/374>
- <https://www.gartner.com/reviews/delay?nextpage=%2Freviews%2Fmarket%2Fmedical-device-security-solutions>
- <https://www.meditologyservices.com/medical-device-iot-security/>
- <https://www.paloaltonetworks.com/blog/network-security/medical-iot-enhancements/>
- <https://www.criticalinsight.com/blog/top-6-hackable-medical-iot-devices>
- <https://www.archonsecure.com/blog/medical-device-iot-security-risk-solutions>
- <https://expertinsights.com/insights/the-top-iot-security-solutions-for-healthcare/>
- <https://ordr.net/article/iot-healthcare-examples>
- <https://phosphorus.io/solutions/healthcare/>
- <https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/industries/healthcare>
- <https://lembertsolutions.com/blog/healthcare-iot-security-essentials-risks-and-practical-solutions>
- <https://www.allegrosoft.com/iot-medical-device-security/>
- <https://comport.com/resources/security/medical-device-iot-security-launch-your-defense-with-palo-alto-and-comport-secure/>
- <https://www.sciencedirect.com/science/article/pii/S2666990022000222>
- <https://www.healthcareitnews.com/news/thousands-medical-devices-and-systems-pose-iot-security-risk>
- <https://www.elisity.com/blog/protecting-patients-ensuring-iot-medical-device-security>
- <https://www.checkpoint.com/solutions/iot-security/>
- <https://www.idc.com/getdoc.jsp?containerId=US48580322>
- <https://www.armis.com/newsroom/press/armis-identifies-the-riskiest-medical-and-iot-devices-in-clinical-environments/>