BodiGuide

1 Introduction

Cardiovascular diseases remain a leading cause of mortality worldwide, underscoring the urgency to develop innovative solutions for early detection and prevention. In this context, the integration of advanced medical devices, such as the BodiGuide Device (1), presents a unique opportunity to revolutionize the way we approach heart health. The BodiGuide Device offers a wealth of valuable data that, if harnessed effectively, can empower users to proactively safeguard their cardiovascular well-being.

The primary challenge at hand is not merely acquiring data from the BodiGuide Device, but ensuring the secure acquisition, storage, analysis, and response to this data in a manner that complies with the stringent standards of the Health Insurance Portability and Accountability Act (HIPAA). This project is motivated by the imperative to bridge the gap between data acquisition and actionable insights, all while adhering to the highest standards of patient data protection.

Overview of Project Sections:

- Problem Statement: In this section, we will delve into the specifics of the challenges posed by the current state of cardiovascular health monitoring and the limitations that necessitate the development of a comprehensive solution.
- Literature Review: A comprehensive examination of existing research and technologies related to cardiovascular health monitoring, data security, and HIPAA compliance. This review serves as the foundation for the development of our innovative solution.
- Solution Design: Here, we will outline the conceptual framework for our solution, detail ing the key components and functionalities required to address the identified challenges.
  - System Design: A detailed exploration of the technical architecture and compo nents of the proposed system, focusing on how data is acquired, processed, and utilized to generate actionable insights.
  - UI Design: User interface design plays a pivotal role in ensuring that users can interact seamlessly with the system. This section will showcase the intuitive and user-friendly design aspects implemented to enhance the overall user experience.
  - Security Design: Given the sensitivity of health data, an in-depth analysis of the security measures implemented to ensure the confidentiality, integrity, and availability of patient information. This section will highlight how our solution aligns with HIPAA compliance standards.
- Usability and Testing: An evaluation of the usability of the system, including user testing methodologies and results. This section will provide insights into how well the solution meets user expectations and requirements.

- Future Works: Envisioning the evolution of our solution, this section will explore poten tial enhancements, technological advancements, and avenues for future research to further advance cardiovascular health monitoring.
- Conclusion: Summarizing the key findings, accomplishments, and contributions of our project, the conclusion will provide a concise overview of the project's impact on cardio vascular health monitoring and the broader healthcare landscape.

Through the exploration of these sections, we aim to provide a comprehensive understanding of our approach to securely acquiring, storing, analyzing, and responding to data from the BodiGuide Device, ultimately empowering users to take preventative measures against heart attacks in a HIPAA-compliant manner.

2 Problem Statement

Heart failure, a prevalent and escalating health concern in the United States, affects six million individuals, a number projected to rise to eight million by 2030. The urgency of this matter is underscored by the prevalence of Acute Heart Failure (AHF), a condition characterized by rapid fluid overload and the primary cause of hospitalization for those over the age of 65. This results in a staggering one million hospitalizations annually, generating a substantial economic burden of $27 billion. Furthermore, heart failure hospitalization not only increases mortality rates but also significantly diminishes the quality of life for affected individuals.

The lack of quantified methods for monitoring a patient's fluid status poses a substantial obstacle to effective heart failure management, leading to avoidable hospitalizations. Current monitoring methods are insufficient, limiting the ability of healthcare providers to optimize treatment plans and deliver timely interventions. This critical gap necessitates the development of a sophisticated remote monitoring system that can accurately and continuously assess pe ripheral edema—a key indicator of fluid status—in a manner compliant with Health Insurance Portability and Accountability Act (HIPAA) standards.

BodiGuide's Solution: Ankle Monitoring for Heart Failure Management In response to this pressing need, BodiGuide has pioneered a solution—a cutting-edge anklet designed for accurate and continuous monitoring of ankle circumference. This innovative device provides a reliable measure of peripheral edema or interstitial fluid volume, offering a patient's ”swelling pattern” as an indicator of their fluid status. This data, when interpreted, provides crucial feedback to patients, caregivers, and clinicians, facilitating improved self-care and opti mized treatment plans. By leveraging this technology, the aim is to minimize hospitalizations and enhance the overall quality of life for individuals managing heart failure and related condi tions.

Project Scope: Developing a Secure and Scalable Remote Monitoring System The goal of this project is to research, design, and develop a prototype system utilizing an AWS scalable architecture. This system will support remote monitoring in the patient setting, ensuring the secure collection of data via medical-grade cellular gateways from BodiGuide's ankle monitoring devices. The envisioned system will process this data, associate patient information with their respective end-users (including patients, non-medical caregivers, and clinicians), and implement BodiGuide's concept of ”Health Metrics.”

Specific Aims and System Components:

- BodiGuide Platform: Design and implement a system in the AWS environment to col lect, store, and manage patient data, associate patient information with end-users, and implement BodiGuide's ”Health Metrics” concept.
- Communications: Research and develop an architecture for two-way data communications between the BodiGuide Platform and environments involved in remote patient monitoring

PAPER	Implementation	Flaw/Issue

(2)	By collecting data, transmitting it to the cloud and providing service to the users, the authors of the paper proposed an architecture to monitor the vital signs of patients with chronic diseases.	This paper does not delve much into securing the framework.
(3)	This paper is about a fog based ECG feature extraction system to improve performance of ECG feature extraction in healthcare IoT applications with Fog server and cloud server.	This does not talk about the data storage, transmission and security.
(4)	This paper discusses the importance of security in MQTT-based IoT applications and proposes a number of security measures that can be implemented to protect MQTT-based IoT systems from attack.	This paper does not discuss about the performance implications of the security.

Table 1: Literature Review

solutions.

- Devices: Obtain and store data from BodiGuide anklets or other devices via a Stel Life medical-grade cellular gateway. Provide instructions for the gateway configuration man ager.
- Patient Data Repositories: Retrieve patient data from repositories such as EHR systems, pharmacies, clinical trial data, assisted living, or home care agencies. Submit patient data to Patient Data Repositories for inclusion in the patient record.
- End Users: Send notifications (text, phone, email, application data) to end-users and collect information via applications.
- Communication Standards: Provide a report on secure communication architecture in the context of industry standards.

This project seeks to bridge the existing gap in heart failure management by creating an ad vanced, secure, and scalable remote monitoring system. By aligning with BodiGuide's vision, the aim is to empower patients, caregivers, and clinicians with timely and actionable insights, thereby revolutionizing the approach to heart failure management and significantly reducing avoidable hospitalizations.

3 Literature Review

Through our literature review, three papers stood out. Theses are the papers summarized in table: 1 and explained in this section.

- "An IoT-inspired cloud-based web service architecture for e-Health applications, (2)"
  - Implementation: The authors propose an architecture to monitor vital signs of pa tients with chronic diseases by collecting and transmitting data to the cloud for user

services.

– Flaw/Issue: Unfortunately, the paper lacks in-depth exploration of securing the framework. Security considerations are vital in healthcare data management, and

the omission of this aspect raises concerns about potential vulnerabilities in the pro posed architecture.

• ”Fog Computing in Healthcare IoT, (3)”

– Implementation: The paper focuses on a fog-based ECG feature extraction system to enhance performance in healthcare IoT applications, utilizing both fog and cloud servers.

– Flaw/Issue: However, the paper neglects crucial aspects related to data storage, trans mission, and security. Without addressing these elements, the system’s reliability and patient data confidentiality may be compromised.

• ”Secure MQTT in IoT, (4)”

– Implementation: The paper discusses the importance of security in MQTT-based IoT applications and suggests security measures to protect systems from attacks. – Flaw/Issue: Notably, the paper falls short in discussing the performance implications of the proposed security measures. Understanding the potential impact on system performance is crucial for balancing security and operational efficiency.

These papers contribute valuable insights to healthcare IoT implementations but highlight specific shortcomings. Addressing these flaws, such as the lack of security considerations in Pescosolido et al.’s work, the oversight of data-related aspects in Gia et al.’s study, and the absence of performance discussions in Singh et al.’s paper, is essential for creating robust and balanced healthcare IoT systems. Future research should aim for a comprehensive approach that integrates security, data management, and performance considerations for optimal imple mentation.

4 Solution Design

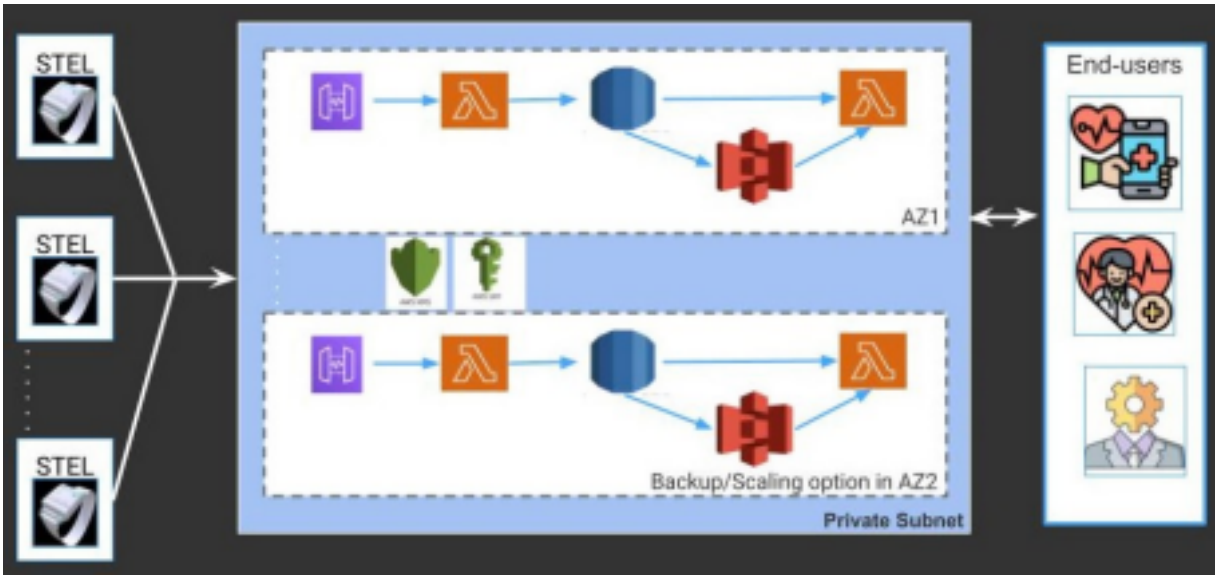


Figure 1: Comparitive study of commonly studied machine learning algorithms

The solution design, as seen in Figure 1 for the remote monitoring system leverages a ro bust architecture, ensuring both security and scalability in managing data from the BodiGuide anklets. Here's an overview of the key components and their functionalities:

- Wearable Technology: - Users wear anklets designed by BodiGuide to continuously monitor ankle circumference, providing valuable data related to peripheral edema.
- STEL Interface: - Each anklet is connected to a STEL interface (5), serving as a gateway to transmit the collected data securely.
- Data Transmission to AWS: - The STEL interface pushes the collected data to the AWS API Gateway, ensuring a secure and reliable connection.
- AWS RDS for Data Storage and Analysis: - The data received through the API Gateway is written into Amazon Web Services (AWS) Relational Database Service (RDS) for further analysis and storage, ensuring efficient data management and retrieval.
- AWS S3 Data Archiving: - A scheduled cron job triggers the transfer of data from AWS RDS to Amazon Simple Storage Service (S3) on a monthly basis. This archival process optimizes data storage while maintaining accessibility for historical analysis.
- API Gateway for Data Presentation: - An additional API Gateway pulls the data from AWS RDS, making it accessible for presentation on the user interface (UI). This gateway plays a pivotal role in ensuring a seamless connection between the backend data and the frontend display.
- User Interface (UI): - The UI is accessible by both patients and physicians, providing distinct functionalities for each user type. - Patients: Have access to their individual data, allowing them to monitor their health metrics and swelling patterns. - Physicians: Can view data for the patients assigned to them, facilitating informed decision-making and personalized patient care.
- AWS Pipeline Redundancy: - The AWS pipeline incorporates a backup system to ensure scalability and robustness. - In cases of increased user load or potential cyber threats such as Denial of Service (DoS) attacks, the backup pipeline can be seamlessly activated to maintain system performance and data integrity.

This solution design not only addresses the immediate need for remote monitoring of heart failure but also prioritizes data security, scalability, and resilience against potential cyber threats. By employing AWS services, the system ensures a reliable and efficient infrastructure for continuous patient care and clinical decision support.

4.1 System Design

Building upon the innovative solution design outlined earlier, let's delve deeper into the intricate details:
1. Anklet-STEL Interface: The Anklet-STEL interface empowers our bodiguide anklet to seamlessly collect and transmit data to the STEL platform. Key features of STEL include:

– Patented Passive Pairing for effortless connectivity.

– Automatic connections to compatible devices without navigating through Bluetooth set tings.

– Reliable Low-Bandwidth and Multi-Carrier Coverage, eliminating concerns about patient

infrastructure.

– Unidentified Data handling ensures privacy, with no PHI or Customer Data shared exter nally. STEL only captures values and meta-data from device peripherals.

– Secure association management by Care teams and Digital Health Orgs without compro mising patient identifiers.

2. AWS Services Setup: Leveraging AWS cloud services, we ensure the secure movement, storage, and analysis of health metrics.
3. UI Design:

– Our UI design process begins with thorough user research and requirement analysis.

– We establish a foundation using UI wireframes, crafting a visually appealing and user friendly prototype.

– The prototype undergoes rigorous usability testing, providing invaluable insights for refin ing and optimizing different elements.

This comprehensive approach ensures a robust and user-centric solution, blending cutting-edge technology with seamless user experiences.

4.1.1 Anklet-STEL Interface

Figure 2: Anklet-STEL Interface

Bodiguide Anklet Details: The BodiGuide Edema Monitor, a unique passive design in wearable technology, provides continuous and direct monitoring of leg edema. It employs sensors and a strap design for easy monitoring with applications ranging from heart failure to post-operative complications.
Unique Features:

• Continuous Monitoring: Measures ankle swelling effortlessly.

• Privacy: Stel prioritizes security, not storing or transmitting PHI.

• Cloud Communication: Seamless transmission of data, algorithmic escalation to patients and caregivers.

Anklet-STEL Interface Stel's groundbreaking Anklet-STEL Interface ensures effortless transmission of vital health data from diverse devices to dedicated care teams. Anchored by the Stel Vitals Hub, equipped with a patented passive-pairing OS, this interface connects patients' devices seamlessly. The hub, using Bluetooth and cellular networks, transmits data securely to the Stel platform without storing or transmitting any Personal Health Information (PHI).
Key Components:

- Stel Vitals Hub: The gateway for Bluetooth-enabled vitals devices, connecting and trans mitting data securely.
- Vitals Devices: An extensive range, from scales to glucometers, transmitting data in the vicinity of the Hub.

- Measures: Discrete values collected by devices with associated metadata. •

Endpoints: Stel transmits real-time measures to destinations via HTTPS endpoints.

In summary, the implemented Anklet-STEL Interface redefines healthcare technology, ensuring privacy, innovation, and seamless communication for enhanced patient care.

4.1.2 AWS Services setup

Our solution harnesses the power of various AWS services for seamless functionality:

- AWS API Gateway: Acts as the entry point, managing API requests and facilitating smooth communication between components.
- AWS Lambda: Enables serverless computing, executing code in response to events, ensur ing efficiency in our data processing.
- AWS RDS (Relational Database Service): Manages our relational databases, ensuring structured and organized data storage.
- AWS S3 (Simple Storage Service): Stores and retrieves large volumes of data, providing durability and accessibility.
- AWS KMS (Key Management Service): Ensures secure key management for encryption, adding an extra layer of data protection.
- AWS IAM (Identity and Access Management): Manages user access and permissions, enhancing security in our solution.

This integration enhances scalability, security, and efficiency, making AWS an integral part of our solution's success.

4.1.3 Data Flow

The Anklet-STEL Interface meticulously manages and secures data flow from the user's device to AWS through a well-orchestrated configuration involving AWS API Gateway, Lambda, and various security measures.

Data Structure:

– User Identification: Captured through ”id.”

– Device Identification: Comprises ”macAddress”,”HubId”, ”make,” and ”model.”

– Health Metrics: Includes ”bpm,” ”temp,” ”angle,” ”dtime,” ”battery,” ”device sequence,” ”circumference of the anklet strap,” ”stand up percentage,” timestamp, and activity type.

AWS API Gateway Configuration:

– Trigger Mechanism: AWS API Gateway triggers AWS Lambda upon data push.

– Authentication: Managed through AWS KMS, validating authorization tokens.

– Device Authorization: Confirmed by cross-referencing device ID with the database to prevent unauthorized IoT devices.

– Data Insertion: Upon successful authentication and authorization, the data seamlessly integrates into AWS RDS.

Validation and Security:

– User Validation: Patient ID cross-verified with database information; data rejected if inconsistencies exist.

– Device Validation: Device ID authenticated against the database; unauthorized devices trigger notifications to admin.

– Error Handling: Admin alerted to any errors during AWS RDS data insertion, ensuring swift investigation.

AWS Security Measures:

– VPC Implementation: AWS VPCs ensure the privacy of services.

– Token Authentication: Utilizes AWS KMS and IAM for role-based access, enhancing se curity.

– RDS Certificate: Ensures a secure DB instance with a valid certificate during data writes.

– S3 Access Rules: Implemented to restrict S3 bucket access to users based on IAM roles, bolstering data security.

This comprehensive approach to data flow and security within the AWS ecosystem reflects a commitment to user privacy, device integrity, and robust system reliability.

4.1.4 UI Design

The UI development lifecycle is a systematic process designed to create user interfaces that are not only visually appealing but also functionally efficient. The process, as listed below, unfolds in a series of well-defined steps, ensuring user satisfaction and system reliability. Step 1. User Research: Concise user research was conducted to gain a deeper understanding of the target demographic for the device. This involved gathering key insights into their char acteristics, needs, and preferences, ensuring a more tailored and effective design approach.
Step 2. User Requirements: Identify stakeholders, including patients and providers, to gather comprehensive user requirements.
Step 3. UI Design: Develop wireframes and mockups to visualize the user interface, ensuring alignment with identified requirements.
Step 4. UI Front End Development: Develop a functional prototype, integrating interac tions, elements and front end API requirements.
Step 5. UI Backend Development: Implement the UI backend, integrating AWS, ReactJS, and Stel for seamless functionality and data flow.
Step 6. User Testing: Assess user experience using the Mars scale and other relevant metrics to identify strengths and areas for improvement.
Step 7. Quality Assurance: Rigorously test usability, functionality, and accessibility, ensur ing the UI meets high-quality standards.
Step 8. Deployment: Release the UI to stakeholders, making it available for use by patients, providers, and other intended users.
Step 9. Monitoring/Maintenance: Continuously monitor user feedback and analytics, fa

cilitating iterative improvements and ensuring sustained quality.
Step 10. Repeat Steps 1 to 9: Iterate based on user feedback and evolving requirements, ensuring the UI remains adaptive and responsive.

This UI development lifecycle is a dynamic and user-centric approach, emphasizing user sat isfaction, system reliability, and continuous improvement throughout the development process.

4.2 Security Design

In conducting a thorough risk assessment and analysis for our cybersecurity framework, we first identified events through integrated threat models, revealing surprising insights into attack sce narios. Our meticulous evaluation encompasses likelihood assessments, success probabilities, and impact scoring, offering a comprehensive understanding of potential risks associated with each event. Let's delve into the details of our risk assessment and explore the quantified landscape of cybersecurity threats and their potential impacts.

- Identification of Events:
  - Utilized Threat models to identify events, defined as the combination of attack and location (what was done and where).
  - Merged attack-tree-data-flow-hybrid charts to create a unified chart, revealing surpris ing insights, notably the absence of events for test user accounts or hospital devices.
  - Identified the highest number of events associated with the STEL device.
- Likelihood Assessment:

  A. Attempt Likelihood:
  - Evaluated the likelihood an attacker would be interested in each goal (root nodes of attack trees).
  - Derived from the combination of component motivation likelihoods, factoring in percentages from credible sources [8].
  - Resulting table showcases calculated component attempt likelihoods.

  B. Success & Goal Likelihood:
  - Introduced a Likelihood score table to assess the success likelihood and goal achievement likelihood for each event.
  - Scored based on available probabilities or likelihood scores for various attack scenarios.

  C. Complete Likelihood:
  - Combined all the likelihood data to create a comprehensive likelihood table for each event.
  - Utilized multiplication of probabilities in the 0-1 range to derive the complete likelihood.
- Impact Assessment:
  - Established a scoring system for impact, ranging from 0 (no effect) to 10 (terminal effect).

– Calculated the impact for each event by considering the maximum impact among associated goals.

• Final Assessment Results:

A. Scores:

– Multiplied likelihood and impact scores to obtain overall risk scores for each event.

– Scores range from 0 to 100, providing a quantifiable representation of the risk associated with each event.

B. Graphical Representation:

– Graphical representations of likelihoods, impacts, and overall scores offer visual insights into the risk landscape.

This comprehensive risk assessment provides a structured approach to understanding and quan tifying potential risks associated with various events. By considering the likelihood, success potential, and impact, organizations can prioritize security measures and focus on mitigating high-risk scenarios.

4.2.1 Identification of Events

The first step was to use the Threat models we had to identify events. The way events are defined for our project is the combination of attack and location. What was done and where. This was done by merging all the attack-tree-data-flow-hybrid charts into one. While merging them, the original goal(s) for each event was saved. This flowchart is seen in Figure: 3.

Figure 3: Flow chart to identify the events

The chart told us that surprisingly no events were found for test user accounts or hospital devices. This is likely a sign that the threat models did not fully take all possible attack routes into account. Unfortunately we do not have enough time to expand our threat model. Interestingly the STEL device had the most events.

4.2.2 Likelihood Assessment

The likelihood of each event is split into three parts: Attempt likelihood, Success Likelihood, and Goal Likelihood.

Attempt Likelihood

The first step was to go through the goals and find the likelihood an attacker would be inter ested in each goal. The goals are simply the root nodes of the attack trees. These likelihoods are somewhat like the amount of motivation each goal has. They are meant to represent the probability a given attack, who attacks, will be interested in a certain goal. The source of the percentages came from [8]

Figure 4 is the chart containing root motives for cyberattacks. These motives are not mu tually exclusive; however, we assume they are independent of each other. In order to calculate the likelihoods the component motivation likelihoods were all combined for each. They are with the following formula. Where x and y are the percentage probabilities you wish to combine and it outputs the combined probability. This is a union. This may be done recursively if there are

Motive	Symbol	Percent
Ransom	R	41%
Insider threat	I	27%
Political	P	26%
Competition	C	26%
cyberWar	W	24%
Angry user	A	20%
motive Unknown	U	11%

Figure 4: Attempt Likelihood scores

$$f(x,y) = y - \left(x * \frac{y}{100}\right) + x$$

more that 2 component motivations. This effectively gives the percent chance that a specific root goal will align with a random attacker (who actually attacks).

Goal	Symbol	Component Motivations	Likelihood	Impact
Grey-hat	G	-	11	5
Activism	A	P	37	4
Black-hat	BH	I,A	52.8	5
Corporate espionage	E	C,W	54.76	4
Harm user	H	I,W	55.52	8
Corporate sabotage	S	C,W,A	66.088	10
Terminate employee	R	I,C,A	67.784	3
Steal Compute Recources	C	R,I	67.93	3
Extract Money	M	R,I	67.93	5
Botnet	BN	I,P,W	69.9448	8
Hardware theft	T	R,I,C	79.1282	1
Data disclocure	D	R,I,P,W	86.777432	7

Figure 5: Percent chance that a specific root goal will align with a random attacker

The above table shows the calculated component attempt likelihoods The full attempt likeli hood then calculated for each event using the same method for calculating the above likelihoods. The results are displayed in Figure 6.

Success & Goal Likelihood The next two parts are done together. The success likelihood is the chance that said event works, or can happen. When possible a more rigorous probability that represents the probability of success is used (multiplied by 10); however, such a probability is not always available. When such a probability cannot be used, the table 2 will be used instead.

This table is also what is used for the goal likelihood, which is the likelihood that the

attacker's goal is accomplished given that the event succeeds. For example, If an attacker gets into someone's email to leak data, what is the chance they will find the data in the emails. Many impacts rely on the attack actually doing something, which is why this likelihood is considered. Below are the tables with each event's likelihood. All spoofing and sniffing events are assigned 0.03 by default due to our encryption, according to (12) RSA (widely used encryption method) has a 0.3% of cracking. Any attempt at hacking an account is assigned 7.3 as according to (11) 73% of passwords can be cracked in seconds. SIM-Jacking is given an 8 due to the 80% success rate reported by (8). Malware is given a 8.765 due to the 95% success rate of default windows defender antivirus according to (9) combined with the 87% rate in which users will ignore their antivirus according to (10).

Social engineering is given a 7.5 by default because of the claim by (7) that at strong

Location	Attack	Goals	Attempt likelihood
User device	Spoof notifications	H,S	84.88
	Hack email	D	86.78
	SIM-Jacking	D	86.78
	Malware	D,A,BN	97.50
	Spoof device	BH,G	57.81
	Sniff traffic	BH,G	57.81
Patient	Steal from patient	T	79.13
	Social engineering	D,M	95.76
Anklet	Hide	T	79.13
	Break	T	79.13
	Pretend broken	T	79.13
	Remove chip	D	86.78
	Rewrite firmware	BN	69.94
	Spoof	BH,G	57.81
	Sniff	BH,D,G	94.42
STEL	Hide	T	79.13
	Break	T	79.13
	Pretend broken	T	79.13
	DoS	H	55.52
	Rewrite firmware	BN	69.94
	Spoof device	BH,G	57.81
	Sniff	BH,G	57.81
	Trojan	BN	69.94
	Spoof fake data	H,S	84.88
AWS	DoS	S	66.01
	Childrens data breach	S	66.01
	Social Engineering	M	67.93
	Trojan	C	67.93
	Spoof	BH,C,G	86.47
	Sniff	BH,D,G	94.42
Developer Machine	Sniff	E	54.76
	Trojan	C	67.93
	Access Account	A,BN,C,D,E,M,S,R	99.99
Developer	Social Engineering	A,BN,C	93.93
Employee	Steal device	T	79.13
	Make work difficult	R	67.78
	Social engineering	E,M,R	95.33
Office Machine	Hack account	R	67.78
	Forge sell data	S	66.01
	Modify packets	M	67.93
UI	DoS	H,S	84.88
	MaS	C	67.93
	Crack passwords	BH,G	57.81
	Injection	A,BH,BN,C,D,E,G,S,R	99.98
	Worm	A,C	79.80
Outsider Device	Frame employee	R	67.78
Outsider	Slander	S,R	89.05
Doctor	Steal hardware	T	79.13
	Social engineering	D,T	97.24

Figure 6: Overall assessment of Likelihood of attacks

Likelihood score	Description

0	Will not be successful
1	Will only work if attacker is very lucky
2	Is surprising if works
3	Usually fails
4	Should not be surprised if works
4	Should not be surprised if works
5	Equally likely to be successful or unsuccessful
6	Should not be surprised if fails
7	Usually works
8	Would be surprising if it did not work
9	Will work unless attacker is very unlucky
10	Will always work

Table 2: Likelihood score

User device	Likelihood of successful attack	Likelihood of achieving goal
Spoof notifications [6]	0.3	2
Hack email [5]	7.3	2
SIM-Jacking [2]	8.0	2
Malware [3][4]	8.765	8.5
Spoof device [6]	0.3	1
Sniff traffic [6]	0.3	2

Table 3: Likelihood of successful attack

Patient	Likelihood of successful attack	Likelihood of achieving goal
Steal from patient	3	10
Social engineering [1]	7.5	7

Location	Attack	Goals	Likelihood of successful attack	Likelihood of achieving goal	Attempt likelihood	Likelihood
	Spoof notifications	H,S	0.03	2	84.88	0.05%
	Hack email	D	7.3	2	86.78	12.67%
	SIM-Jacking	D	8	2	86.78	13.88%
	Malware	D,A,BN	8.765	8.5	97.50	72.64%
	Spoof device	BH,G	0.03	1	57.81	0.02%
User device	Sniff traffic	BH,G	0.03	2	57.81	0.03%
	Steal from patient	T	3	10	79.13	23.74%
Patient	Social engineering	D,M	7.5	7	95.76	50.27%
	Hide	T	9	2	79.13	14.24%
	Break	T	9	2	79.13	14.24%
	Pretend broken	T	2	1	79.13	1.58%
	Remove chip	D	3	6	86.78	15.62%
	Rewrite firmware	BN	2	1	69.94	1.40%
	Spoof	BH,G	0.03	7	57.81	0.12%
Anklet	Sniff	BH,D,G	0.03	6	94.42	0.17%
	Hide	T	9	2	79.13	14.24%
	Break	T	9	2	79.13	14.24%
	Pretend broken	T	2	1	79.13	1.58%
	DoS	H	2	2	55.52	2.22%
	Rewrite firmware	BN	2	1	69.94	1.40%
	Spoof device	BH,G	0.03	7	57.81	0.12%
	Sniff	BH,G	0.03	6	57.81	0.10%
	Trojan	BN	0.0015	10	69.94	0.01%
STEL	Spoof fake data	H,S	9	7	84.88	53.47%
	DoS	S	4.625	3	66.01	9.16%
	Childrens data breach	S	1	1	66.01	0.66%
	Social Engineering	M	1	8	67.93	5.43%
	Trojan	C	0.5	8	67.93	2.72%
	Spoof	BH,C,G	0.03	8	86.47	0.21%
AWS	Sniff	BH,B,G	0.03	8	94.42	0.23%
	Sniff	E	0.03	8	54.75	0.13%
	Trojan	C	8.765	8	67.93	47.63%
Developer Machine	Access Account	A,BN,C,D,E,M,S,R	7.3	10	99.99	72.99%
Developer	Social Engineering	A,BN,C	7.5	9	93.93	63.40%
	Steal device	T	5	10	79.13	39.56%
	Make work difficult	R	6	8	67.78	32.54%
Employee	Social engineering	E,M,R	7.5	9	95.33	64.35%
	Hack account	R	7.3	8	67.78	39.59%
	Forge sell data	S	0.03	5	66.01	0.10%
Office Machine	Modify packets	M	0.03	2	67.93	0.04%
	DoS	H,S	4.625	2	84.88	7.85%
	MaS	C	0.5	7	67.93	2.38%
	Crack passwords	BH,G	7.3	10	57.81	42.20%
	Injection	A,BH,BN,C,D,E,G,S,R	2	9	99.98	18.00%
UI	Worm	A,C	0.5	5	79.80	1.99%
Outsider Device	Frame employee	R	3	9	67.78	18.30%
Outsider	Slander	S,R	1	9	89.05	8.01%
	Steal hardware	T	4	10	79.13	31.65%
Doctor	Social engineering	D,T	7.5	9	97.24	65.64%

Figure 7: Overall assessment of Likelihood of attacks

engineering attack can succeed up to 75% of the time.

Patient	Likelihood of successful attack	Likelihood of achieving goal
Steal from patient	3	10

Social engineering [1]	7.5	7

STEL	Likelihood of successful attack	Likelihood of achieving goal
Hide	9	2
Break	9	2
Pretend broken	2	1
DoS	2	2
Rewrite firmware	2	1
Spoof device[6]	0.03	7
Sniff [6]	0.03	6
Trojan [3][6]	0.0015	10
Spoof fake data	9	7

Trojans are given 0.0015 to combine the fact that the antivirus on STEL does not need human approval, and that the trojan update must somehow crack the encryption of the communication leading to a tiny likelihood.

AWS	Likelihood of successful attack	Likelihood of achieving goal
DoS [7]	4.625	3
Childrens data breach	1	1
Social Engineering	1	8
Trojan [3]	0.5	8
Spoof [6]	0.03	8
Sniff [6]	0.03	8

Calculation of Final Likelihood

Now we can combine all of them. This is done by simply multiplying them all together as probabilities (0-1) and we get our final likelihoods as shown in Figure 7.

4.2.3 Impact Assessment

Impact is calculated as one number between 0-10 for each goal. Table 4 displays the rules used for calculating impact. Below are the impacts for each goal. From here we calculate the impact for each event using their associated goals' impacts. This is usually the max of the the

associated goals' impacts, however if deemed necessary, the impact of an event can be raised even higher due to the combined effect of multiple outcomes happening per event.The impacts of each event is seen in Figure 8.

4.2.4 Final Assessment Results

The likelihoods and impacts are then scored by multiplying them on a range of 0-100. Figure 9 displays the score table and scores are graphed out in Figure 10.

Heat Map Analysis

Heat maps serve as invaluable tools in risk assessment analysis, providing a visual representation of complex data that enhances comprehension and decision-making. In risk assessment, where diverse factors contribute to the overall risk landscape, heat maps offer a succinct and intuitive way to highlight critical information.

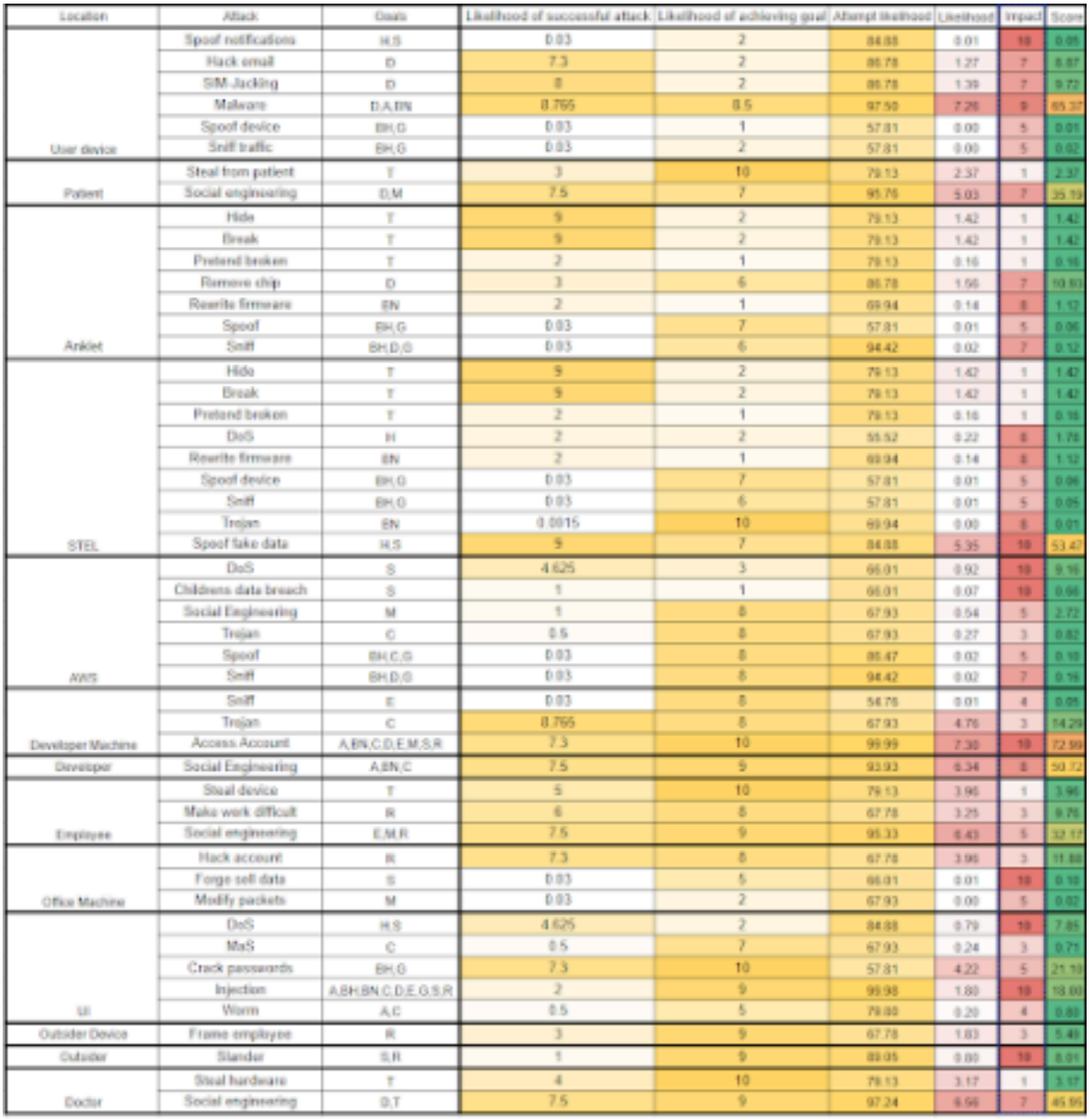
Goal	Symbol	Component Motivations	Likelihood	Impact
Grey-hat	G	-	11	5
Activism	A	P	37	4
Black-hat	BH	I,A	52.6	5
Corporate espionage	E	C,W	54.76	4
Harm user	H	I,W	55.52	8
Corporate sabotage	S	C,W,A	66.008	10
Terminate employee	R	I,C,A	67.784	3
Steal Compute Recources	C	R,I	67.93	3
Extract Money	M	R,I	67.93	5
Botnet	BN	I,P,W	69.9448	8
Hardware theft	T	R,I,C	79.1282	1
Data disclocure	D	R,I,P,W	86.777432	7

Figure 8: Impacts for each Attack goal

Impact score	Description
0	No effect Attack either effects the company in no way or is beneficial to the company
1	Unnoticeable effect Has an effect, but will likely be unnoticed
2	Negligible effect Can effectively be ignored
3	Minor effect Employees may be subconsciously aware and affected parties aware
4	Notable effect Company is mostly aware of incident
5	Moderate effect Small section of the public is made aware
6	Substantial effect A large portion of the public is aware
7	Major effect Most of the public is aware and event is

	picked up by major news
8	Permanent effect Lasting consequences on company ranging from legal issues to major internal changes
9	Catastrophic effect Company survives, but will likely never fully recover
10	Terminal effect Company is annihilated. No recovery of any amount possible

Table 4: Impact Assessment Rules



Location	Attack	Goals	Likelihood of successful attack	Likelihood of achieving goal	Attempt likelihood	Likelihood	Impact	Score
User device	Spoof notifications	H,S	0.03	2	84.88	0.01	10	0.05
	Hack email	D	7.3	2	86.78	1.27	7	8.87
	SIM Jacking	D	8	2	86.78	1.39	7	9.72
	Malware	D,A,BN	8.765	8.5	97.50	7.26	9	65.37
	Spoof device	BH,G	0.03	1	57.81	0.00	5	0.01
	Sniff traffic	BH,G	0.03	2	57.81	0.00	5	0.02
Patient	Steal from patient	T	3	10	79.13	2.37	1	2.37
	Social engineering	D,M	7.5	7	95.76	5.03	7	35.19
Anklet	Hide	T	9	2	79.13	1.42	1	1.42
	Break	T	9	2	79.13	1.42	1	1.42
	Pretend broken	T	2	1	79.13	0.16	1	0.16
	Remove chip	D	3	6	86.78	1.56	7	10.93
	Rewrite firmware	BN	2	1	69.94	0.14	8	1.12
	Spoof	BH,G	0.03	7	57.81	0.01	5	0.06
	Sniff	BH,D,G	0.03	6	94.42	0.02	7	0.12
STEL	Hide	T	9	2	79.13	1.42	1	1.42
	Break	T	9	2	79.13	1.42	1	1.42
	Pretend broken	T	2	1	79.13	0.16	1	0.16
	DoS	H	2	2	55.52	0.22	8	1.78
	Rewrite firmware	BN	2	1	69.94	0.14	8	1.12
	Spoof device	BH,G	0.03	7	57.81	0.01	5	0.06
	Sniff	BH,G	0.03	6	57.81	0.01	5	0.05
	Trojan	BN	0.0015	10	69.94	0.00	8	0.01
	Spoof fake data	H,S	9	7	84.88	5.35	10	53.47
AWS	DoS	S	4.625	3	66.01	0.92	10	9.16
	Childrens data breach	S	1	1	66.01	0.07	10	0.66
	Social Engineering	M	1	8	67.93	0.54	5	2.72
	Trojan	C	0.5	8	67.93	0.27	3	0.82
	Spoof	BH,C,G	0.03	8	86.47	0.02	5	0.10
	Sniff	BH,D,G	0.03	8	94.42	0.02	7	0.16
Developer Machine	Sniff	E	0.03	8	58.76	0.01	4	0.05
	Trojan	C	8.765	8	67.93	4.76	3	14.29
	Access Account	A,BN,C,D,E,M,S,R	7.3	10	99.99	7.30	10	72.99
Developer	Social Engineering	A,BN,C	7.5	9	93.93	6.34	8	50.72
Employee	Steal device	T	5	10	79.13	3.96	1	3.96
	Make work difficult	R	6	8	67.78	3.25	3	9.76
	Social engineering	E,M,R	7.5	9	95.33	6.43	5	32.17
Office Machine	Hack account	R	7.3	8	67.78	3.96	3	11.88
	Forge sell data	S	0.03	5	66.01	0.01	10	0.10
	Modify packets	M	0.03	2	67.93	0.00	5	0.02
UI	DoS	H,S	4.625	2	84.88	0.79	10	7.85
	MaS	C	0.5	7	67.93	0.24	3	0.71
	Crack passwords	BH,G	7.3	10	57.81	4.22	5	21.10
	Injection	A,BH,BN,C,D,E,G,S,R	2	9	99.98	1.80	10	18.00
	Worm	A,C	0.5	5	79.80	0.20	4	0.80
Outsider Device	Frame employee	R	3	9	67.78	1.83	3	5.49
Outsider	Slander	S,R	1	9	89.95	0.80	10	8.01
Doctor	Steal hardware	T	4	10	79.13	3.17	1	3.17
	Social engineering	D,T	7.5	9	97.24	6.56	7	45.95

Figure 9: Complete Risk Assessment of the Bodiguide system

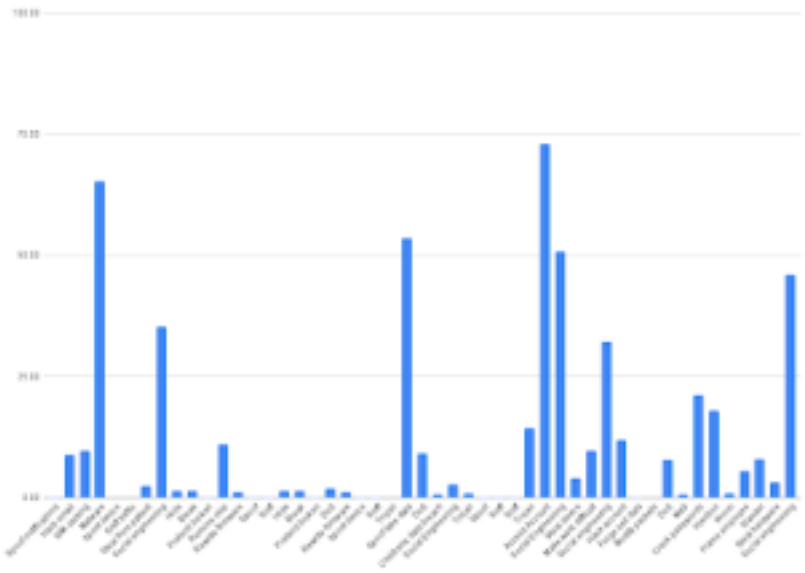


Figure 10: Complete Risk Assessment of the Bodiguide system Graphed out

By color-coding data points based on their significance, heat maps allow for quick identifica tion of high-risk areas, enabling stakeholders to prioritize and allocate resources effectively. The visual clarity provided by heat maps aids in understanding the interplay between likelihood and impact, fostering a more informed and strategic approach to risk mitigation. Additionally, heat maps facilitate communication by presenting intricate risk scenarios in an accessible format, fostering collaboration among team members and stakeholders. This visual representation not only simplifies the interpretation of complex risk data but also empowers decision-makers to focus on the most critical areas, ultimately enhancing the overall risk management process. The heat map seen in Figure:11 and the table: 12, can be used as references to look at the major threats the solution would face.

Recommendations for the major 8 threats

Let us now recommend actions and explain in more detail each of these major threats. User Device Malware

– This is if a user's device gets infected with malware. The impact is high at 9 as there is a risk of data being breached and the user's device being added to some kind of botnet. The company being associated with user devices getting infected could end very badly if it is found that our system is what infected them.The likelihood of this attack is also relatively high at 7.26. Since users often ignore their antivirus and there is a lot of motivation for infecting a user with malware, the chances of this happening are higher than one may expect.

– A good course of action would be to encrypt data stored locally on the user's system to make it harder for user data to be stolen by malware. Another defense would be to have an antivirus scan updates for trojans in the case of an insider attack. It is also recommended to remind users to use and trust an antivirus, even if it is just windows defender.

Patient Social Engineering

– This is if an attacker employs phishing to get patient data or payment data from the patient. The impact of this is a 7. It is not too high as this event does not affect the company directly very much. However, this event can severely affect the reputation of

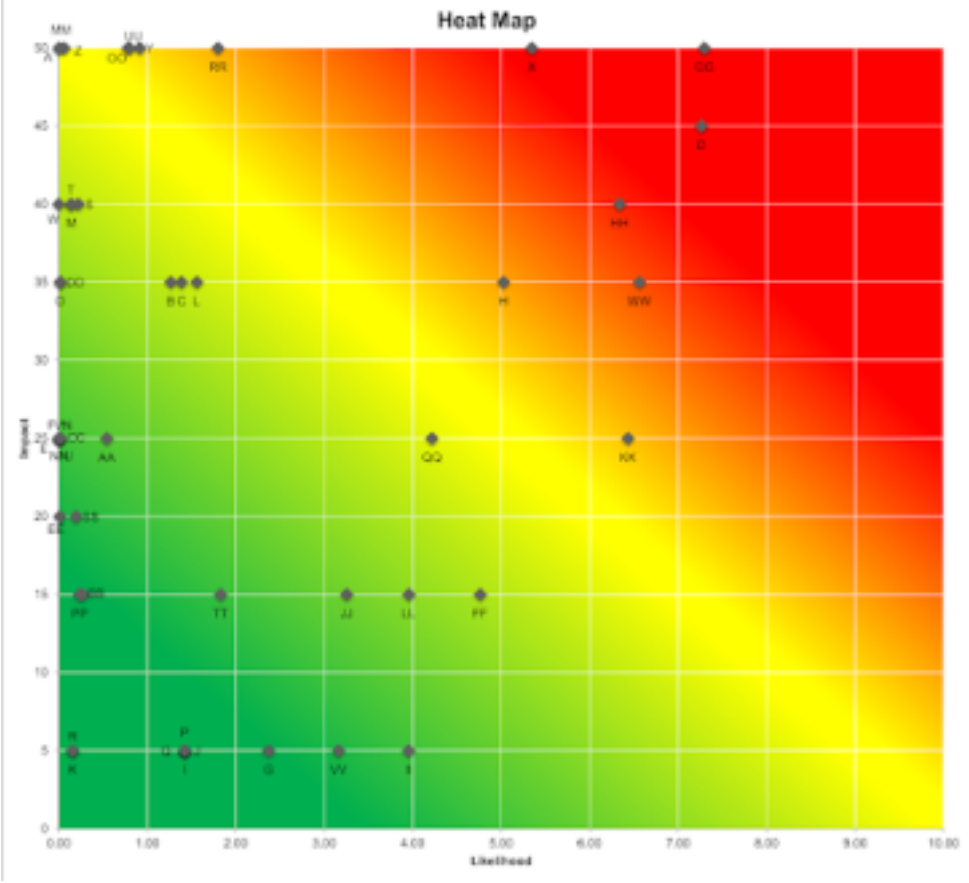


Figure 11: Major threats pointed out in the Heat Map

Location	Attack	Symbol	Likelihood	Impact	Score
User Device	Malware	D	7.26	9	65.37
Patient	Social engineering	H	5.03	7	35.19
STEL	Spoof fake data	X	5.35	10	53.47
Developer Machine	Access Account	GG	7.30	10	72.99
Developer	Social Engineering	HH	6.34	8	50.72
Employee	Social engineering	KK	6.43	5	32.17
UI	Injection	RR	1.80	10	18.00
Doctor	Social engineering	WW	6.56	7	45.95

Figure 12: Table explaining the major 8 threats

the company if attackers find it easy to social engineer the users off this system and cost the company current users. The likelihood is 5.03, which is not very high. This is due to the medium high success rate of a social engineering attack and the medium high rate at social engineering leading to the attacker's goal combining to make a medium likelihood. The attempt rate will be high due to this leading to 2 highly motivated goals, but this is reliant on the patient giving accurate details.

– A good course of action is to set up a strict mode of communication with the patients. Let

them know that we will never communicate with them outside of this method and to not trust any communications from us from other sources. For example, saying we will only communicate via email and app notifications; furthermore, we will only send messages from the official BodiGuide account and bodiguide@example.com email.

Spoofing Fake STEL Data

– The next attack is Spoofing fake data to the STEL device. While artificially creating and sending fake data would be nearly impossible, it would be quite easy for an attacker to either just wear the anklet themself or convince the user to switch how they wear the anklet. The impact of this attack is a 10. The associated goals are corporate sabotage and harming users. Both of these can lead to catastrophic and even potentially doomsday outcomes for the company. False readings could not only lead to users making poor health decisions, but also tank the company's reputation. The likelihood of this is only 5.35. The only reason this is not a tiny number is because if a loved one or roomate of the user was the attacker, they may easily be able to steal the anklet at night to have it send their readings, tamper with the anklet, or convince the user to tamper with it.

– A good course of action would be to give users clear instructions to not tamper with the anklet, and to set up some mechanism to make it difficult to remove without the user's knowledge .

Accessing Developer/Admin Accounts

– This is the event with the highest score at 72.99. The impact could be catastrophic to doomsday at a 10 since the attacker could do nearly anything to the system with admin privilege and it may be very difficult to remedy once it occurs. The likelihood is also high due to the extremely high demand for such an attack and the ease of cracking most passwords.

– A good course of action is to make sure the admin account has a very strong password that is changed regularly and maybe even only has limited uses per change. A redundant admin account may help remedy this event if it occurs. App-based multi-factor authentication is also highly recommended. Other variations of multifactor such as phone and email are susceptible to attacks like SIM-jacking and password cracking.

Social Engineering the Developer/Admin

– This is less of phishing for their password and more of convincing them to do something. The impact (8) of this is lesser than accessing the account due to the fact that you have to sneak your attack past the developer/admin. The likelihood is also lesser at 6.34 due to the slightly lower demand and lower chance of achieving the goal with this route. This attack may manifest itself as the attacker impersonating upper management or another developer/admin.

– A good course of action is to have admins trained on social engineering and to use a ticketing system for requests to the admin to eliminate the human communication. Restrict

the official requests with the admin to predefined text options when possible and set it up so the admin must initiate contact with the requestor if contact by phone or email is necessary.

Social Engineering an Employee

– This is a more corporate attack. The motivations for this are extracting money, getting an employee fired, or performing corporate espionage. The impact is comparatively small to the other attacks mentioned at 5 as these goals can hurt the company, they should be fairly easy to recover from and the public will likely not care much about these sorts of attacks. The danger of this attack comes from the likelihood being 6.43. This is mainly due to the ease of such an attack and the surprisingly high interest at 95.33/100. The main issue with this attack is that it is a moderate sized attack that can be carried out easily,

– A good course of action is to train employees on basic cybersecurity, and to have a rigorous system for investigating employee complaints in the case of an attacker trying to get an employee to quit. Requiring card or passkey access to physical offices is another good way to prevent attackers from impersonating employees, third-parties, or contractors in person.

Code Injection through UI

– This is the event with the lowest score of the notable events. This is largely due to the low likelihood of this event. The danger is that the impact of this event is a 10. Code injections are powerful, effective, and in high demand. The only thing holding them back is that newer systems, like ours, are quite resistant to this sort of attack. A code injection can accomplish almost anything an admin can as you can use some code injections to give yourself admin privileges.

– The low likelihood and current state of security against this attack in our system means there are no changes or actions needed at the moment; however, with the high demand, effectiveness, and impact of this threat; it is important to keep an eye out for new code injections being discovered and to maintain a development mindset of separating data and code, while also checking buffer and input sizes.

Social Engineering Doctors

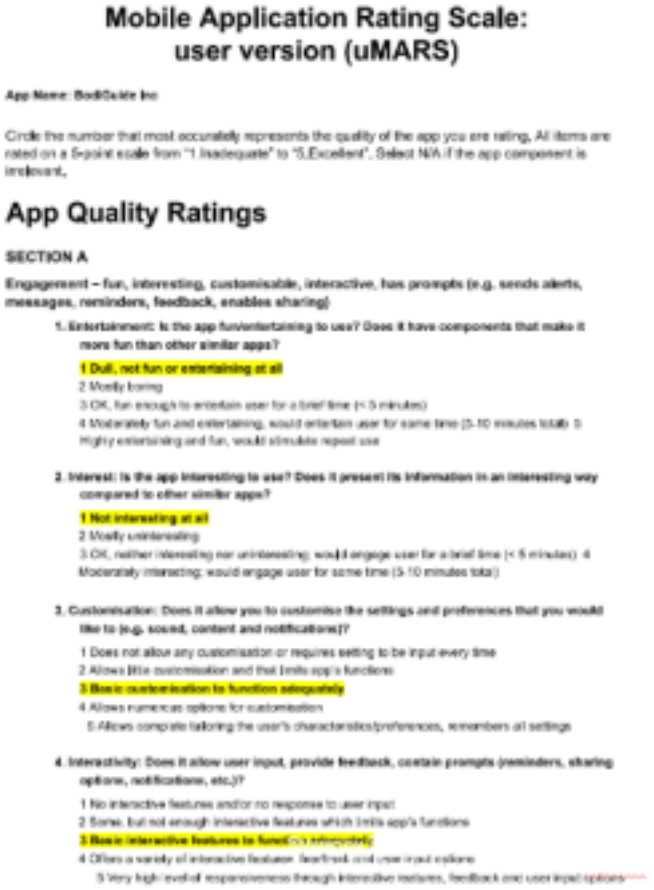
– The final event of interest is social engineering doctors. This is mainly for getting patient data from them, but can also be used to attempt to steal hardware from them. The impact is 7 due to the potential for patient data to be leaked, while the theft of hardware will have a negligible effect on the company. The likelihood is moderately high at 6.56 due to the relatively high interest in such an attack and the ease of such an attack.

– A good course of action is to let doctors know to not speak about patient data to others. One good step would be to make the patient data HIPAA protected. This will give legal obligation to the doctors to not share patient data.Make the doctors aware that they are responsible for the theft, intentional damage, and loss of their hardware. This will shift the impact of hardware theft off the company.

5 Usability Testing

Usability testing is essential because usability testing offers firsthand information on how actual users interact with a system or product. This testing determines how well users can accomplish their goals, how naturally the interface directs them, and where they could run into problems or become confused. Through identification of these problems, developers and designers may make

well-informed changes to enhance the user experience. Usability testing also ensures that the product fulfills the requirements and expectations of the users, which increases user engagement and happiness. It's an essential stage in developing an accessible, effective, and user-friendly device, which will eventually help the product succeed and keep users. To conduct comprehensive usability testing, we employed two distinct methodologies.



Mobile Application Rating Scale: user version (uMARS)

App Name: BodiGuide Inc

Circle the number that most accurately represents the quality of the app you are rating. All items are rated on a 5-point scale from "1.Inadequate" to "5.Excellent". Select N/A if the app component is irrelevant.

App Quality Ratings

SECTION A

Engagement – fun, interesting, customisable, interactive, has prompts (e.g. sends alerts, messages, reminders, feedback, enables sharing)

1. **Entertainment: Is the app fun/entertaining to use? Does it have components that make it more fun than other similar apps?**
   1 Dull, not fun or entertaining at all
   2 Mostly boring
   3 OK, fun enough to entertain user for a brief time (< 5 minutes)
   4 Moderately fun and entertaining, would entertain user for some time (5-10 minutes total) 5 Highly entertaining and fun, would stimulate repeat use

2. **Interest: Is the app interesting to use? Does it present its information in an interesting way compared to other similar apps?**
   1 Not interesting at all
   2 Mostly uninteresting
   3 OK, neither interesting nor uninteresting; would engage user for a brief time (< 5 minutes) 4 Moderately interesting; would engage user for some time (5-10 minutes total)

3. **Customisation: Does it allow you to customise the settings and preferences that you would like to (e.g. sound, content and notifications)?**
   1 Does not allow any customisation or requires setting to be input every time
   2 Allows little customisation and that limits app's functions
   3 Basic customisation to function adequately
   4 Allows numerous options for customisation
   5 Allows complete tailoring the user's characteristics/preferences, remembers all settings

4. **Interactivity: Does it allow user input, provide feedback, contain prompts (reminders, sharing options, notifications, etc.)?**
   1 No interactive features and/or no response to user input
   2 Some, but not enough interactive features which limits app's functions
   3 Basic interactive features to function adequately
   4 Offers a variety of interactive features (feedback and user input options)
   5 Very high level of responsiveness through interactive features, feedback and user input options

Figure 13: User version of the Mobile App Rating Scale

Dimension	Scores	Average Score
Engagement	1, 1, 3, 3, 4	2.4
Functionality	3, 5, 4, 3	3.75
Aesthetics	5, 5, 3	4.33
Information	3, 2, 4, 5	3.5
Overall		**3.4958**
Converted to 100-point scale		**87.4**

Figure 14: Score from the uMARS survey

- User Interface Checklist

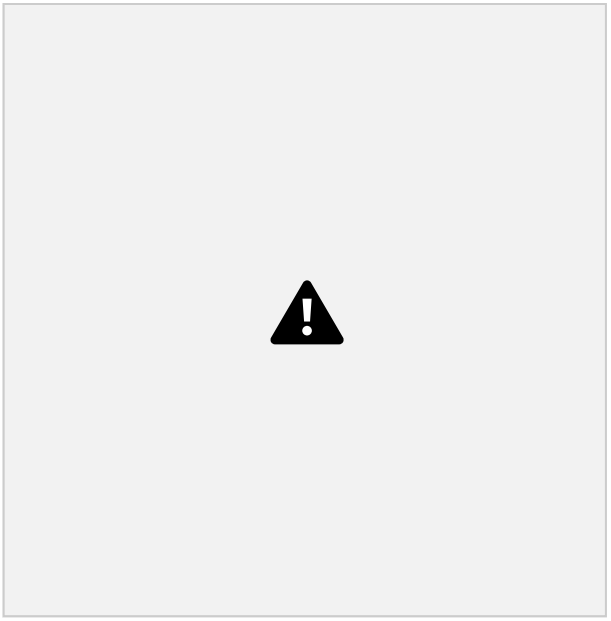


Figure 15: User Interface checklist

– We utilized a detailed interface checklist, as seen in Figure: 15, meticulously assessing every aspect of the UI, including interactions, visual elements, navigation, clicks, scrolls, and more. This ensured a thorough evaluation of the user interface's functionality and design. In the initial assessment, the app's user interface successfully met the established testing benchmarks except for the login and registration components, which span both the client and server sides. Following the integration and successful activation of the login and registration APIs, the interface underwent a further review to validate its functionality and was thusly cleared on those tests.

• uMARS: User Version of Mobile App Rating Scale

– We, then, implemented the renowned Mobile App Rating Scale, as seen in Figure: 13, a leading evaluative tool developed by Stoyanov et al. in 2015. This scale is specifically designed to assess the quality of health mobile and web applications. Its widespread cita tion and robust framework make it the most reliable tool currently available for evaluating health applications, providing us with a deep understanding of the app's usability in the healthcare context. We used the version of the scale that has been adapted for users, known as the user version of the Mobile App Rating Scale (2016). The Mobile App Rating Scale (MARS) for users assesses apps using four concrete dimensions (Engagement, Func tionality, Aesthetics, Information Quality), one subjective dimension, and App-Specific Characteristics. In our initial usability test, we focused on the concrete dimensions, ex cluding Subjective Quality and App-Specific Characteristics as they were not relevant at this stage. The testing process involved users interacting with the app for 10 minutes, followed by completing the uMARS survey. The scores, as seen in Figure: 14, were av eraged and converted to a 100-point scale, resulting in a promising initial score of 87.4. Strengths were noted in Aesthetics, attributed to the app's intuitive gestural design and visual appeal, while Engagement was identified as an area for improvement due to the current minimalistic feature set.

6 Conclusion and Future Work

In concluding our current course project phase, we recognize the strides made in developing a robust remote monitoring system for cardiovascular health. As we look ahead, the identified future works serve as a road-map for advancing the capabilities, user experience, and security of our solution. The foundation laid for the remote monitoring system is robust and promising. However, there are exciting avenues for future development and enhancement across various dimensions of the project.

- Data Enhancement: Future efforts should focus on further enriching the data processing capabilities. This involves exploring advanced anomaly detection techniques beyond null data, potentially incorporating machine learning models for predictive analytics. Addi tionally, the integration of real-time data streaming technologies can enable more dynamic and responsive health monitoring.

- UI Refinement: The user interface is a dynamic aspect of any remote monitoring system. Future works in UI design should explore adaptive and personalized interfaces, tailoring the presentation of health data based on individual user preferences. Incorporating user feedback and conducting usability studies will continue to contribute to an interface that resonates with users, ensuring a positive and engaging experience. The next steps include using the Eyetracking technology with GazeRecorder, adding more features as well as elements to increase the Engagement quality of the UI.

- Expanded Functionality: Continued development in functionality could involve ex panding the range of health anomalies detected and notified to users. This might include incorporating additional physiological metrics or integrating with other wearable devices to provide a more holistic health picture. Furthermore, exploring features that enhance user engagement beyond notifications, such as interactive health insights and personalized health recommendations, can be considered.

- Risk Mitigation Strategies: Future work in risk assessment should involve the re finement of risk mitigation strategies. This may include the development of automated responses to identified risks, reducing the reliance on manual interventions. Continuous monitoring of potential threats and proactive measures to address emerging risks will be crucial in maintaining the system's integrity and security.

- Scaling and Performance Optimization: Scalability remains a key consideration for the future. Optimization of the Health Anomaly Detection Algorithm for efficiency and resource utilization will be essential as user numbers grow. Additionally, exploring cloud native technologies beyond AWS, such as serverless architectures, can contribute to en hanced scalability and cost-effectiveness.

- AWS Security Evolution: As AWS evolves, future works should adapt security mea sures accordingly. Regular updates to AWS services and features, along with ongoing training for system administrators, will ensure the most effective use of AWS security tools. Exploring additional AWS security features and staying abreast of industry best practices will contribute to a resilient and well-protected system.

In summary, the future works for our remote monitoring system span multiple facets, from data processing and user experience to enhanced functionality, risk mitigation, scalability, and security evolution. These endeavors aim to continually elevate the effectiveness, user satisfaction, and security posture of our cardiovascular health monitoring solution.

References

[1] ”BodiGuide Inc”. Website: https://www.bodiguide.com/. Last visited: Dec 14th 2023.

[2] Pescosolido, R. Berta, L. Scalise, G. M. Revel, A. De Gloria and G. Orlandi, ”An IoT-inspired cloud-based web service architecture for e-Health applications,” 2016 IEEE International Smart Cities Conference (ISC2), Trento, Italy, 2016, pp. 1-4, doi: 10.1109/ISC2.2016.7580759.

[3] T. N. Gia, M. Jiang, A. -M. Rahmani, T. Westerlund, P. Liljeberg and H. Tenhunen, ”Fog Computing in Healthcare Internet of Things: A Case Study on ECG Feature Extraction,” 2015 IEEE International Conference on Computer and Information Technology; Ubiqui tous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, Liverpool, UK, 2015, pp. 356-363, doi: 10.1109/C IT/IUCC/DASC/PICOM.2015.51.

[4] M. Singh, M. A. Rajan, V. L. Shivraj and P. Balamuralidhar, ”Secure MQTT for Internet of Things (IoT),” 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 2015, pp. 746-751, doi: 10.1109/CSNT.2015.16.

[5] ”Stel Life”. Website: https://www.stel.life/. Last visited: Dec 14th 2023.

[6] Stoyanov SR, Hides L, Kavanagh DJ, Wilson H ”Development and Validation of the User Version of the Mobile Application Rating Scale (uMARS)” JMIR Mhealth Uhealth 2016;4(2):e72 doi: 10.2196/mhealth.5849

[7] ”Why Social Engineering works”. Website: https://purplesec.us/learn/why-social engineering-works/. Last visited: Dec 14th 2023.

[8] ”What is SIM Attack and Why Fast Detection is important”. Website: https://www.incognia.com/the-authentication-reference/what-is-sim-swap-attack-and why-fast-detection-is-important. Last visited: Dec 14th 2023.

[9] ”Microsoft Windows Defender Security Center”. Website: https://www.pcmag.com/reviews/microsoft-windows-defender-security-center. Last visited: Dec 14th 2023.

[10] ”Why people ignore security alerts”. Website: https://news.sophos.com/en us/2016/08/19/why-people-ignore-security-alerts-up-to-87-of-the-time/. Last visited: Dec 14th 2023.

[11] ”Three quarters of the most popular passwords can be cracked instantly”. Web site: https://cybernews.com/security/three-quarters-of-the-most-popular-passwords-can be-cracked-instantly.Last visited: Dec 14th 2023.

[12] ”What are the odds of an RSA Private key collision?”. Website: https://security.stackexchange.com/questions/70693/what-are-the-odds-of-an-rsa-private key-collision. Last visited: Dec 14th 2023.

[13] T. Sommestad, H. Holm and M. Ekstedt, ”Estimates of Success Rates of Denial-of-Service Attacks,” 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, China, 2011, pp. 21-28, doi: 10.1109/Trust Com.2011.7.