BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI
WORK-INTEGRATED LEARNING PROGRAMMES DIVISION

SEMESTER 3
2022-2024

SESAP ZG566
Secure Software Engineering

Assignment

Submitted by

2022MT93172 - PAVITHRA.S

Contents

Question 1

Suggest few primary parameters which need to be considered before re-structuring SDLC for the product to implement (Design an efficient methodology or life cycle to implement health monitoring system) & Design a Flow diagram or Data Flow Diagram which senses hearth attach and communicate securely to Doctors and Guardians.

Answer:

In today's world, technology is playing a very important role in our day-to-day life and has become an important part. It is useful in various ways including keeping track of our health. A health monitoring system will be very useful to detect any issues at an earlier point and get the best care as soon as possible.

Existing Health Monitoring System

The existing health monitoring systems provide several features such as,

- **Vital sign monitoring** – Vital signs such as heart rate, body temperature, blood pressure, and oxygen level can be monitored. These data will help the doctors understand the patient's condition.
- **ECG and EKG monitoring** – Using the electro cardiogram measurements, the doctors can understand irregular heart rhythms and diagnose heart conditions.
- **Activity tracking** – With the help of accelerometers and gyroscope sensors, the devices can keep track of physical activity such as the number of steps taken, distance travelled and calories burned. This is mainly found in fitness trackers and smartwatches.
- **Sleep tracking** – The duration and the quality of the sleep can be monitoring to understand the overall sleep health.
- **Medication reminders** – Some health systems provide mobile apps that can be useful for the patients to track and view their data. Medication reminder features are also available to alert the user when a medicine is to be taken.

Limitations of Existing System

Even though we have these features, there is still scope for more and the health monitoring system can be improved. There are several limitations too.

Some of the limitations of the current health monitoring system are,

- **Lack of real-time monitoring** – Most of the health monitoring systems currently available process the data on a periodic basis and provide insights rather than real-time monitoring.
- **Limited predictive capability** – The current health monitoring systems focus on collecting the basic data and presenting them to the users to view. But they are not equipped to detect or predict any change in the data which can be crucial for saving lives. For example, change in the heart rate, if predicted early can be useful to detect heart attacks.
- **Limited data integration** – The health data is available in multiple sources from various systems and in different formats. But there is no proper integration between the data from these sources. The users will need to use multiple devices or platforms which can be highly inconvenient.
- **Privacy and security concerns** – The health data from people is private and needs to be protected. The health monitoring systems many not have the required security measures in place to safeguard and protect the health data. If the patient data is stolen, there could be severe consequences such as identity theft or misuse of medical info.
- **Cost and Investment** – The advanced health monitoring systems will involve higher investments to build. So, the cost of using the devices may be high and may not be affordable for all.

In our use case, we are considering a health monitoring system that will track the heart beat of the patient and analyse the data in order to help preventing heart attacks.

AI and Predictive Analysis Techniques

AI and predictive analysis techniques can be used in the health monitoring system for making the system more efficient and useful in identifying the heart attacks at the right time.

Some of the techniques that can be used are,

- **Anomaly detection** – A base line for normal heartbeat patterns can be established for a patient and any deviations from the baseline can trigger an alert.
- **Predictive analysis** – The AI algorithms can be trained on historical patient data that can be useful to identify any patterns or risk factors that can happen before a heart attack. This can be achieved by continuously analysing the real-time data from the heart sensor. Through predictive analysis, early warning signs can be provided.

- **Pattern recognition** – The AI algorithm can recognize the pattern and trends in the heart rate data. The specific pattern that occurred before a cardiac arrest can be detected.
- **Real-time monitoring and Alerts** – In the real-time, the system can analyse the heart rate data in real-time. If there is a trend that indicates a potential issue, a trigger can be set to alert the doctors for immediate action.

Heart Beat Tracking Methods

In order to track the heartbeat, multiple methods are available.

Some of the methods are,

- **Chest band devices** – The heart rate can be tracked using electrical detection. The electrical activity of the heart is detected through a band that is wrapped around the chest.
- **Wrist or forearm worn devices** - There are two major arteries in the forearm and wrist. The radial artery runs towards the thumb, and the ulnar artery runs towards the pinky and ring fingers. At the skin surface of the wrist and forearm, these two arteries provide plenty of blood. These wearables have light-emitting diodes (LEDs) and sensors that rest against the skin in that area. With the help of LED light, the sensor detects the tiny expansions of the blood vessels underneath the skin's surface.
- **Smart rings:** Smart rings are devices that are to be worn like a piece of jewellery on the fingers similar to a ring. They use optical detection to track the heart rate and other vital signs. These devices are new to the market and growing. So, limited data on their accuracy.
- **Pulse oximeters:** The pulse oximeter is like a clip that is worn on a finger. This device also uses the optical detection method. These track pulse rate and blood oxygen levels. It is widely used in the hospitals to get the data instantly.
- **Smartphones:** There are several apps that has the ability to measure the pulse rate. Some of the apps use the camera's flash to illuminate the blood vessels under our skin. The user is asked to hold their finger to the camera lens and with use optical detection the pulse rate is identified. Another way is to use the camera itself. The camera is pointed at the face to detect the pulse rate based on visible (but undetectable with your eyes) changes in the skin.

The accuracy of these devices commonly depends on the device's type of detection and the user’s activity while wearing the device.

Device	**Accuracy**
Chest-band devices	They are the most accurate when properly used. Since they measure the heart rate directly rather than the pulse rate, the accuracy level is high.
Wrist- or forearm-located wearables	These devices can be very useful and accurate while resting, walking, running, cycling or various exercise devices. But. The readings could be inaccurate if we are using arms for exercise activities.
Smart rings	They are new and not commercially available yet. More research to be done to understand it’s accuracy.
Pulse oximeters	They are useful for doctors. But, may not be suitable for exercise or other activities.
Smartphones	The phone and its camera are not designed for this purpose. The apps where the user have to touch the camera lens is more accurate than the face scan, but they are still prone to errors.

Proposed System

Based on the study done on the current limitations in the health monitoring system, AI and predictive analysis methods available and the methods to track the heartbeat, the new health monitoring system is going to be designed.

This proposed system considers solving the below limitations that are present in the existing health monitoring system,

- **Lack of real-time monitoring**

  Current systems track and send the data to the cloud for processing where the data is stored and maintained. In order to implement real time monitoring, we can make use of edge computing. Using edge technology, the data can be processed at the source point, near the edge of the network where the data is collected real time and alerts can be sent. Then, the data can be synced to the cloud. This would solve the lack of real-time monitoring problem.

- **Limited predictive capability**

  Based on the collected data, the patterns can be analysed and any anomaly in the data can be identified with the help of AI. This is where AI and predictive models will be useful. Once the data is synced to the cloud which will happen on periodic basis, the AI predictive analysis techniques such as anomaly detection and pattern recognition techniques can be utilized.

  This will enhance the predictive capability of the health monitoring system.

- **Limited data integration**

  The health-related data is currently stored and managed by different applications and platforms. The data formats are different, but at the core it all contains sensitive information of the users which needs to be stored safely and utilized with care. So, to securely save and use the data in a common format, blockchain technologies can be utilized.

  A patient records blockchain network can be created and shared only with the concerned apps based on user given permissions. Since the blockchain network is immutable and all transaction history are maintained, the data can be stored and managed securely. Multiple apps can fetch data and store the transactions to the blockchain network for effective data integration.

Capturing the Heart Rate

Since we are trying to monitor the heart rate on a continuous basis while the user is performing their day-to-day activities, having them connected to bigger devices for capturing the heart rate is not going to work. So, the aim is to use a device that the user is going to wear close to his body and also not affect the day-to-day activities.

So, using a smart watch like wearable device to capture the heart rate and other vital signs possible can be used. This will be easy to wear for the user and also the required data can be tracked. The device will have the required sensors to capture the data for processing.

Flow of the Proposed Heart Monitoring System

Below is the step-by-step flow of how the proposed system will work.

1. **Data Capture**

   The system starts with a wearable device. The smart watch like wearable includes a heart rate sensor which is now attached to the patient's body. This sensor continuously monitors the patient's heartbeat and tracks the data.

2. **Edge Computing with AI**

   The collected heart rate data is processed locally on the wearable device using edge computing technologies. The Edge AI technology is used to process the data and identify any anomaly or pattern in the heart rate. If anything is detected, the wearable device will show an alert to the user. The user will also be given the choice to dismiss the alert or share it with their emergency contact.

   This localized processing method will help reduce latency and conserves power while performing initial data preprocessing.

3. **Secure Data Transmission**

   After local processing, the data is transmitted to a secure network. This transmission is carried out using strong encryption to protect the integrity and confidentiality of the data during transit as the medical information of the users are to be maintained with high security.

4. **Cloud-Based Storage**

   The transmitted data will be securely stored in a cloud environment. This allows for scalability and accessibility from various locations. Cloud storage ensures that the data is readily available for AI analysis and generating alerts. The AI predictive models are used in the cloud to analyse the patient data and send alerts to the specified health professional.

5. **AI Predictive Analysis**

   In the cloud, the AI predictive models are used in the cloud to analyse the patient data. Advanced machine learning algorithms will be used to analyse the data in real-time to detect anomalies, irregular heartbeats, or patterns that may indicate a potential health issue.

6. **Anomaly Detection**

   If the AI analysis identifies any anomalies or significant deviations from the patient's baseline heart rate, an alert is generated to the specified health professional in charge. The system determines the severity of the anomaly and assesses whether it warrants immediate attention.

7. **Alert Notification**

   The generated alert is transmitted to the appropriate recipients, such as doctors or emergency contacts. The notification includes information about the detected anomaly and patient details for reference. This alert is sent to the mobile app that includes the patient and doctor interface.

8. **Blockchain Data Storage**

   To maintain the security and integrity of the medical data, the system will store the heart rate data in a blockchain network. Blockchain technology will ensure immutability and tamper resistance, making it a good choice for sensitive health information.

   It will also be easy for integration of data with multiple application through the common blockchain network for medical data and stored transactions.

9. **Compliance and Regulation**

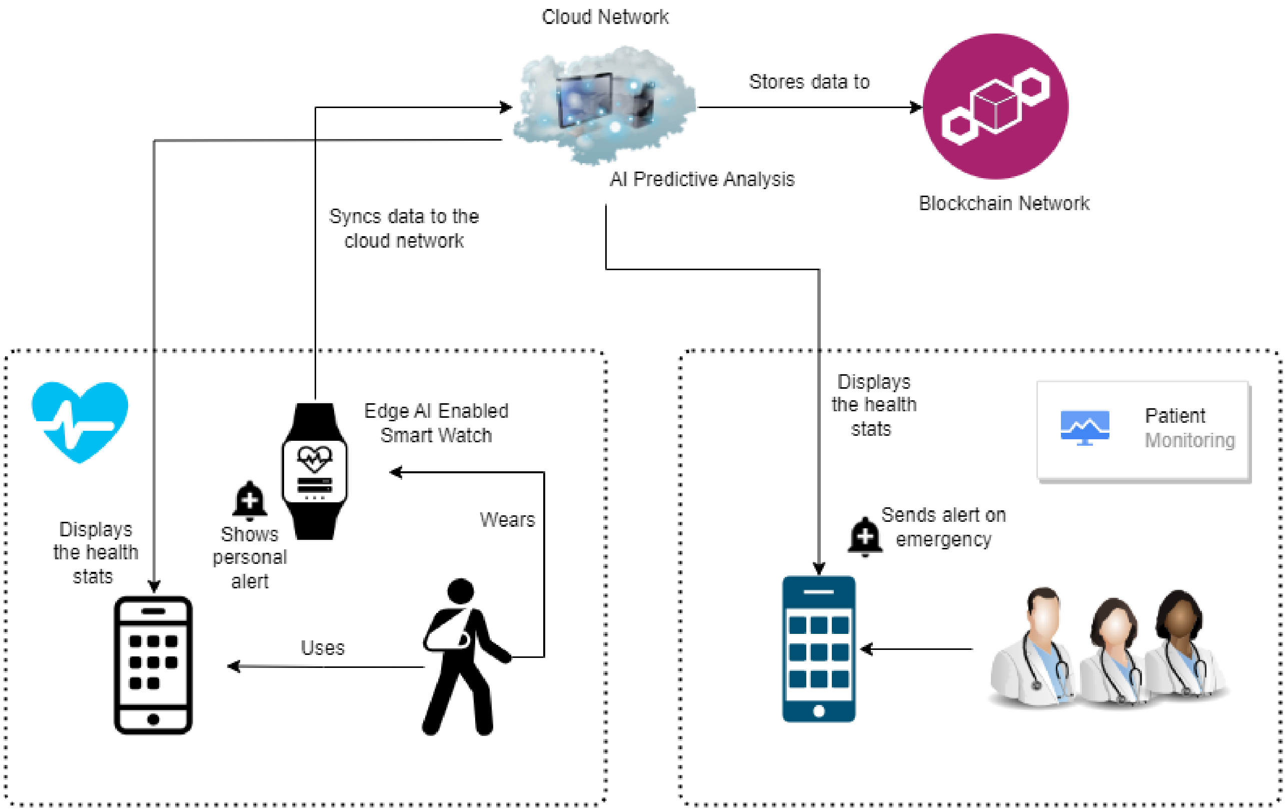
   The system is ensured to adhere to the healthcare regulations and standards, such as HIPAA or GDPR, to ensure the privacy and security of patient data.

10. **Regular Maintenance**

    The system will be maintained on a regular basis, including regular updates to the AI models, security patches, and monitoring for system health.

This proposed system is designed in such a way to provide continuous, accurate heart rate monitoring, early anomaly detection, and secure data storage, all while incorporating AI predictive analysis and blockchain technology to ensure the safety and integrity of the patient's medical data. It aims to improve the chances of early intervention in cases of potential heart-related issues and contribute to better patient outcomes.

Data Flow Diagram for Proposed System



The diagram shows the flow of data and events between the multiple components and users of the health monitoring system.

The user will be wearing the Edge AI enabled smart watch which will capture the heart rate information and process it using the Edge AI technologies. The processed data is securely transmitted to the cloud.

The mobile app will get the data from the could and display the stats to the users.

In the cloud, the data is processed using AI models to give alerts based on any anomaly to the emergency contacts or doctors.

The data from the cloud is then stored in the blockchain network for secure storage and integration with multiple systems.

Penetration points

Below are the attack points that an attacker could exploit and take advantage of.

1. **Data Transmission**

   Attack Point: The transmission of health data from the wearable device to the local gateway is a potential target. Attackers may attempt to intercept or manipulate data during this transmission.

   Mitigation: Implement secure and encrypted communication protocols (e.g., HTTPS) to protect data during transmission.

2. **AI Predictive Analysis Module**

   Attack Point: The AI module, responsible for predicting health issues, is a valuable target. Attackers may try to manipulate predictions or gain unauthorized access to sensitive algorithms.

   Mitigation: Implement strong authentication for the AI module, encrypt sensitive algorithms, and monitor for unusual patterns in access or usage.

3. **Blockchain Integration**

   Attack Point: The blockchain, while inherently secure, may be vulnerable to attacks if not properly configured. Smart contract vulnerabilities or unauthorized access could compromise data integrity.

   Mitigation: Ensure secure smart contract development, implement access controls, and regularly audit the blockchain network for potential vulnerabilities.

4. **Alert System**

   Attack Point: The alert system may be targeted to trigger false alarms or disrupt communication between the system and healthcare providers.

   Mitigation: Implement secure communication channels, use redundant alert systems, and monitor for unusual patterns in alert generation.

5. **Continuous Learning Mechanism**

   Attack Point: If the continuous learning mechanism is not secured, attackers may attempt to manipulate learning algorithms or introduce biased data.

   Mitigation: Regularly update and validate learning algorithms, monitor for anomalous patterns, and implement measures to detect and mitigate bias.

Question 2

List and explain all the software and hardware components needed with detailed explanation (Need to answer why specific Software/ Hardware needed) and Discuss challenges of mass production of this product.

Answer:

Hardware and Software Components

In order to build the proposed health monitoring system, various hardware and software components are required. The system includes a variety of components to come together and play along with the respective software's to function as per the requirements.

Hardware Requirements

1. **Wearable Device**

   Description: The wearable device, like a smartwatch or fitness tracker that are worn by the users to monitor their heart health continuously.

   Key Features:

   - Biometric Sensors:
     - Photoplethysmography (PPG) sensor for heart rate monitoring.
     - Electrocardiogram (ECG) sensor for detailed heart health analysis.
     - Blood pressure monitor sensor.
   - Microcontroller Unit (MCU):
     - Arm Cortex-M series MCU for sensor data processing.

   Connectivity: Built-in Bluetooth or other wireless technologies for communication with the local gateway.

2. **Edge Computing Module**

   Description: The edge computing module is responsible for immediate analysis, feature extraction, and data preprocessing.

   Key Features:

   - High-Performance Processor:
     - Intel Core i5 or higher for real-time analysis.
   - Memory:
     - Sufficient RAM for data processing (8GB or more).
   - Security Chip:
     - Dedicated security chip for encryption and secure processing.
   - Storage:

    - Solid State Drive (SSD) for quick data access.

3. **AI Predictive Analysis Hardware**

   Description: The AI predictive analysis hardware for performing AI data processing.

   Key Features:

   - Graphics Processing Unit (GPU):
     - NVIDIA GeForce or similar for running complex AI models.
   - Dedicated AI Accelerators:
     - Google Tensor Processing Units (TPUs) or similar.
   - Memory:
     - High-capacity RAM for handling model parameters.

4. **Blockchain Network Nodes**

   Description: The server hardware for the blockchain network nodes.

   Key Features:

   - Server or Node Hardware:
     - Enterprise-grade servers or dedicated devices for running blockchain nodes.
   - Storage:
     - High-capacity Hard Disk Drive (HDD) for data storage.
   - Network Interface:
     - Gigabit Ethernet or higher for fast communication.

5. **Security Considerations for Hardware Components**

   Description: The Security related considerations for the hardware of the health monitoring system.

   Key Features:

   - Hardware Security Modules (HSM):
     - Integrated into each device for secure key storage and cryptographic operations.
   - Secure Boot and Firmware Updates:
     - Ensure devices support secure boot processes and can receive firmware updates securely.
   - Biometric Authentication Hardware:
     - For enhanced user and system security.
   - Tamper Detection:
     - Implement sensors or mechanisms to detect physical tampering with devices.

Software Requirements

1. **Edge AI Software**
   - The Edge AI software is required for heart rate analysis with the AI model and associated algorithms.
   - These software components are designed in such a way run efficiently on the wearable device's hardware.
   - The AI model on the wearable device will perform real-time analysis of heart rate data, and detects any anomalies at an early stage. This will help in saving the patient at the right time.
   - It optimizes the resource usage by running on the device itself. As we are using Edge AI, the processing is done here itself and alerts are sent to the mobile app for the user.
   - Specific AI frameworks and libraries may be needed for model development and deployment.

2. **Data Preprocessing Software (Edge)**

   - The data preprocessing software is responsible for cleaning the data, filtering it, and normalizing incoming heart rate data before it is passed to the AI mode for processing.
   - It makes sure that the data is in a suitable format for AI analysis and reduces the noise in the signals.
   - This helps in improving the overall accuracy of heart rate monitoring and anomaly detection.

3. **End-to-End Encryption Software (Edge)**

   - Security software is needed to encrypt the data before transmitting it over the network. This is crucial for protecting the sensitive health information from being tampered or unauthorized access.
   - This software ensures the confidentiality and integrity of the data during transmission.
   - Encryption protocols such as TLS/SSL are typically used to make the data transmission more secure.

4. **Mobile App (Software)**

   - The mobile app serves as the user interface for the wearable device.
   - It connects to the wearable device and can receive alerts.
   - The mobile app provides a user-friendly interface for wearers to receive alerts and view heart rate data.
   - It enhances user engagement and accessibility.

5. **Cloud Services (Software)**

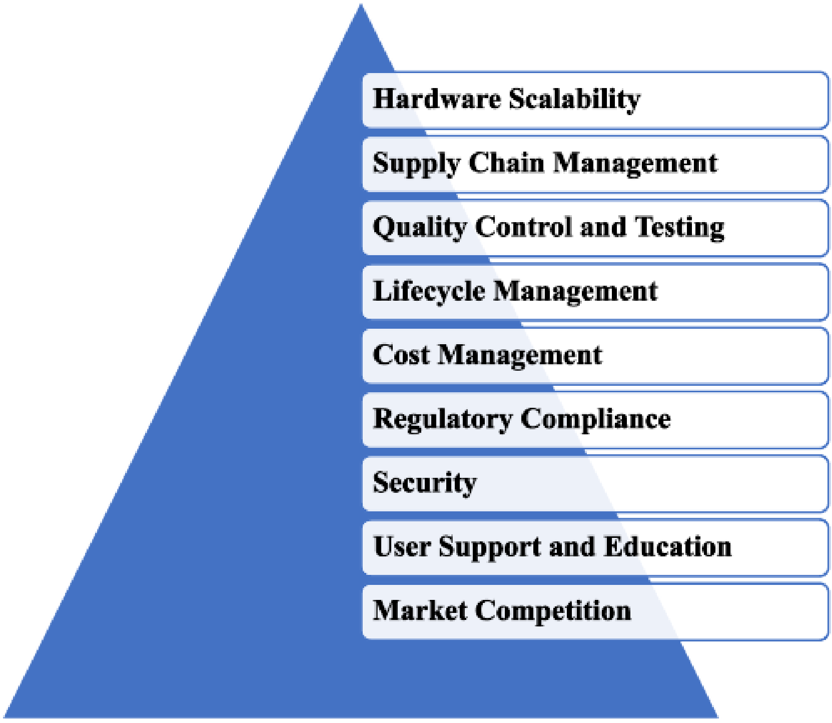
   - Cloud services include the AI analysis, storage, and data synchronization components.
   - These services run in the cloud and are responsible for long-term data storage, advanced AI analysis, and alert generation.
   - They provide scalability and accessibility while centralizing resource-intensive processing.

6. **Blockchain Software (Cloud)**

   - Blockchain software is used for secure and tamper-proof storage of patient's heart rate data.
   - It ensures data integrity and prevents unauthorized modifications.
   - Specific blockchain platforms, such as Hyperledger, can be used.
   - This can be useful to integrate data from and to different applications and platforms by having the ledger as the source of truth.

Challenges of Mass Production

Some of the challenges in mass producing the products are,



1. **Hardware Scalability**

   Challenge:

   To have a consistent and high-quality supply of wearable devices for mass production can be challenging. The variations in the hardware or firmware can lead to inconsistencies in performance.

   Details:

   - The sourcing components, manufacturing, and quality control must be carefully managed to keep the consistency intact.
   - In order to make sure that each unit meets the specified technical standards and operates seamlessly with other components, proper testing and quality control activities needs to be performed.

2. **Supply Chain Management**

   Challenge:

   Coordinating the supply chain for getting the wide range of diverse components, including sensors, microcontrollers, processors, and other specialized hardware, can be complex.

   Details:

   - Ensuring a stable supply chain for all components is crucial. Delays or shortages in any component can disrupt production schedules.
   - Managing suppliers, negotiating contracts, and securing long-term partnerships are essential for a smooth supply chain.

3. **Quality Control and Testing**

   Challenge:

   Ensuring the reliability and accuracy of each individual unit during mass production is a significant challenge.

   Details:

   - Implementing thorough quality control processes is essential to identify and rectify defects.
   - Rigorous testing, including functional, stress, and performance testing, is necessary to meet quality standards.
   - Any issues in the software need to be identified while testing itself as a human life will depend on the performance on this system.

4. **Lifecycle Management**

Challenge:

Managing the product lifecycle, including software updates, hardware upgrades, and end-of-life considerations.

Details:

- A proper strategy for the software/firmware updates needs to be put in place to address any security vulnerabilities that may arise and also introduce new features.
- We also need to plan for the eventual phasing out of older product versions and transitioning to the new iterations.
- The product will need continuous updates as per the customer needs and requirements.

5. Cost Management

Mass production requires cost-effective manufacturing processes to keep the product affordable for a broader audience. This includes,

- Optimizing hardware costs,
- Sourcing components efficiently, and
- Managing production overhead.

Challenge:

Balancing the costs associated with high-quality components, regulatory compliance, and production efficiency is a delicate task.

Details:

- Achieving profits while maintaining quality at the same time is a constant challenge.
- The fluctuations in the raw material prices, tariffs, and unexpected expenses can impact the overall cost structure.
- Since this is an advanced system, the cost of the product could be a little longer and may not be affordable for all.

6. Regulatory Compliance

Challenge:

Healthcare and data privacy regulations, such as HIPAA or GDPR, is crucial. Ensuring that the product complies with relevant standards adds complexity to mass production.

Details:

- We need to ensure that the product complies with regional and international standards for healthcare devices.
- Adapting to changes in regulations and obtaining necessary certifications can be time-consuming and resource-intensive.

7. **Security**

   Challenge:

   Managing the security of sensitive health data and ensuring user privacy poses unique challenges.

   Details:

   - As the system deals with sensitive health data, robust security measures must be in place to protect patient information and maintain the confidentiality of medical records.
   - Complying with data protection regulations and establishing transparent data handling practices also needs to be done.

8. **User Support and Education**

   Challenge:

   Mass-produced wearable devices needs user support, including

   - Onboarding,
   - Troubleshooting, and
   - Training,

   to ensure user satisfaction and engagement.

   Details:

   - Developing comprehensive user manuals, tutorials, and customer support channels is necessary.
   - Addressing potential resistance to adopting new health monitoring technologies.

9. **Market Competition**

   In a rapidly evolving market, competition from other health monitoring devices and wearables may pose challenges.

Addressing these challenges is essential for successful mass production and adoption of the Heart Monitoring System, ensuring it meets the health monitoring needs of a broad user base.

Overcoming Challenges

1. **Holistic Project Management**

   We need to implement a robust project management approach that integrates all aspects, from supply chain to quality control.

2. **Agile Adaptation**

   We need to be adaptable and agile in response to unforeseen challenges or changes in market dynamics.

3. **Continuous Improvement:**

   Establishing mechanisms for continuous improvement in manufacturing processes and product features is also required to overcome the challenges.

In order to successfully overcome these challenges, a multidisciplinary approach is required. It will involve collaboration between engineering, manufacturing, regulatory compliance, and business management teams. The continuous monitoring and adaptation to market dynamics are key to the success of mass production for a product as complex as a Heart Rate Monitoring System.

Acknowledgement

I would like to express my gratitude for the support and guidance provided for the completion of this assignment report. This report is a part of my M.Tech program in Software Engineering and represents my individual effort.

I want to thank my professor for their valuable insights and mentorship, which have been instrumental in enhancing my understanding of secure software engineering.

This assignment report reflects the knowledge I have gained during my program, and I am grateful for the opportunity to apply these learnings in a practical context.

References

[1]. https://my.clevelandclinic.org/health/diagnostics/23429-heart-rate-monitor

[2]. https://www.sciencedirect.com/science/article/abs/pii/S0045790621004699

[3]. https://www.researchgate.net/figure/AI-based-Patient-Monitoring-System_fig2_369299264