KU LEUVEN

DEPARTMENT OF
COMPUTER SCIENCE

Document Processing service (DocProc)

Part 1A

Requirements Analysis

Gharanfoli–Ngo–Nicolas

Academic Year 2021 – 2022

H09B5B: Software Architectuur
H07Z9B: Software Architecture

Sobhan Gharanfoli (r0734169)
Triet Ngo (r0869104)
Georgio Nicolas (r0875445)

1. Utility tree of ASRs

	Quality Attribute	Attribute Refinement	**Summary** **Rationale *Business Value*** **Rationale *Architectural Impact***
1	Availability	PMS database availability	PMS database must be available for the subsystems to access for 99.9% of the time.
			H: *As the core of the system (data are required for handling requests from Gateways, HIS, etc.). Its uptime is the first priority since downtime can interrupt the system as a whole which can affect the agreed availability target in the contracts and lose the providers money and reputation.*
			H: *Downtime of PMS database will delay or result in failure in other parts of the system. Changes in the database will require changes in the system (different setup, data structure, data framework, etc.).*
2		PMS ML risk assessment availability	PMS must be available to assess risk level by applying the ML models for 99% of the time.
			H: *Risk assessment is one of the core functionalities of PMS that are required to determine emergencies. Crashes in this part can lead to delay in assessing emergencies cases and negatively impact the reputation and compensate cost.*
			M: *Downtime of PMS ML will delay the assessment queue. While it will still be processed eventually when the service is back online, this can cause damages in case of emergency. Then human interventions are required (such as manually classify risk).*
3		Gateway availability	Gateway must be available for the users for 99% of the time. At most 2 hours of down-time is allowed without degrading the reliability of PMS.
			M: *It is important to have the Gateway available to receive data from sensors and interchanging data with PMS. Down-time from Gateway only affects the user and not the system, unless it is an emergency.*
			M: *Down-time from Gateway limits the transmission between subsystems. This require prior design whether to add cache in wearable unit in case of crash in gateway or discard the information.*
4		Emergency call center availability	Emergency call center must be available to receive and handle emergency calls from users 99.9% of the time.
			H: *It is extremely important to handle health emergencies as fast as possible. Delays can cause irreversible damage to the patient's health, hospital and doctor reputation.*
			L: *Changes are not required in the system in case of down-time to handle emergencies.*
5		ML provider availability	ML provider must be available to provide model updates 95% of the time. A day off from the ML provider will not negatively impact the system.

	Quality Attribute	Attribute Refinement	Summary Rationale *Business Value* Rationale *Architectural Impact*
			L: *While it is relatively important to retrieve the newest ML models, the models that are already in the system should be reliable enough to handle the system in a day or two without sacrifices on a large margin of accuracy.*
			L: *Down-time from ML provider does not affect the Gateway or PMS too much since there is already existing models in them.*
6	Security	Patient data integrity	Patient records/risk level changes by unauthorized personals are detected, assessed, processed and reverted in less than 3 hours.
			H: *This is very important because patient data privacy is maintained by law and violations are very troubling to deal with (costly, etc.).*
			H: *Security relating to data requires careful design and subject to changes (upgrade to deal with new attacks, maintenance when breach) but in the system overall it is an outer layer that does not require changes in the system. However, the data that is changed can produce unforeseen/undesirable system behavior (i.e. risk level changes subject to involvement of handling emergency).*
7		Patient data confidentiality	The amount of patient records shown vulnerable by attacks are lower than 1% of the total data.
			H: *The less data leaks out during attack, the easier it is to detect, compensate and improve the system. For example: it is easier to deal with lawsuits about leaking 1% of the data than 50% of the data.*
			L: *The data that leaks out are usually labeled exposed data and require investigation to deal with but does not affect the other parts of the system.*
8		Hospital staff authentication: PMS database access	Staffs such as nurses, physicians and cardiologist can interact with PMS to accessing patient data. Depending on roles and permissions, there are limitations on accessing these kind of data. Hence, the time to detect and block a forged identity certificate to access the PMS to retrieve patient data must be less than 3 seconds.
			H: *It is very important to verify the roles and identity of the user since there are limits in data and functionalities in terms of roles. Attacks using false-role can damage the system and can be costly to repair.*
			M: *Attacks using false identity can damage sub-systems and can bring changes to the system.*
9	Performance	Process speed for handling high risk patients	High risk or emergency situations must be prioritized by the PMS for applying ML model estimation, notify related parties, send updates so that the duration of this procedure is at most 2 seconds.
			H: *High risk patients require immediate intervention from either the physicians or emergency center.*
			M: *There should be wait queue managed by the PMS in order to realize this requirement.*

	Quality Attribute	Attribute Refinement	Summary Rationale *Business Value* Rationale *Architectural Impact*
10		Handling concurrent patients	ML estimation should happen in parallel for simultaneous patient data arrival if they have the same priority(risk level): waiting time for risk level estimation of patients with same priority should not differ more than 0.1 second.
			H: *This ensures that the performance of the system will have small variance. By using parallelism system can take advantage of multicore hardware to increase the general performance.*
			M: *Threads have to be used for running each new ML estimation, so thread management is required.*
11	Adaptability	Compressed packages in case of poor internet connection	Packages sent from the gateway must be compressed before been sent in case of poor internet connection so that packages sent from the gateway must be compressed before been sent in case of poor internet connection so that $compressed\_data\_transmission + compression\_time < normal\_data\_transmission$.
			M: *Increasing the up-time of system through sending smaller amount of bytes results in better performance in case of poor internet connection.*
			M: *compression and decompression algorithms must be implemented in the gateway app and server.*
12	Interoperability	Sensors - Gateway data interoperability	When sensors send sensor data (heart rate, etc.) to the Gateway, the Gateway receives the data and interprets them. The probability of that data is as same as the data the sensors send (correctness) is 99%.
			H: *the precision of health data is important since different data can negatively impact the decision of the doctor or ML model in determining the risk level of the patient which damages the reputation of the system.*
			M: *If gateway records wrong data sent from the sensor, it will send the wrong data that affects other system part but does not require changes in other part of the system.*
13	Reliability	Lightweight ML model reliability	The accuracy of the ML model in Gateway is at least 80%.
			M: *the higher accuracy of the lightweight model is, the less workload in sorting and processing from the PMS.*
			M: *Since the data will be evaluated again from PMS ML models so that the reliability only needs to be high enough to not overload PMS.*
14		PMS ML models reliability	The accuracy of the ML models in PMS is at least 95%.
			H: *Reliability of the ML models in PMS is extremely important since false evaluation requires attention from other parties such as doctors, emergency call centers, etc. which increases their workload hence decreases the reputation of the data from the ML models later on.*
			H: *Results from PMS ML models will directly affect other subsystems (record in database, notify emergency personals, etc.).*

	Quality Attribute	Attribute Refinement	Summary Rationale *Business Value* Rationale *Architectural Impact*
15	Modifiability	Adding New Hospital	In the future, there can be more hospital wants to use the PMS system. HIS must be integrated with the existing ones in the hospital, patients from the hospital must use the wearable units, hospital personals must use the PMS system. This process of adding and integrating must be less than 1 month.
			H: *It has to be easy to add the PMS system to the new hospital. More hospital will bring more profit and reputable for the system.*
			M: *New hospital has to set up the HIS in the hospital and register hospital staff and patients to the systems.*
16	Scalability	Storage scalability	Adding new amount of storage when a new patient is registered to the system, should take at most 1 hour.
			H: *This will help the system store patient data and avoid unnecessary communication with the HIS which results in higher performance of the system.*
			M: *The database of the system should be designed in a way that adding new storage to the system does not require changes to other part of the system.*
17		Computation power scalability	Average throughput of the system in high load (100 patient data/ minute) should be at most 10% worst than average load (5 patient data/minute).
			H: *This will help the system provide good quality service when the load becomes high.*
			H: *In order to scale the system in realtime, there is a need to monitor the load of the system and add hardware automatically in a short amount of time.*
18	Usability	Simple data representation	When patients consult their status from the app, they should be able to understand it in less than a minute.
			M: *Having a clear data representation for the patient would have positive impact on the experience of using the system in general.*
			L: *This can be realized by good UI design which does not have high architectural impact.*
19	Robustness	Ability to deal with partial data	The PMS should be able to function in case data is partially available. This can be due to sensor faults or transmission problems from the gateway. A minimum of 50% of the complete data package should be enough for the system to work.
			M: *Missing data can always happen in real life situations so it is important to consider these possibilities.*
			M: *Missing data should be checked and PMS should try to fill in an estimate for those using previous and current patient records.*
20	Testability	Testing in collaboration with the hospital	Ability to set up a test for the whole chain of the system (simulating sensor data and sending it to the gateway and then to the PMS servers then to the HIS, Physician, GP or emergency center) in collaboration with the hospital in less than an hour.
			H: *It is very important to be able to test all the parts of the system and the system as a whole in order to provide a reliable service.*

	Quality Attribute	Attribute Refinement	Summary Rationale *Business Value* Rationale *Architectural Impact*
			L: *Architecture of the system does not need to be changed for this. Arrangement with the hospital is necessary.*
21	Distributivity	Geographically spreading of PMS servers	Spread PMS service centres across Europe according to the patients locations: up time for gateway data should be approximately same for all patients across Europe.
			M: *This could be important if the hospital has international reputation.*
			H: *This requires transferring data between data centres in case a patient moves to another place, so communication between servers has to be added to the system.*

2. Quality Attribute Scenarios

2.1 Security: User authentication - PMS database access

PMS consists of subsystems that require patient data to work on. Hospital staff and patients have different permission and access scope to data. Hence, it is important to ensure to check for user authentication when processing requests that access patient data (i.e. whether the users are who they claim they are and that they have the appropriate permission to access the data that they request).

- **Source:** Registered user (hospital staff, patient, ML provider staff, etc.) or Unauthorized users
- **Stimulus:**
  - PMS users attempt to access the patient data that they don't have the permission to by masking their request to PMS (UC6, UC9). For example, try and error for a patient id.
  - PMS users attempt to change the patient data (risk assessment, risk level, etc.) that they are not responsible for (UC7, UC8) by impersonating the doctor that is responsible for the patient.
  - Trained nurses attempt to (de)register a patient without the confirmation of either the patient or the cardiologist (UC10, UC11).
  - PMS users (usually hospital staff) attempt to retrieve massive patient data from PMS (similar to DDoS attacks).
  - PMS users attempt to access/clone/distribute patient data to unregistered devices.
- **Artifact:** Patient data in the PMS database
- **Environment:** Normal operation
- **Response:**
  - Any requests that involve accessing patient data require authentication. The authentication is responsible by PMS or can be delegated to the hospital via Oauth2 and OpenID.
  - Access control is required at any level of accessing scope in the PMS database. In other words, PMS users can only access the patient data that they are involved with/responsible for.
  - Any requests that involve accessing patient data must be made via PMS registered devices. For example, hospital computers, hospital distributed computers for staff, personal computers and phones must be registered.
  - Any requests that involve with accessing patient data require details logging, the logging contains
    - Timestamp of the request
    - Identification of the PMS user
    - Details regarding the patient data that they access to for example patient id, data output (short summary, risk status, details report, patient record, etc.).
    - Status of the request (Valid access, Unauthorized access, etc.).
  - PMS keeps a separate log of the users that have requests resulting in Unauthorized access. The account will be blocked and the PMS admin is notified. The patient data that is requested unauthorizedly will be flagged as exposed but won't be blocked for valid uses of other authorized users.
  - The amount of patient data that PMS user can access must be assigned by their role. For example, patients only need 5 requests/second but hospital staff such as cardiologists may require a large amount of data to analyze their patients. This number must be considered appropriately to ensure that the system won't be overloaded but as the same time provide the PMS users with ease of use.
- **Response measure:**
  - The authentication to PMS must be strong enough to withstand password-guess attacks and the same level must be applied to the hospital security level since it is possible to login to PMS via hospital portal (delegation resemble to "login with google"):

    - User password must have at least 10 characters, at least 2 numeric characters, and at least 1 special character. The password cannot contain information that is publicly accessible such as the user's name, birthday, etc.
    - Any account using "log-in-via-hospital" must be registered by the hospital and assess and assign roles by PMS.
  - The access control to PMS data is maintain by PMS and it cannot be manipulated or customized by PMS users:
    - Identification check and permission assertion are required for any requests that involve accessing the PMS database.
    - The identification and access link must be unique, random and long with respect to access duration, allowed users, etc. so that it cannot be customized by hand-made by learning the pattern of the identification.
  - Hospitals and PMS must have agreement regarding the registering procedure for devices. Only registered devices can make and store result from PMS database.
  - All access to the PMS database must be successfully assessed and logged before issuing the response to the requesting user.
  - Any Unauthorized access request issued user will be warned by the system 3 times before blocking their account. Unblocking account only possible by PMS admin.
  - Any Unauthorized access request issued user will notify the PMS admin and HIS security staff within 1 minute.

2.2 Availability: PMS database availability in case of crashes

There are multiple components in PMS but one of the most important ones is PMS database where patient data is stored. In this scenario, we consider the case where the PMS database is not responding (unable to retrieve data due to crashing or overloading).

- **Source:** Internal
- **Stimulus:**
  - The internal component managing the database fails or crashes.
- **Artifact:** The internal component
- **Environment:** Normal execution
- **Response:**
  - The crashes guarantee that no patient data will be lost. The state before crashing and awaited-request should be recorded for consistency.
  - Prevent the fault from becoming a failure. In other words, the PMS database should have a minimal up time.
  - Detect the fault:
    - PMS administrators are notified about the crash.
    - The crash and its cause including the state of database before crashing are detailly logged for investigation.
  - Recover from the fault:
    - PMS database can still be able to detect the crash and goes into degraded mode:
      - PMS databases can use replicas (if available) as a backup version and limit the operations/requests from PMS users to read only requests and block requests that attempt to modify the database in degraded mode (UC 7, 8, 11, 14, 15, 17).
      - Gateways are able to detect degraded mode and temporarily store the packages for write-request (UC4) and send to PMS after it becomes online later on.

        - After receiving notification regarding the fault, PMS administrators fix the problem. For example, replace the hardware in case of malfunctioned hardware or reload the database from one of its replicas.
        - When repaired, the Gateways are notified and release the temporarily stored requests to the PMS.

- **Response measure:**
    - Detect the fault:
        - PMS administrators are notified about the crash within 15 minutes.
        - The details of the crash should contain the detail regarding the requests and operations performed in the database in the last 24 hours.
    - Recover from the fault:
        - The time for PMS detects the crash is less than 1 minutes
        - The time for PMS switches to degraded mode must be less than 5 minutes.
        - The time for the administrators to fix the crash and make the database becomes available again is at most 10 hours.
    - The PMS database should be available for 99.9% of the time

2.3 Performance: Process speed for handling high risk patients

There are different patients registered in the PMS system and each of them are in different situations. PMS should try to handle high risk patients as fast as possible and prioritize them over others.

- **Source:** Patient gateway
- **Stimulus:**
    - Gateway sends patient data after recognizing that the patient is in an emergency situation by using lightweight ML models(UC 3).
    - Gateway sends periodic data of a patient with high level risk(UC 4).
    - Gateway sends periodic data of a patient with normal level risk(UC 4).
    - Gateway sends periodic data of a patient with low level risk(UC 4).
    - Physician consults new patient data from the PMS, which in turn forwards this request to the gateway(UC 9, 4).
- **Artifact:** PMS System
- **Environment:** Normal execution
- **Response:**
    - PMS server receives data package.
    - It checks whether the received data is from a registered patient by checking the authentication token of the package.
    - If it validates the token it proceeds, if not PMS will discard the data.
    - PMS determines whether the data package is an emergency notification or not.
    - If it is an emergency notification PMS has to perform an emergency validation using ML models. This estimation should be prioritized over normal and low level risk patients which have sent sensor data concurrently or wait for the PMS to perform risk estimation.
    - If PMS decides that the emergency notification is false, it proceeds with sending the data to the hospital information system (UC 17).
    - If the PMS validates the emergency situation, it notifies the emergency call center with all the emergency details and updates the patient records in the HIS (UC 17).
    - If it is not an emergency notification, PMS determines the risk level of the patient.

  - In case the patient is in a high risk level, it must be prioritized over normal and low level risk patients which have sent sensor data concurrently or wait for the PMS to perform risk estimation.
  - In case the patient is in normal risk level, it must be prioritized over low level risk patients which have sent sensor data concurrently or wait for the PMS to perform risk estimation.
  - PMS will eventually run the ML models and determine the new risk level of the patient (UC 12) and send patient data and the new risk level to the HIS (UC 17).
  - If the new estimate of the patient risk level changes, it will notify the interested parties (Physician, cardiologist, patient) (UC 5).
- **Response measure:**
  - If the received data from the gateway is an emergency notification or it is from a patient in a high risk level, this process as a whole should happen in less than 2 seconds independent of the current load on the server.

2.4 Modifiability: Adding new Hospital

Right now the PMS system only supports a few hospitals but in the future, the PMS system would expand the business and want to have more hospitals join their system and use their service.

- **Source:** The new hospital
- **Stimulus:**
  - The new hospital would like to integrate PMS to their own existing HIS system.
- **Artifact:** HIS integrates PMS to their system for hospital staff usage, PMS adds the new hospital to their database, and registers the new hospital staff and facilities.
- **Environment:** At run-time
- **Response:**
  - While integrating PMS to the existing HIS and adding the new hospital to the PMS system, the modification should not affect the workflow of other hospitals and minimize the affecting artifacts in the new hospital.
  - The preparation for the transition in the hospital includes preparing wearable units, adding PMS framework and software to the hospital system (computer, phone, etc.). Then the implementation will be applied to a small portion of the hospital.
  - The hospital testing portion will train their nurses, cardiologists, and patients to use the PMS system after the PMS tests the system beforehand.
  - After the testing period, the implementation will extend to the whole hospital and deploy the PMS system to use in practice.
  - PMS registers the new hospital to their database and processes the administration part (adding hospital staff users, etc.).
- **Response measure:**
  - The modification procedure to add a new hospital to the PMS system takes less than 1 month to implement, test the small portion of the hospital.
  - Changes in integrating PMS to the hospital's HIS takes less than 2 month to implement, and to test the small portion of the hospital.
  - The deployment of changes to their whole hospital for using PMS in their hospital takes less than 1 man month.