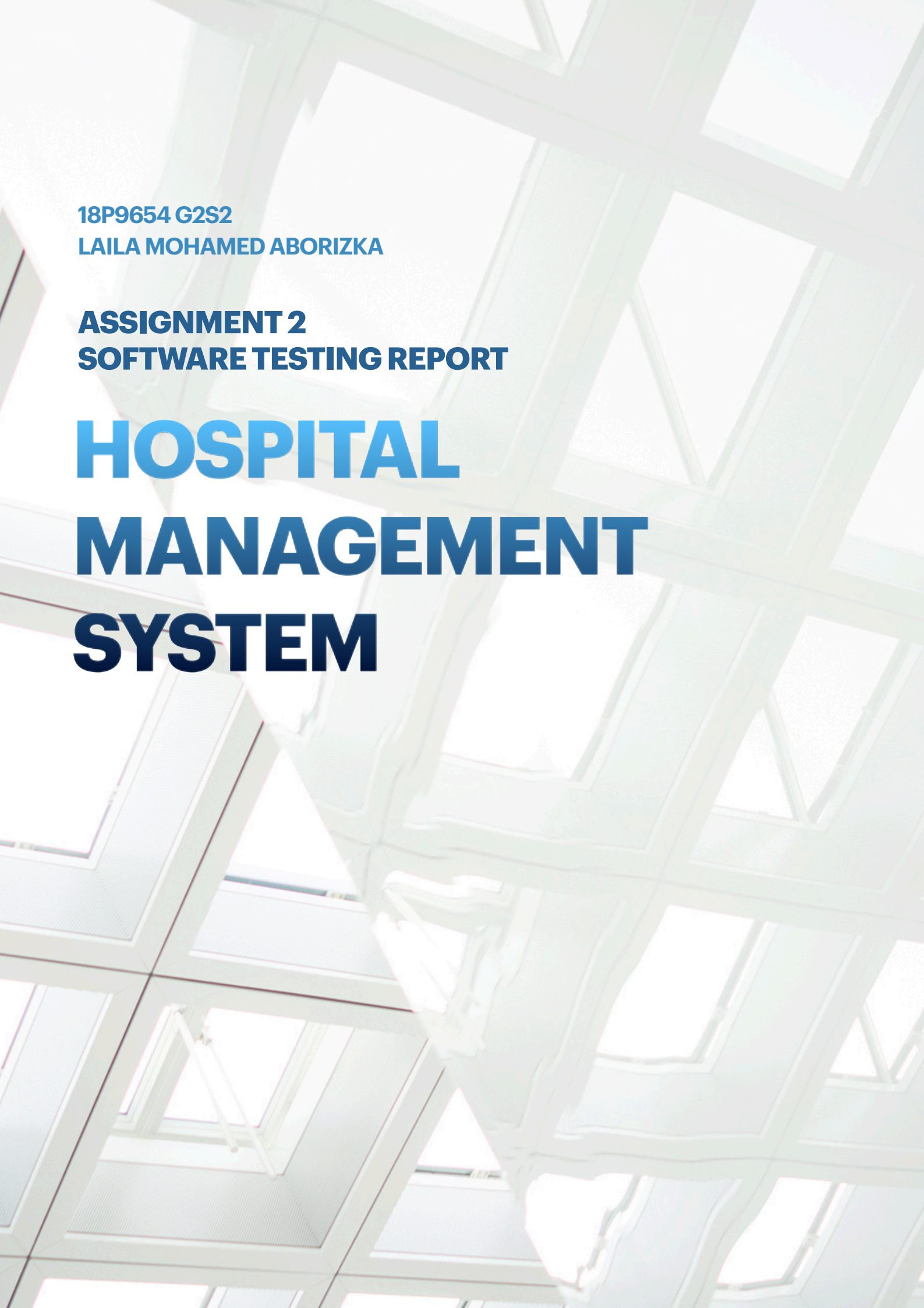
18P9654 G2S2
LAILA MOHAMED ABORIZKA

ASSIGNMENT 2
SOFTWARE TESTING REPORT

HOSPITAL MANAGEMENT SYSTEM



QUESTION ONE

This section discusses integration testing. This is the phase in which we combine individual software modules and test them as a group to ensure they're still working properly when joined together.

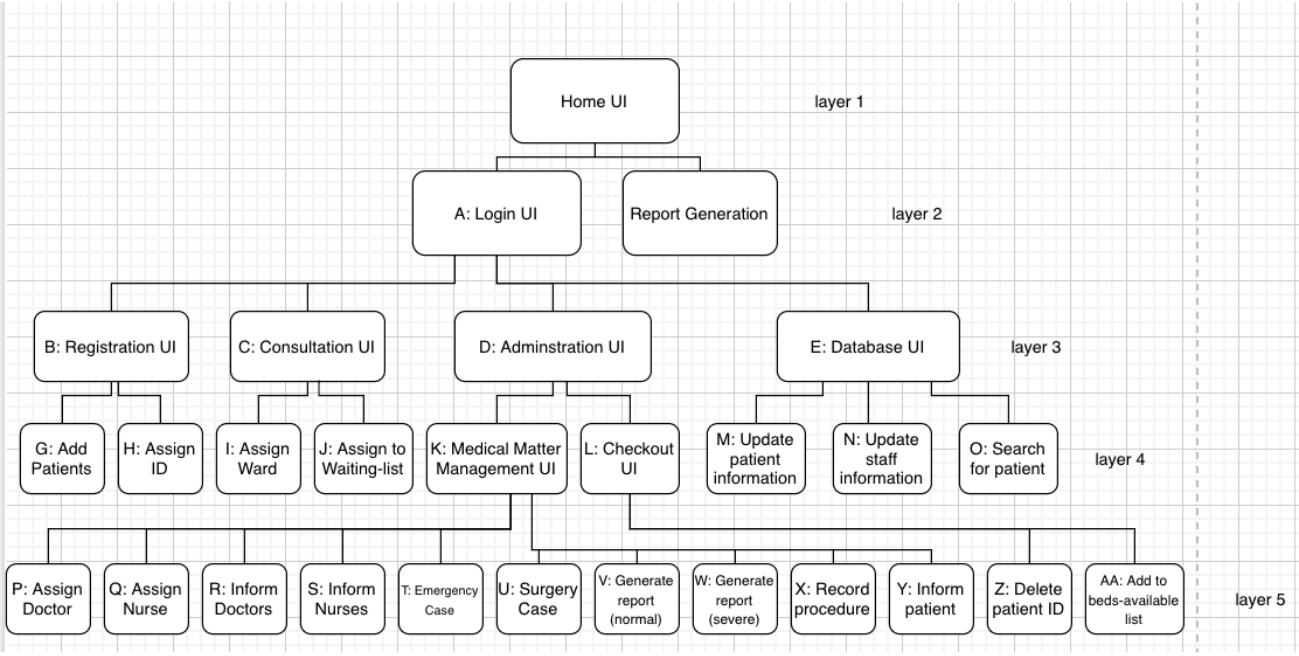
The technique that is going to be used to test the hospital management system is the Top Down Testing strategy.

This model is good as it minimizes the number of drivers and drivers are usually harder to write than stubs. In other words dummy code is reduced. In addition to that it ensures that the top layers are tested first which are the most important parts in our case because they are the UI.

Below is how this model can be applied on this system.

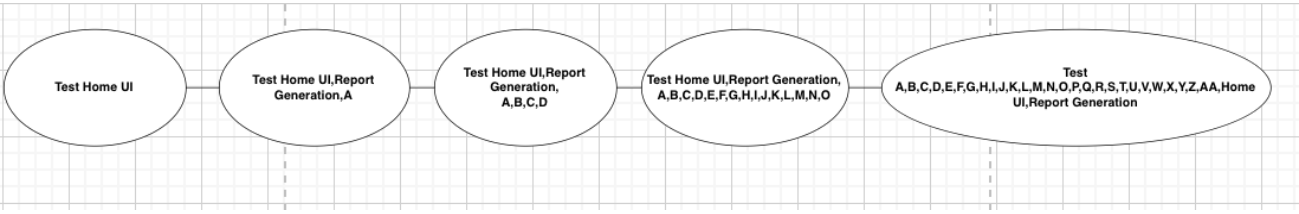
SYSTEM SKELETON

The system is designed as follows. Starting with a home screen that displays reports and takes users to the login screen if needed. Then the Login UI that takes users to the interface specified for them.for example front desk are taken to registration UI. Nurses to consultation. Administrative to Administration. And all of them came aces the database, etc... the diagram below further illustrates this.



There are some assumptions on which the following testing scenario is built. Firstly, the development process starts with the UI (top down) that's why the top down testing approach is the most suitable. Also, The test cases for each module are specified.

So for testing:



First of all stubs are created to test the first layer which is the Home UI.To make sure it displays the reports generated correctly and takes the user to the Login UI when needed. Followed by functional testing defining all test cases with the selected unit or component. Then structural testing that is defining the test cases that exercise the selected unit or component . Then we execute performance tests and keep records of all test cases and activities of testing.The same steps are repeated layer by layer until we reach the bottom layer each time testing the modules we have according to the test cases that need to be covered.

QUESTION TWO

In this part we get to determine the different system testing techniques that are essential for the hospital management system.

Assumptions:

-Complete software system is developed

-Unit testing is complete together with integration testing

-Specifications for the product are complete

-Test scripts and schedules are done

The following tests are the suitable tests for this system testing:

Limit testing

The System must support 1000 people at a time.

Testing requirements:

Test the system with 1000 users at a time and check how the system performs. The system shall give responses in 1 second after checking the patient's information. And The user-interface screen shall respond within 5 seconds.

Test cases:

Test the system with 1000 people registered

Test the system with 1000 concurrent users

Test the system with 1000 concurrent logins

Stress testing

Testing requirements:

Test the system with more than 1000 users at a time and check how the system performs and how unstable it can get.

Test cases:

Test the system with 1200 people registered

Test the system with 1200 concurrent users

Test the system with 1200 concurrent logins

Test the system with 2500 people registered

Test the system with 2500 concurrent users

Test the system with 2500 concurrent logins

Test the system with 150000 report generated

Soak testing

This system is expected to be working 24/7 since it is a hospital. In the same time the system has to be delivered within 6 months (assumption).

Testing requirements:

Test the system after several periods of time and check the performance and stability of it.

Test cases:

Test the system after 1 month

Test the system after 3 months

Test the system after 5 months

Spike Testing

This system is prone to extreme emergency situations such as a fire

accidents highway accident, any natural disaster casualties so spike testing has to be performed

Testing requirements:

Test the system with a normal number of people

Test the system in case of a disaster

Test the system again with normal flow

Test cases :

Test the system with 5o users

Test the system with 900 users

Test the system with 40 users

Recovery testing

In the extreme cases There may be loss of power or loss of internet connection the data in the system can’t be lost it has to be recovered.

Testing requirements:

Test the system after loss of power and check if data is recovered properly.

Test the system after loss of internet connection and check if data is recovered.

Test cases:

Test after Disconnecting the internet

Test after cutting off power

Compatibility testing

Testing requirements:

Test the system with windows 10

Test the system with all web browsers (Google Chrome,Microsoft Edge, etc..)

Test cases:

Test system with windows 10

Test system with Google Chrome

Test system with Microsoft Edge

Usability testing

Testing requirements:

System UI doesn’t frustrate users, easy to use and works properly

Test cases :

Test system with front desk staff

Test system with administration

Test system with nurses

Documentation testing

Testing requirements:

Documentation is useful and readable and accurate

Test cases :

read document

Check solution for an issue in document

check accuracy of document

Security testing

Testing requirements :

The system requires the patient to identify himself /herself using PHN Logon ID Any user who uses the system shall have a Logon ID and Password. These are sensitive info that need to be protected

Nurses shall have access to database and consultation only

Administration shall have access to medical matter management, checkout and database only.

Front desk shall have access to registration and database only

Test cases:

Test access trial from non authorized users

Test front desk users

Test nurses

Test administration

Acceptance testing

Testing requirements:

pilot, alpha and beta testing

Test cases

Test system aș a small scale experiment in a controlled environment

Test system in-house user testing

Test system in the hospital (public user testing)

QUESTION THREE

In this section we shall conduct the threats modeling approach to identify the main potential threats for our system.

The threat modeling approach allows us to categorize and analyze the threats to our hospital management system.

— Firstly we assemble the team with all the experts and consultants

— We identify our assets:

-patient personal information (e.g. PHN numbers and IDs)

-staff personal information

-Users Login credentials

-Patients medical reports

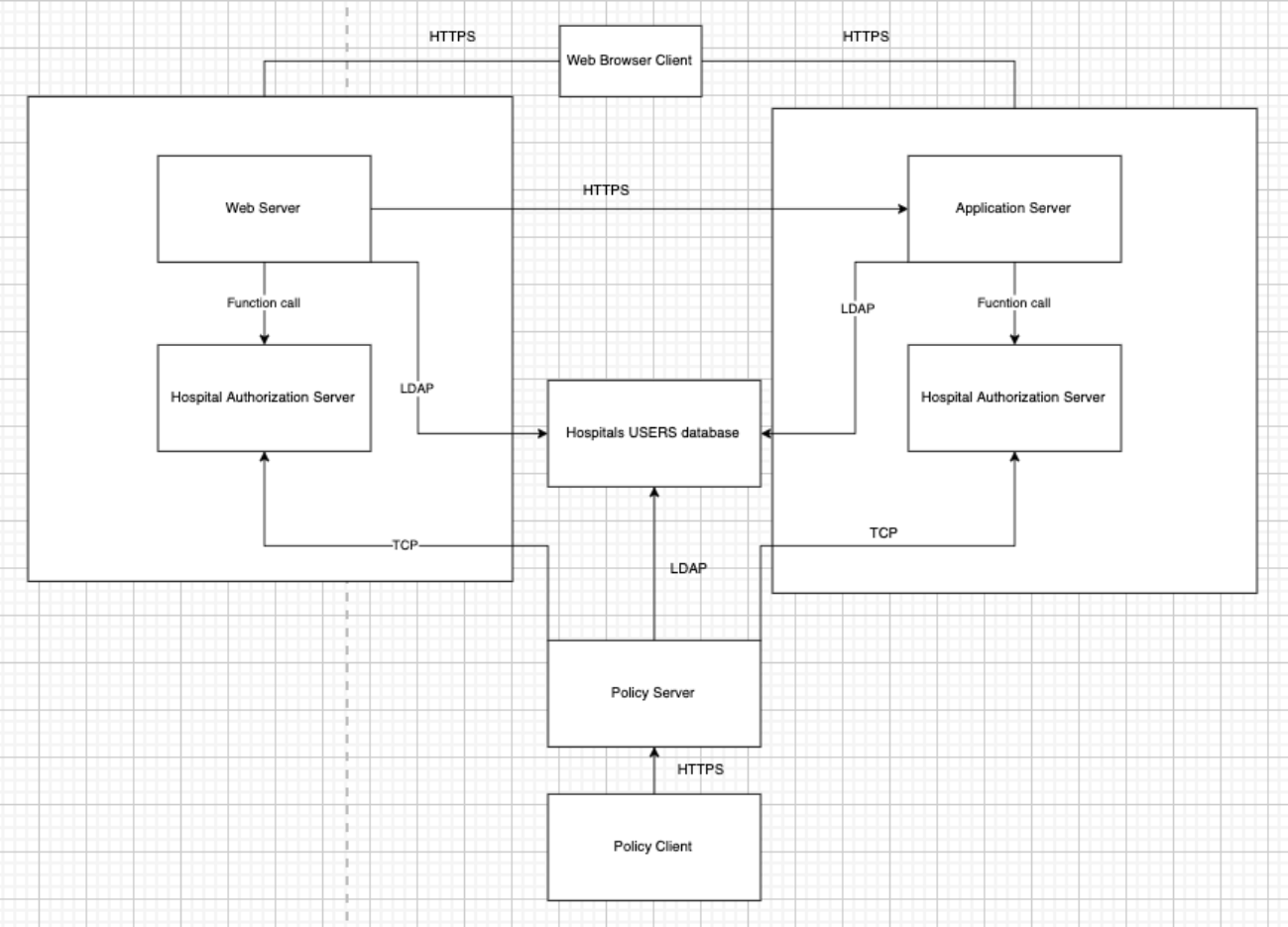
-sensitive medical information

— Then we identify threats, describe them, classify them and rank then

Threat	STRIDE	Rank
Hacker gets a patient's PHN and authentication information and so is able to get service as if they are the real patients	Spoofing	Medium as this won't have a major effect on the hospital however patients will be badly affected .
Hacker gets access to staff authentication information	Spoofing	High if someone manages to hack the system and access staff information he can use this info to mess with the whole system accessing very sensitive data and stealing it which may result in huge problems .
Hacker may access patients medical reports	Information Disclosure	Low, this data should be private however if seen by another person this won't cause a problem right away.

Hacker may mess up waiting lists and sensitive information such as available rooms or surgery appointments.	Tampering with data	High, this would result in unfair advantages and would cause many problems to the hospital. For example changing surgery schedules may lead to loss of life.
Hackers may stop admins from registering patients	Denial of service	High, the hospital won't be able to take in new cases.
Hackers may interfere with emergency cases	Denial of service	High, this is a disaster emergency case actions have to be performed safely and right away or else it might result in death of people and legal problems to the hospital.
Front desk staff may gain unauthorized access to admin UI which is illegal and not allowed for them	Elevation of Privilege	Medium, this will allow front desk staff to alter and interfere with admins work which is a problem but not the worst because after all they are still hospital workers.however it still should be prevented.
Front desk staff or admins may gain unauthorized access to consultation UI	Elevation of Privilege	High, both admins and front desk don't have a medical background they can't make or interfere in any medical decisions. So consultation has to be totally secure and only nurses are allowed access.

This leads to the following security architecture suggestion:



How is this configuration useful for security?

First of all using several servers provides better security against cyberattacks and in the case of attacks this prevents access to the database.

Also some components interact through secure HTTPS protocol that is because they connect through the internet.This ensures confidentiality of data and protection of Login credentials and authorization information which means both security and privacy.

Also the presence of a policy client ensures that only authorized users are permitted access and that hospital privacy terms are applied.

Through this security architecture most cyber security attacks including malware ,phishing, URL Manipulation, etc...