TÉCNICO LISBOA

Health Care

NETWORK AND COMPUTER SECURITY

28 December 2021 | Campus Alameda - Group 26

THE TEAM:

Ana Albuquerque	André Proença	Joel Russo
ist1102209	ist1102327	Ist1102098

1. Problem

Health care institutions gather and store sensitive information from patients. The information systems should allow fine-grained and contextualized access to the records to the relevant staff.
One of the relevant types of data stored are test results. Some of the medical tests can be performed inside a hospital lab, but in many cases, tests are done in partner labs, that have a distinct infrastructure, remote from the infrastructure of the hospital, that need to be interconnected. In addition, the privacy clause is a key issue for safe and successful access to patient health information. Current approaches do not always provide patients with the ability to establish appropriate rules for accessing their information in a secure manner.

A patient's medical records are extremely sensitive data. The historical records made by doctors facilitate the process of diagnosing a patient, ensuring their quality, which helps clinical staff to treatquickly and accordingly.
This data should be kept private, allowing only the discriminating staff to access it. We believe, thatall healthcare facilities should have access to this type of information so that patients can receive healthcare anywhere and at any time. Therefore, the data should be protected from external agents(i.e., outside the medical institutions) and from unauthorized people within the institutions.

This report aims to demonstrate a secure system that allows secure and confidential access to patient medical records of certain healthcare organizations. It also demonstrates the secure interconnection (sending and receiving of medical records) of partner healthcare organizations. In such manner, a patient will be able to access his/her medical records in every healthcare organization where he/she is registered.

1.1. Solution Requirements

Client application requirements:

As a user (depending on my privilege) I am able to...

- Read my medical records (send requests to the system);
- Receive responses from the system (receive replies from the system).
- Change my system password

As a Doctor and Nurse, I am able to...

- Create/Read/update medical records.

As a Patient Service Assistant and Porter, I am able to…

- Read specific information about which patient is assigned to me.

DIGITAL RECORDS HEALTH CARE

As a Ward Clerk I am able to…

- Register a patient in the system.

As a Patient I am able to…

- Read my medical records.

As the System Administrator, I am able to…

- Create new personnel within the organization.

Server application requirements:

The System…

- Ensures confidentiality and integrity of medical records;
- Ensures confidentiality and integrity of communications with the web application;
- Ensure successful authentication of citizens;
- Authenticates citizens in a secure way;
- Ensures that only authorized staff and patients have an account;
- Ensures different “roles” have access to different privileges;
- Ensures there is only one account per citizen, using citizen ID card number;
- Prevents access to medical records if the citizen does not have privileges;
- Allows user A to change the privileges of user B, if user A is a system administrator;
- Validates and sanitize form input;
- Uses HTTPS to encrypt communications;
- Stores and manage symmetric and asymmetric keys;
- Defines a restricted set of rules on the firewall;
- Establishes mutual authentication and shares medical records with partner institutions;
- Minimizes the impact of attacks inside the system.

1.2. Trust Assumptions – TO DO

Fully trusted:	Partially trusted:	Not trusted:
- Hospital and Laboratory Frontend (that are servers)	- Certified user machine	- Not Certified user machine
- Hospital and Laboratory Backend (that are servers)		
- Hospital Backend Server		

2. Proposed solution

In order to simulate real systems and their interconnection, our solution is based on the development of two systems representing healthcare institutions. A hospital and a partner laboratory. The goal is to have two completely independent and functional healthcare institutions, each with its own data storage system and independent web platform, and simultaneously simulate the sending of confidential patient's medical records in a secure way from one institution to the other. Authorized hospital and laboratory staff as well as patients will be able to access their respective hospital and laboratory remotely or locally.

2.1. Overview

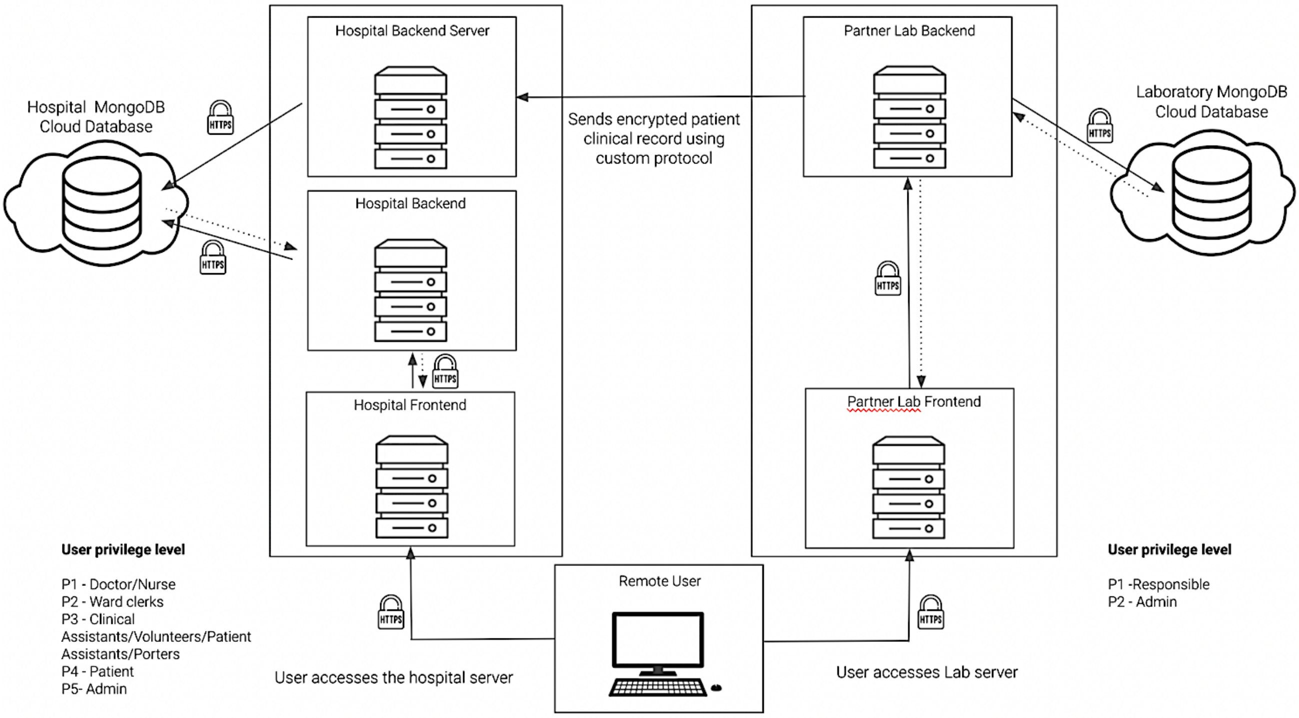
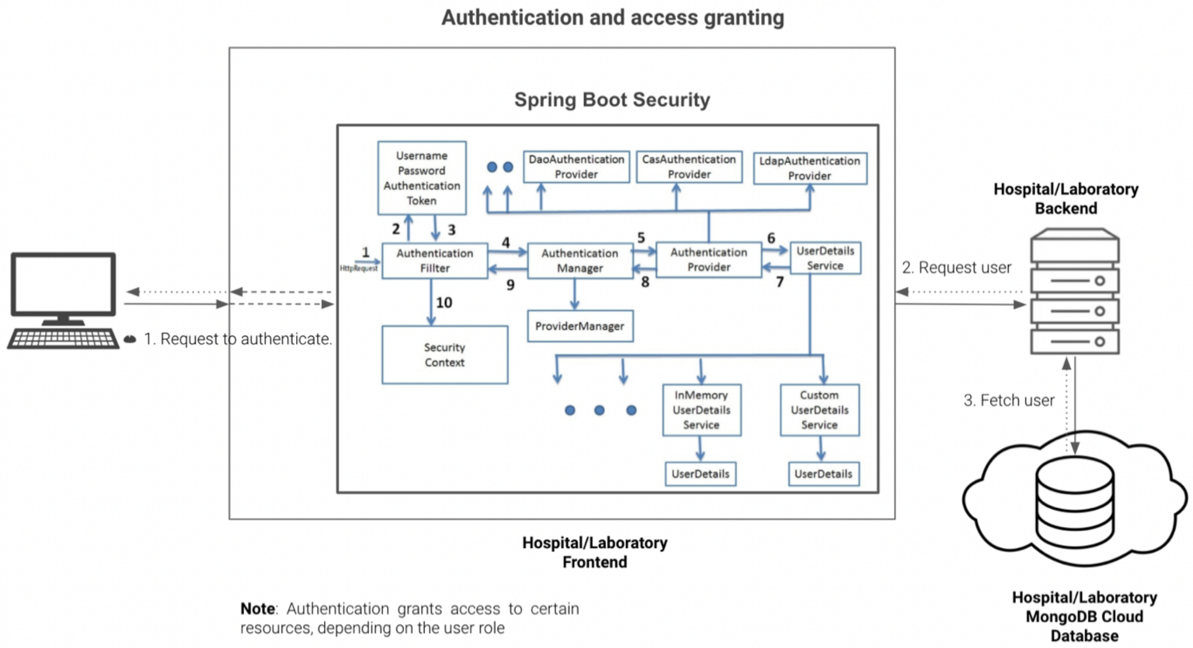


Figure 1. General Architecture

Spring Security, Security policy language

Spring Security is a powerful and highly customizable authentication and access-control framework. It is the de-facto standard for securing Spring-based applications.

Spring Security is a framework that focuses on providing both authentication and authorization to Java applications. It has features like Comprehensive and extensible support for both Authentication and Authorization. Protection against attacks like session fixation, clickjacking, cross site request forgery, etc…


Authentication and access granting
Spring Boot Security
Username Password Authentication Token
DaoAuthentication Provider
CasAuthentication Provider
LdapAuthentication Provider
1
HttpRequest
2
3
4
5
6
7
8
9
10
Authentication Fillter
Authentication Manager
Authentication Provider
UserDetails Service
ProviderManager
Security Context
InMemory UserDetails Service
Custom UserDetails Service
UserDetails
UserDetails
1. Request to authenticate.
2. Request user
3. Fetch user
Hospital/Laboratory Backend
Hospital/Laboratory Frontend
Hospital/Laboratory MongoDB Cloud Database

Note: Authentication grants access to certain resources, depending on the user role

Figure 2: Authentication and access granting.

2.2. Deployment

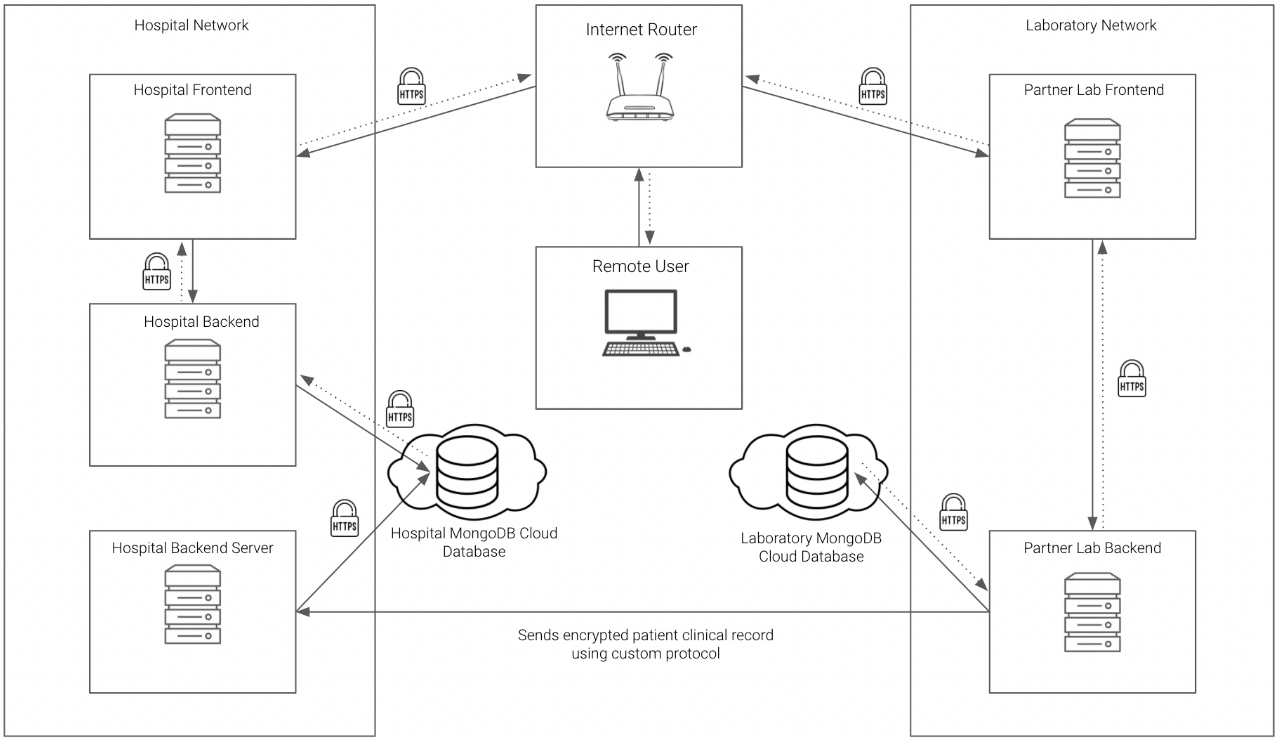


Figure 3: Network Architecture.

As you can see, 7 virtual machines running Ubuntu Server are deployed.

- 1 for the router that will simulate the internet;
- 1 for Hospital Server, which will receive the clinical records from Partner Lab Backend;
- 2 for the hospital and laboratory respective frontends;
- 2 for the hospital and laboratory respective backends;
- 1 for local or remote users which will access the frontend servers. To change the location of users on the network, just change the properties of the VM in the hypervisor (VirtualBox, for example). This way we avoid creating multiple VM's for each local and remote user.

2.3. Secure channels configured

Who is communicating?

- A user accesses any of the health institution platforms through the HTTPS protocol, thus encrypting the communication and making it secure. Each of the health institutions has a frontend that authenticates a user according to his/her "role", processes, validates, sanitizes form data and makes requests to the api of the respective backend institution to authenticate users, or to fetch a user or a medical/clinical specific information, which then makes a request to the respective database. The connections to the databases, as well as the connections from frontends to backends, use the HTTPS protocol, thus ensuring content integrity and confidentiality.

SSL certificates

- By default the backends connect to their databases via HTTPS. SSL is configured in the backends application.properties. For the frontends and backends, self signed certificates were created with the help of the keytool. To establish the HTTPS connection were also configured the application.properties files in the frontends and backends of both institutions.

2.4. Secure custom protocol developed

Who is communicating?

- Each time a partner Laboratory responsible creates a clinical record, the record is automatically sent to the hospital in a secure and confidential way. To establish this connection, it is necessary to ensure a mutual authentication by the laboratory and the hospital server. If the authentication is successful, the laboratory makes a request to the hospital server, asking if the patient exists in the hospital's database. If the patient exists, the clinical record will be sent and then registered in the hospital's database.

Which keys will exist and how will they be distributed?

- Each Health Institution is a certifying entity that issues its own certificate. Each of theseinstitutions have an asymmetric key pair, stored in a keystore, which will be used to communicate and establish secure connections. Symmetric keys are generated when establishing a connection between laboratory backend server and hospital server, and are temporarily stored in the keystore. Certificates were created with the help of keytool and are stored …

Security properties ensured:

- The Protocol ensures integrity, confidentiality.

3. Used technologies

- Frontend: Java Spring Boot
- Backend: Java Spring Boot
- Database: MongoDB
- Security policy language: Spring Boot Security
- Virtual Machines: Ubuntu Server
- Firewall: UFW (Uncomplicated firewall)

4. Results

4.1. Milestones

Basic Version:

- Design system, set up the login method in Health Institutions frontend servers, set up andconfigure the security policy language (Spring Boot Security)

Intermediate Version:

- Design and implement the secure custom protocol. Ensure secure communication via TLS, Use asymmetric cryptography to authenticate the connection establishment and symmetric cryptography to guarantee integrity and confidentiality in communication.

Advanced Version:

- Backup servers.

5. References

Spring io

Spring Initializer

Spring Boot Rest Tutorial

Spring Boot Security

Spring Security Tutorial

Rest Template Framework

Thymeleaf

Spring Boot Form Validating

KeyStore

Keytool

SSL Certificate

Ubuntu Server VM

Ufw firewall