MINISTRY OF EDUCATION AND RESEARCH OF REPUBLIC OF MOLDOVA
TECHNICAL UNIVERSITY OF MOLDOVA
FACULTY OF COMPUTERS, INFORMATICS, AND MICROELECTRONICS
DEPARTMENT OF SOFTWARE ENGINEERING AND AUTOMATICS

SanatOS

Project Report

Mentor: Mihai Găidău, university assistant,
Students: Vlad Ursu, FAF-212
Botezatu Marius, FAF-212
Bucătaru Daniel, FAF-211
Ciumac Alexei, FAF-212
Telug Anatolie, FAF-212

Chișinău, 2023

Abstract

Web-based medical card applications play a critical role in healthcare, demanding a heightened focus on security to safeguard sensitive patient information and ensure regulatory compliance. This abstract provides a comprehensive overview of crucial considerations and strategies for developing secure web-based medical card applications.

Web-based medical card applications serve as a vital link in the healthcare ecosystem, facilitating the secure storage and retrieval of patient medical records and sensitive information. This abstract delves into key aspects of secure web-based medical card application development, including:

- **Identity and Access Management**: Robust authentication methods, multi-factor authentication (MFA), and strict access controls ensure that only authorized healthcare professionals can access patient records.
- **Data Encryption**: Strong encryption protocols should be implemented to protect patient data both in transit and at rest, meeting the rigorous security standards demanded by healthcare regulations like HIPAA.
- **Patient Consent and Authorization**: Establishing clear mechanisms for obtaining patient consent and authorization ensures that medical records are accessed and shared in compliance with patient preferences and legal requirements.
- **Secure User Interfaces**: Employing secure design principles, such as input validation, to protect against vulnerabilities like Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF).
- **Secure Communication**: Ensuring secure communication channels for transmitting medical data through the application, including using secure messaging protocols and encrypted email.

In conclusion, developing secure web-based medical card applications demands a multifaceted approach, combining stringent security measures, regulatory compliance, and user education. By prioritizing the security and privacy of patient data throughout the application's lifecycle, healthcare organizations can build trust with patients, protect sensitive medical information, and comply with the stringent regulations governing the healthcare sector.

Keywords: security, data protection, authentication, secure design

Content

Introduction **4**

Domain analysis **5**

1 Domain analysis **5**

1.1 Problem Overview 5

1.2 Solution Concepts 6

1.3 Objectives 7

1.4 Functional 8

1.5 Non-functional 9

1.6 CIA: Confidentiality, Integrity, Availability 11

1.6.1 Confidentiality: 11

1.6.2 Integrity: 11

1.6.3 Availability: 11

2 Software Architecture/Diagrams **13**

2.1 Use Case Diagrams 13

2.2 Sequence Diagrams 15

2.3 Activity Diagrams 17

Introduction

In an era characterized by rapid advancements in healthcare technology and the digitization of patient records, the development and implementation of secure web-based medical card applications have emerged as a critical imperative. These applications bridge the gap between healthcare professionals, patients, and medical records, offering convenient access to vital patient information while ensuring the utmost security and compliance with stringent healthcare regulations.

As the healthcare industry continues its digital transformation, web-based medical card applications have become an integral component of modern healthcare delivery. These applications facilitate the secure storage, retrieval, and exchange of patient medical records, allowing healthcare providers to make informed decisions, improve patient care, and enhance the overall efficiency of medical practices. Moreover, they empower patients to take control of their health information, enabling them to access, share, and manage their medical records with ease.

However, with this digital evolution comes a heightened need for security. The sensitive and highly confidential nature of patient data, coupled with the increasing frequency and sophistication of cyberattacks, places a profound responsibility on developers, healthcare organizations, and regulatory bodies to ensure the security and privacy of medical card applications. The consequences of data breaches in healthcare are far-reaching, encompassing not only financial and reputational damage but also endangering patient welfare and violating strict regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in Europe.

This report delves into the multifaceted realm of web-based secured medical card applications, exploring the intricacies of their development, security measures, regulatory compliance, and the evolving landscape of healthcare data protection. By examining the challenges and opportunities in this domain, we aim to provide insights and guidance to healthcare professionals, developers, and policymakers alike, fostering a secure and efficient healthcare ecosystem that places patient privacy and data security at the forefront.

1 Domain analysis

The initial section of the project report provides context by furnishing background details concerning the issue, the relevant domain, and the consequences of this issue within that domain. Furthermore, gaining an understanding of the domain enables the identification of target audiences and allows for customer validation, thereby substantiating the significance of the problem and the project's necessity.

Moreover, it holds importance to place the project within a comparative analysis framework, in comparison to its analogs. This approach enables the project team to underscore the deficiencies in existing analogs and highlight the potential enhancements that the new solution can offer.

1.1 Problem Overview

The healthcare industry is currently experiencing a profound shift towards digitalization, with the introduction of web-based medical card applications representing a significant milestone in the evolution of patient care and medical record management. These applications have the potential to revolutionize the way healthcare providers access and share patient information, offering convenience, efficiency, and improved patient outcomes.

However, alongside these promising advancements come a host of critical challenges and concerns, especially in the context of web-based secured medical card applications. The problem at hand revolves around the need to balance the tremendous benefits of digital healthcare with the critical imperatives of security, privacy, and regulatory compliance.

- **Data Security and Privacy**: One of the foremost concerns is the security of patient data. Medical card applications house a treasure trove of highly sensitive and confidential information, including medical histories, treatment plans, and personal identifiers. Ensuring that this data remains impervious to unauthorized access, cyberattacks, and data breaches is paramount.
- **Regulatory Compliance**: The healthcare industry is subject to a labyrinth of stringent regulations, such as HIPAA, GDPR, and various national healthcare data protection laws. Compliance with these regulations is non-negotiable, and failure to do so can result in severe penalties, legal ramifications, and a tarnished reputation.
- **Interoperability**: The seamless exchange of medical data between different healthcare providers, systems, and applications is essential for comprehensive patient care. Achieving interoperability while maintaining security is a complex challenge.
- **User Experience**: While prioritizing security, it is crucial not to compromise the user experience. Healthcare professionals, as well as patients, must find these applications intuitive, accessible, and efficient to encourage adoption and maximize their potential benefits.

- **Integration**: Integrating these web-based applications with existing electronic health record (EHR) systems, healthcare infrastructure, and various stakeholders while maintaining data integrity and security is a multifaceted problem.
- **Patient Consent**: Striking the right balance between patient control over their data and the necessity of medical professionals to access it is a delicate issue. Developing mechanisms for obtaining and managing patient consent is a challenge in itself.

The development and deployment of web-based secured medical card applications are poised to bring substantial benefits to the healthcare industry. However, addressing the array of challenges related to data security, privacy, compliance, and usability is essential to unlock their full potential while ensuring patient trust and regulatory adherence. This problem overview sets the stage for a comprehensive examination of these issues and the exploration of effective solutions.

1.2 Solution Concepts

These solution concepts represent a comprehensive approach to addressing the security challenges associated with web-based secured medical card applications. Implementing a combination of these strategies can help create a secure and trustworthy platform for managing patient health records and improving healthcare delivery:

- **End-to-End Encryption**: Implement robust end-to-end encryption to ensure that patient data is protected both in transit and at rest. Employ strong encryption algorithms and regularly update encryption protocols to stay ahead of emerging threats.
- **Multi-Factor Authentication (MFA)**: Enforce MFA for healthcare professionals accessing the application, adding an extra layer of security by requiring something they know (password) and something they have (e.g., a mobile device).
- **Blockchain Technology**: Explore the use of blockchain to create an immutable and tamper-proof ledger of patient data access and modifications. This technology can enhance transparency and trust in data management.
- **Secure APIs**: Develop secure application programming interfaces (APIs) with strong authentication and authorization mechanisms, allowing for safe integration with other healthcare systems and services.
- **Secure User Authentication Methods**: Offer modern and secure authentication methods, such as biometrics (e.g., fingerprint or facial recognition), to enhance user experience while maintaining high security standards.
- **Patient Data Consent Management**: Develop a robust system for managing patient data consent, allowing individuals to control how their information is accessed and shared. Ensure that consent records are securely stored and auditable.

1.3 Objectives

The objectives for a web-based secured medical card application are multi-faceted and revolve around providing secure, efficient, and user-friendly management of patient medical records. These objectives typically include:

- **Data Security and Privacy**: Ensure the highest level of data security and patient privacy by implementing robust encryption, access controls, and compliance with healthcare regulations (e.g., HIPAA, GDPR).
- **Seamless Accessibility**: Enable authorized healthcare professionals and patients to access and update medical records securely from anywhere, facilitating timely and informed decision-making.
- **Interoperability**: Ensure interoperability with existing electronic health record (EHR) systems and other healthcare applications, allowing for seamless data exchange among different healthcare providers and facilities.
- **User-Friendly Interface**: Provide an intuitive and user-friendly interface for healthcare professionals and patients, making it easy to navigate, search, and update patient records.
- **Patient Consent Management**: Implement a comprehensive system for managing patient data consent, allowing individuals to control how their information is accessed and shared, in compliance with regulations.
- **Audit Trails and Monitoring**: Maintain detailed audit logs to track user activities and data access, and set up real-time monitoring and alerts for suspicious or unauthorized actions.
- **Integration with Telehealth**: Facilitate integration with telehealth platforms to enable secure virtual consultations while seamlessly accessing patient records during appointments.
- **Emergency Access**: Implement emergency access protocols that allow authorized personnel to quickly access critical patient information in urgent situations, following strict authentication and authorization procedures.
- **Scalability and Performance**: Ensure that the application can scale to accommodate growing numbers of users and patient records without compromising performance or security.
- **Regular Security Audits**: Conduct regular security audits, vulnerability assessments, and penetration tests to proactively identify and remediate security weaknesses.
- **Compliance and Reporting**: Generate compliance reports to demonstrate adherence to healthcare regulations and provide transparency regarding data access and usage.
- **User Training and Support**: Offer training resources and support for healthcare professionals and patients to ensure they can effectively use the application and address any questions or concerns.
- **Incident Response Plan**: Develop and regularly update an incident response plan to swiftly and

effectively respond to security breaches or data incidents, minimizing potential damage.

- **Continuous Improvement**: Continuously gather feedback from users and stakeholders to identify areas for improvement, and regularly update the application to address evolving needs and emerging security threats.

1.4 Functional

The functional requirements of a secure web-based medical record management system encompass a wide range of features and capabilities to ensure efficient and secure management of patient records. Here is an outline of the project's functional requirements:

- **User Authentication and Authorization:**
  - Implement user authentication with secure password policies.
  - Define role-based access control (RBAC) for user permissions.
  - Support multi-factor authentication (MFA) for enhanced security.
- **Patient Record Management:**
  - Allow authorized healthcare professionals to create, view, update, and delete patient records.
  - Enable patients to access and review their own medical records.
  - Implement data validation for record accuracy.
- **Secure Data Storage:**
  - Utilize strong encryption for securing patient data at rest.
  - Implement data integrity mechanisms to protect against corruption and loss.
- **Interoperability:**
  - Support integration with electronic health record (EHR) systems using industry-standard protocols (e.g., HL7 FHIR).
  - Facilitate data exchange between different healthcare providers and systems.
- **User-Friendly Interface:**
  - Create an intuitive and responsive user interface for healthcare professionals and patients.
  - Implement search and filter options for efficient data retrieval.
  - Enable file uploads and document management.
- **Consent Management:**
  - Develop a consent management system for patients to control data access and sharing.
  - Ensure compliance with legal and regulatory requirements for patient consent.
- **Audit Trails and Monitoring:**
  - Maintain detailed audit logs of user activities and data access.
  - Implement real-time monitoring and alerting for suspicious or unauthorized actions.
- **Integration with Telehealth:**

- **Emergency Access:**
  - Implement emergency access protocols with strict authentication and authorization procedures for critical situations.
- **Scalability and Performance:**
  - Ensure the application can scale to accommodate a growing number of users and patient records without performance degradation.
- **Security Measures:**
  - Conduct regular security assessments, including vulnerability scanning and penetration testing.
  - Implement security measures to protect against threats like Cross-Site Scripting (XSS) and SQL injection.
- **Compliance and Reporting:**
  - Generate compliance reports to demonstrate adherence to healthcare regulations (e.g., HIPAA, GDPR).
  - Provide transparency regarding data access and usage.
- **User Training and Support:**
  - Offer training resources and user support to healthcare professionals and patients.
  - Ensure users understand security best practices and responsible data handling.
- **Incident Response Plan:**
  - Develop and regularly update an incident response plan to address security breaches or data incidents swiftly and effectively.
- **Continuous Improvement:**
  - Gather feedback from users and stakeholders for ongoing improvements and updates to the application.

These functional requirements form the foundation of a secure web-based medical record management system, ensuring the application meets the needs of healthcare professionals, patients, and regulatory requirements while prioritizing data security and privacy.

1.5 Non-functional

- **Performance:**
  - Ensure efficient response times for data retrieval and updates.
  - Handle concurrent user access and large datasets without significant performance degradation.
  - Implement load balancing and caching mechanisms for scalability.
- **User Experience (UX):**
  - Design an intuitive and user-friendly interface for healthcare professionals and patients.
  - Prioritize accessibility features to accommodate users with disabilities.

  - Conduct usability testing and gather user feedback to continually improve the user experience.
- **Scalability:**
  - Design the application to scale horizontally and vertically to meet growing user and data demands.
  - Implement auto-scaling capabilities to allocate resources dynamically based on workload.
- **Security:**
  - Ensure data security through encryption, access controls, and secure authentication methods.
  - Regularly update security measures to protect against emerging threats.
  - Conduct regular security audits and penetration testing.
- **Reliability and Availability:**
  - Achieve high availability with minimal downtime for system maintenance.
  - Implement redundancy and failover mechanisms to ensure uninterrupted access to patient records.
  - Develop backup and disaster recovery strategies to safeguard data.
- **Compliance:**
  - Ensure compliance with healthcare regulations, including HIPAA, GDPR, and other relevant standards.
  - Maintain audit trails and compliance reporting capabilities.
- **System Limitations:**
  - Specify system limitations and constraints, such as maximum concurrent users, data storage capacity, and supported file formats.
  - Document any geographical or legal restrictions on data access and storage.
- **Data Backup and Recovery:**
  - Implement regular data backups and automated backup testing procedures.
  - Ensure data can be quickly restored in case of data loss or system failures.
- **Auditability:**
  - Maintain comprehensive audit trails and logs for user activities, system changes, and data access.
  - Ensure audit data integrity and protection from tampering.
- **Documentation:**
  - Create comprehensive system documentation, including user manuals, technical guides, and security policies.
  - Keep documentation up to date with system changes and enhancements.

1.6 CIA: Confidentiality, Integrity, Availability

1.6.1 Confidentiality:

- **Patient Data Encryption:** Implement robust data encryption mechanisms to protect sensitive patient medical records, both during transmission and while at rest. This ensures compliance with healthcare regulations such as HIPAA and GDPR, safeguarding patient confidentiality.
- **Identity and Access Management (IAM):** Employ stringent authentication methods, including multi-factor authentication (MFA) and role-based access controls, to ensure that only authorized healthcare professionals can access patient records. This bolsters data confidentiality by limiting access to those with legitimate needs.
- **Patient Consent and Authorization:** Develop clear and compliant mechanisms for obtaining patient consent and authorization for accessing and sharing medical records. This strengthens confidentiality by respecting patient preferences and legal requirements.
- **Secure Communication:** Implement secure communication channels for transmitting medical data through the application, including encrypted messaging protocols and secure email, reinforcing patient data confidentiality during transit.
- **Data Access Auditing:** Maintain detailed audit logs to track and monitor access to patient records, promoting transparency and ensuring confidentiality through oversight.

1.6.2 Integrity:

- **Data Validation:** Implement rigorous data validation processes to prevent the entry of invalid or malicious data, reducing the risk of data corruption and unauthorized alterations in patient records.
- **Data Integrity Checks:** Employ checksums and digital signatures to verify the integrity of patient data, both in transit and storage, ensuring data remains tamper-proof and reliable.
- **Version Control:** Maintain version control for code and data to track changes and prevent unauthorized modifications, preserving the integrity of medical records.
- **Error Handling:** Develop robust error-handling mechanisms to detect and respond to data corruption or tampering attempts promptly, protecting the integrity of patient information.

1.6.3 Availability:

- **Redundancy and Failover:** Design the system with redundancy and failover mechanisms to ensure high availability. This minimizes downtime in the event of hardware or software failures, ensuring healthcare professionals have continuous access to patient data.
- **Load Balancing:** Implement load balancing to distribute traffic evenly across multiple servers, pre-

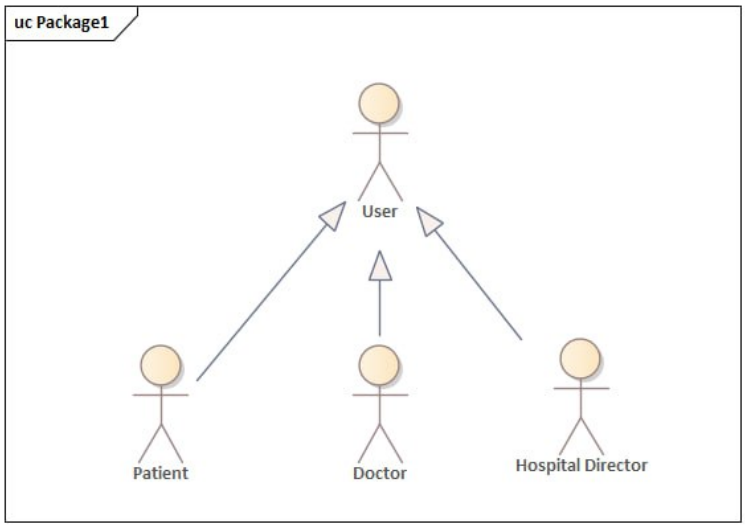
venting overload and maintaining system availability, even during peak usage.

- **Monitoring and Alerting:** Utilize monitoring tools and alerting systems to promptly detect and respond to performance issues or outages, ensuring the continuous availability of the application.
- **Data Backup and Disaster Recovery:** Establish regular data backups and create comprehensive disaster recovery plans to recover the system in case of catastrophic events, preventing data loss and ensuring continued availability.
- **Scalability:** Ensure the system is scalable to handle increased loads and traffic, supporting the growing demands of healthcare professionals and patients without compromising availability.
- **Service Level Agreements (SLAs):** Define and adhere to SLAs for system availability, meeting user expectations and ensuring that healthcare professionals can rely on the system to access critical patient data.

2 Software Architecture/Diagrams

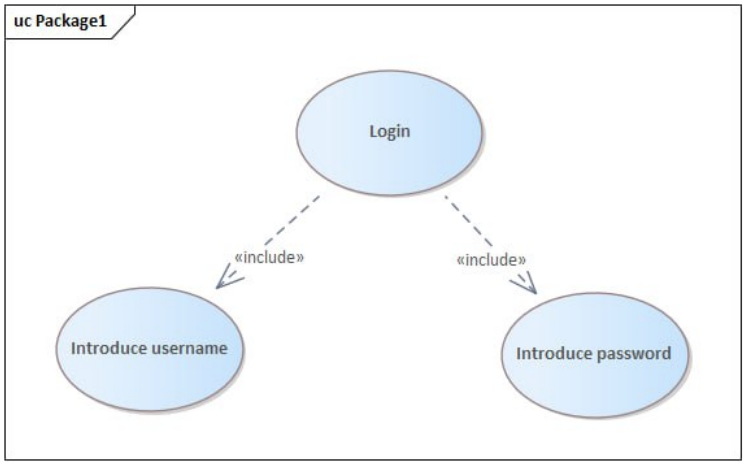
2.1 Use Case Diagrams

In the medical card web application project, use case diagrams illustrate the numerous user roles (actors) and their interactions with the system's primary features (use cases). These use cases include actions like creating, reading, updating, and deleting medical cards, as well as incorporating access control and search features.



In (Figure fig.2.1 is represented the User that for the Medical Card application will be: Patients, Doctors, and The Hospital Director.

Figure 2.1 - Use Case: Users



In (Figure 2.2) is represented the Login system, where user is logging he needs to insert the username and to introduce the password.

Figure 2.2 - Use Case: Login

In (Figure 2.3) is represented the app system and how users interact with it. The Patients can just view their medical history, Doctors can go through the history of all their Patients, modify their history if needed. And the Hospital Director will be responsible for adding or removing Doctors as well as view the number of Patients they are taking on.

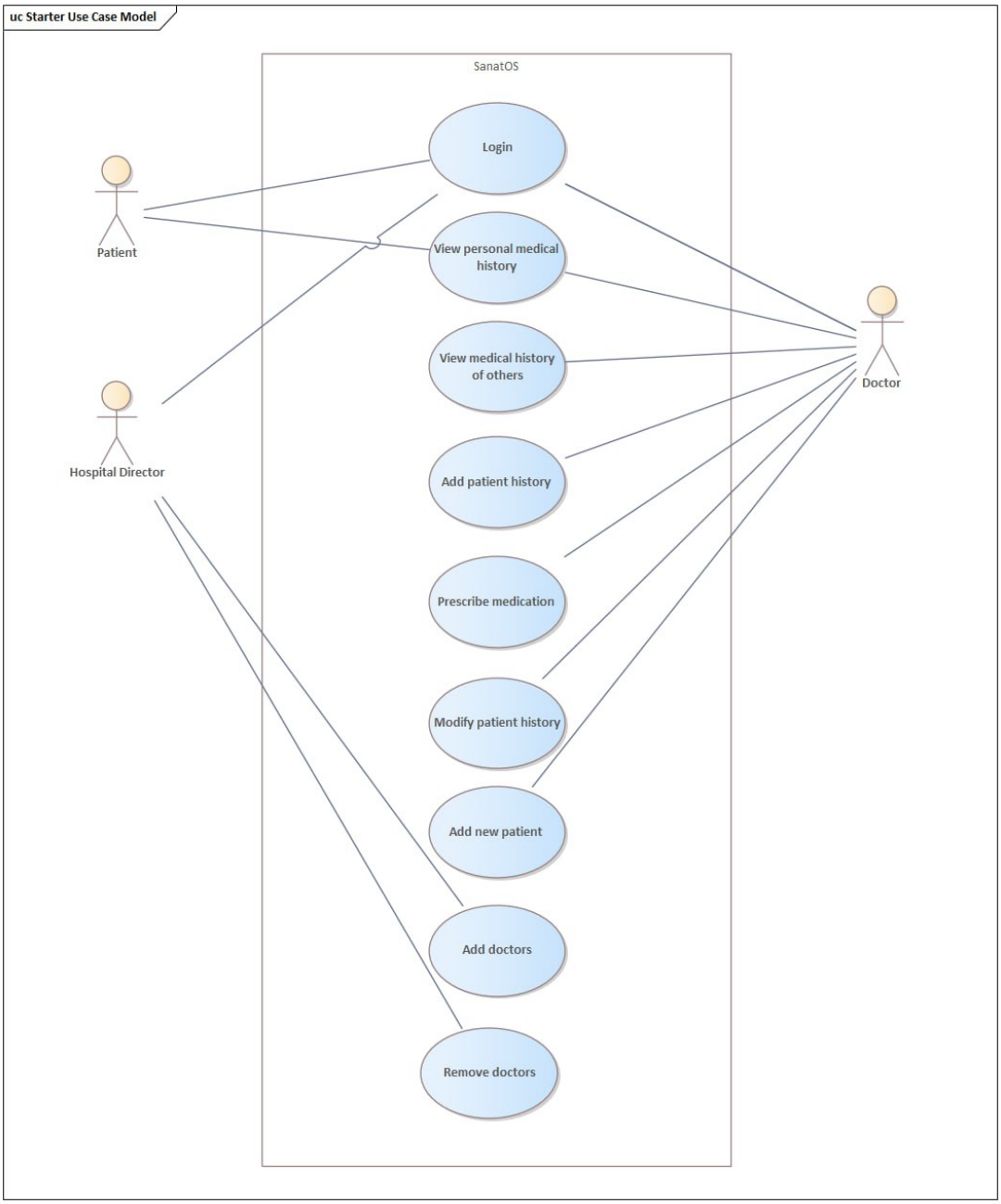


Figure 2.3 - Use Case: System

2.2 Sequence Diagrams

In the medical card web application project, sequence diagrams represent the dynamic interactions between various system components, actors, and objects. These graphs depict the chronological order of messages.

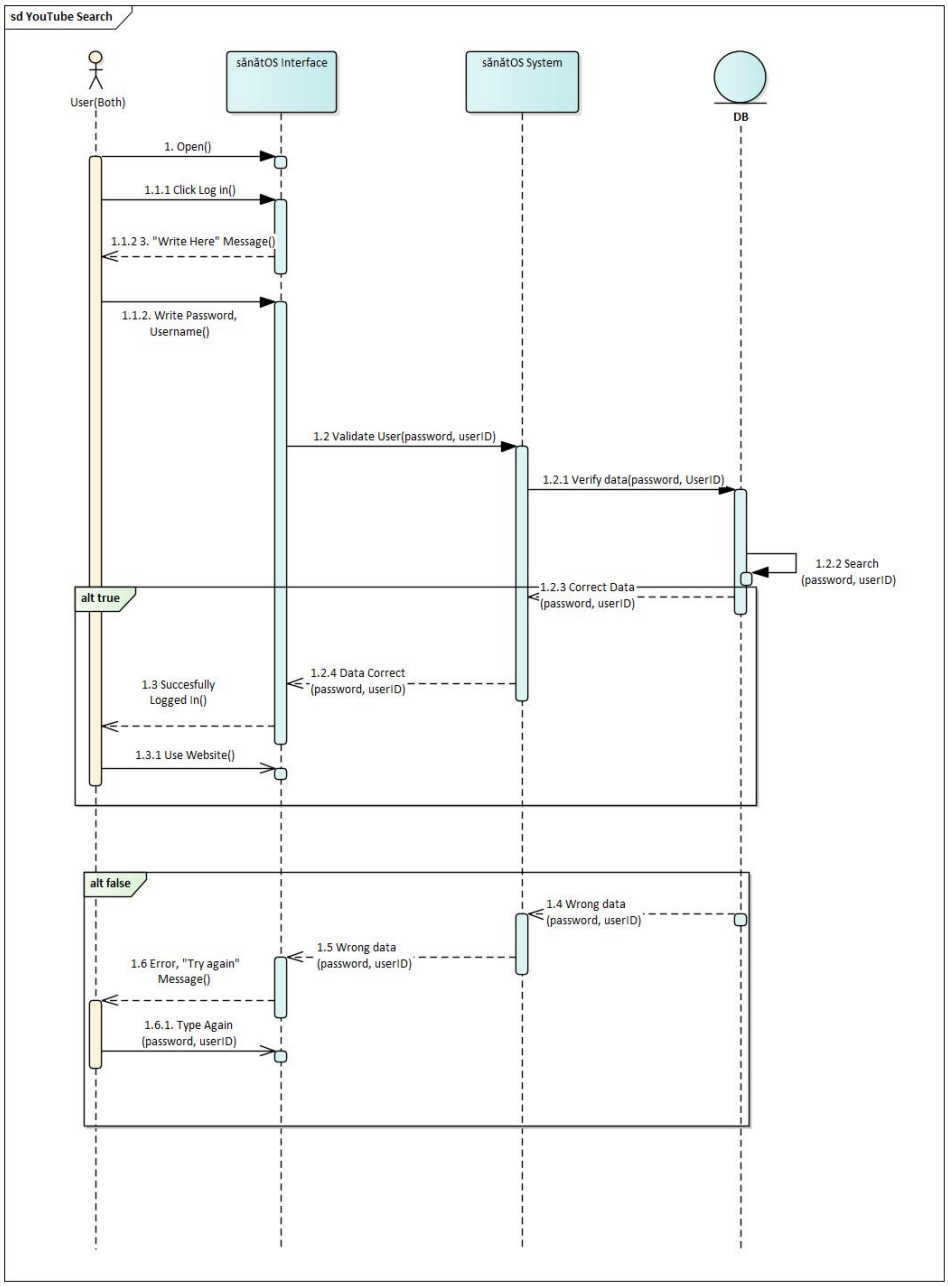
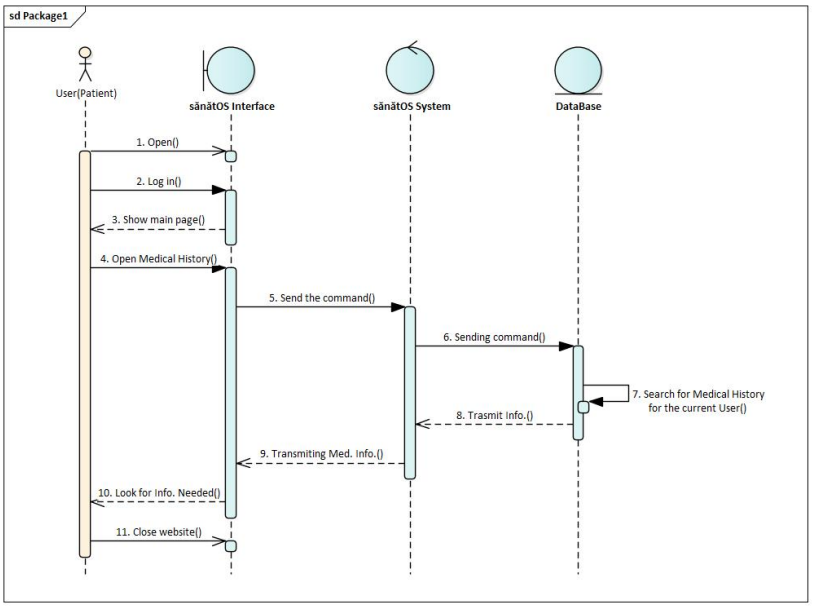
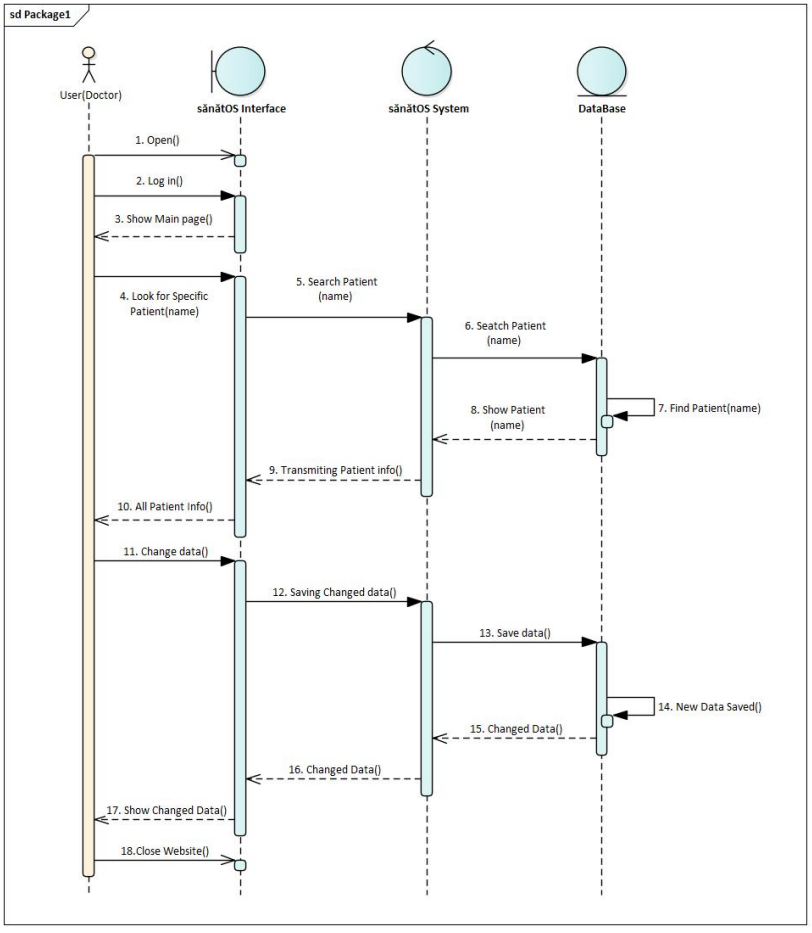


Figure 2.1 - Sequence: Users



This sequence diagram (Figure 2.2) illustrates the actions of a patient when opening their medical history within the system.

Figure 2.2 - Sequence: Patient



This sequence diagram (Figure 2.3) represents the interactions of a doctor within the system.

Figure 2.3 - Sequence: Doctor

2.3 Activity Diagrams

In the medical card web app project, activity diagrams illustrate the flow of activities and actions within the system. These diagrams show the sequential steps that users go through when engaging with the application, such as establishing or changing medical cards, logging in, and searching for patient records.

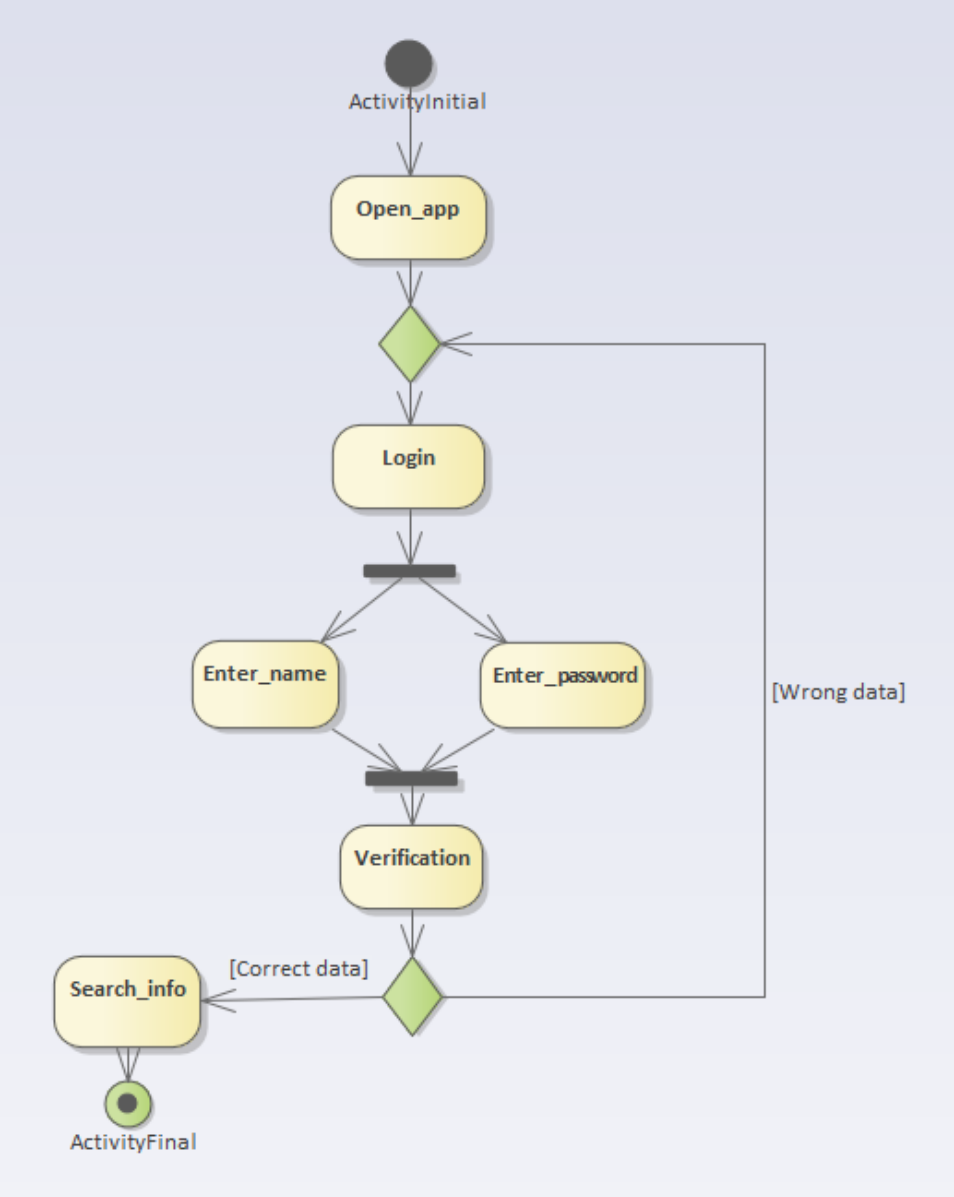


Figure 2.1 - Activity: Login Process

In (Figure 2.1) is represented the Login Process. So after inserting the password and name, in the verification process if the data is entered wrong the user will be needed to reenter it till it will satisfy the verification. After the data is inserted correctly the user will be able to Login successfully.

The activity Diagram in (Figure 2.2) represents the Doctor interaction with the web application .

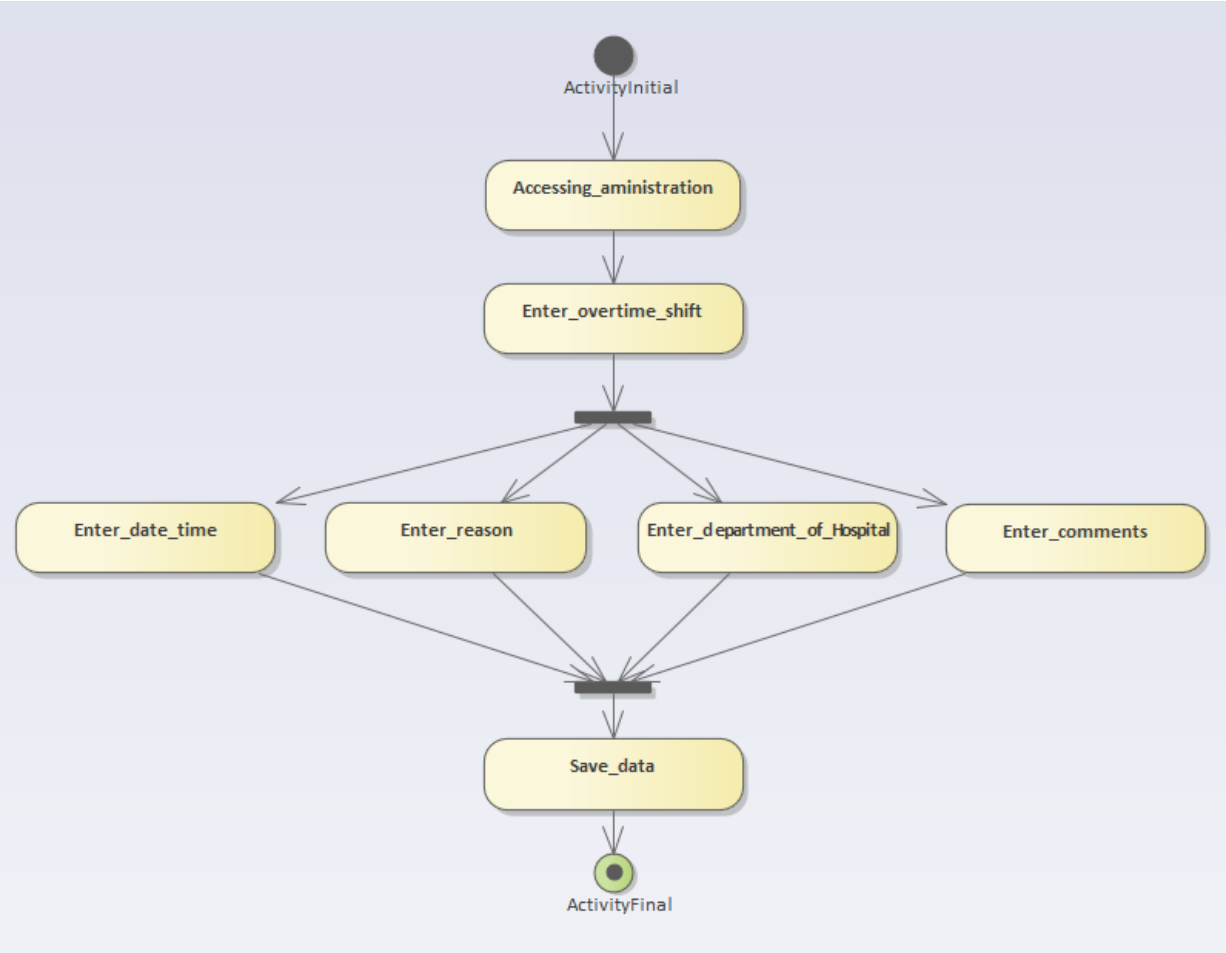


Figure 2.2 - Activity: Doctor Activity

Where he can work with Patients he can choose the date, reason in what department is he present and of course some comments. Of course for security reasons he can't do more, for more permissions the Doctor needs to contact the higher ups.