Issue 14, 2023

https://doi.org/10.23939/sisn2023.14.267

УДК 004.056.5

DATA SECURITY REQUIREMENTS OF THE MEDICAL INFORMATION SYSTEM

Igor Pavliv[1], Nataliia Kunanets[2]

[1] xneelo (Pty) Ltd, SA
[2] Lviv Polytechnic National University, Information Systems and Networks Department,
12, S. Bandery str., Lviv, Ukraine
[1] Email: ihor.i.pavliv@lpnu.ua, ORCID: 0009-0003-0957-0843
[2] Email: nataliia.e.kunanets@lpnu.ua, ORCID: 0000-0003-3007-2462

This document presents the conclusions and insights regarding the requirements for an information system project and its secure component in the context of cloud technologies and the QMS project. It emphasizes significant factors contributing to the project's success, including the necessity to deliver tangible value, ensuring global access to resources, and the use of advanced security technologies. The document discusses the role of aspects such as SSL connections, reliable authentication and authorization mechanisms, password encryption, and CSRF tokens. It also focuses on the importance of constant system updates and high data availability. Ultimately, analyzing the implementation of these requirements in the Quality Medical System (QMS), the document illuminates how, through intensive integration with various third-party services, QMS successfully addressed the defined challenges, providing a high-quality, scalable, and adaptable service.

Keywords: software; cloud technology; private medicine; cloud application security; some medical services.

Introduction

The emergence of private healthcare in Ukraine has been marked by a series of advantages aimed at harnessing state-of-the-art medical equipment. This has become a significant competitive advantage for private medical institutions, which, to some extent, spurred the public sector to renovate its infrastructure. The enhancement of technological resources undoubtedly attracted patients in need of high-quality and efficient medical services.

Over time, there arose a need for a quality electronic support system for clinic operations. Services such as electronic scheduling and the creation of patient electronic profiles were introduced. Electronic scheduling allows patients to book appointments at a time convenient for them, eliminating the need to wait in queues. The establishment of electronic patient profiles enables patients to track their visits and familiarize themselves with the diagnoses provided by the clinic's medical professionals, representing a significant step towards patient comfort.

Furthermore, the state-of-the-art equipment in private medical institutions provided a competitive edge due to superior precision in laboratory analyses, disease diagnosis, and the effectiveness of prescribed treatments, all of which, in conjunction, contribute to better patient recovery outcomes. To solidify their competitive advantages, a quality management system for medical services, known as QMS (Quality Medical System), was implemented, making use of cloud technologies.

Accurate diagnosis was a critical factor in determining the quality of medical care. The presence of highly qualified specialists capable of providing precise diagnoses based on patient data and symptoms became a primary advantage of these institutions.

Knowledge forms the foundation of any medical profession. Professional knowledge acquired through education and continuous improvement is essential for ensuring the delivery of high-quality medical care.

Motivation influences the level of engagement and effectiveness of healthcare professionals. A motivated medical staff is ready to provide high-quality services and continually enhance their professional skills.

Education is essential to keep the knowledge and skills of the healthcare personnel current. New methods and technologies in healthcare constantly emerge, and medical professionals must stay informed about these innovations.

Control is a key aspect of ensuring the quality of medical services. Continuous monitoring and assessment of the activities of healthcare personnel can identify potential issues and assist in their resolution.

Feedback is important for improving service efficiency. Through constructive criticism and feedback, staff can promptly address potential shortcomings in their work and gain insights into the aspects of their work most valued by patients.

Formalation of the problem

In an era marked by increasing reliance on digital health records and the cloud, ensuring data integrity and protection takes center stage. The challenge lies in devising a robust information system project that not only meets the functional requirements but also guarantees the utmost security for sensitive medical data. This problem statement underscores the pivotal role of secure connections and regular updates as key components in fortifying the system against potential threats. As we delve deeper into the article, it will become apparent how these challenges are addressed, providing valuable insights into the data security requirements of the QMS cloud system and, by extension, the broader landscape of medical information systems.

.

Analysis of recent research and publications

The utilization of cloud computing in medical systems represents a significant technological advancement that creates opportunities for optimizing medical processes, improving the quality of patient care, enhancing the accessibility of medical information, and increasing the security of personal data. Foreign researchers Dilip Kumar Sharma, Raja Sarath Kumar Boddu, Narinder Kumar Bhasin, S. Shajun Nisha, Vipin Jain, and Md. Khaja Mohiddin, in their article titled “Cloud Computing in Medicine: Current trends and Possibilities” explore current trends and possibilities of using cloud computing in the field of medicine. They analyze how cloud technologies can ensure the efficiency, accessibility, and economic benefits for healthcare institutions.

The publication highlights the current issue of using cloud technologies in medicine, which can contribute to the improvement of the quality of medical services and the optimization of healthcare facilities' operations. The authors examine current trends in cloud computing and assess the potential applications in various aspects of medical practice. Additionally, the publication provides specific examples of using cloud computing in medicine, enabling readers to better understand the advantages and practicality of such technologies [1].

In the article “Cloud-Based Architecture to Implement Electronic Health Record (EHR) System in Pakistan: a cloud architecture for implementing an electronic health records (EHR) system in Pakistan is described. The authors analyze the possibilities of utilizing cloud technologies to create an efficient, accessible, and secure EHR system in the country [2].

In the article “M-Health Application for Managing a Patient's Medical Record based on the Cloud: Design and Implementation” the procedure for developing and implementing a mobile application for managing patient medical records based on cloud technologies is analyzed [3].

In the article “Application of Computer Big Data Technology in Chinese Medicine Based on Ancient Record Database and Cloud Computing” the results of research on the application of big data and cloud computing in Chinese medicine are presented, based on historical data and a database. Researchers Guodong Lin, Jiexian Chen, Kaiyue Guo, Suhua Xu emphasize the relevance and importance of these technologies, pointing out the need for effective analysis and utilization of historical medical records to improve diagnosis and treatment. The article describes the methodology for processing large volumes of data stored in the Chinese medicine database. The authors use cloud computing to enhance the efficiency of data processing and analysis [4].

The article “Cloud Computing Management Architecture for Digital Health Remote Patient Monitoring” focuses on the development of an information system architecture for cloud computing management in the context of forming a “digital health” system for remote patient health monitoring. An essential aspect of this research is the utilization of cloud technologies to improve the quality and accessibility of healthcare services. The authors of the article, Xuan Su, Lixter Yao, Dennis Hou, Miles San, Jianpu Hou, Jeffrey Ing, Sin-Yu Feng, Po-Ing Chen, Raymond Hou, have developed and tested a new and improved information system architecture based on cloud computing. These processes involve the development of specific algorithms and protocols that would be particularly useful in the context of remote patient health monitoring. The researchers compare the results obtained with existing methods, demonstrating the unique advantages and potential limitations of their information system, as well as suggesting possible ways for further improvement [5].

The article "Privacy Preserving Based Personal Health Records Sharing Using Rail Fence Data Encryption (RFDE) for Secure Cloud Environment" focuses on safeguarding the confidentiality of Personal Health Records (PHR) using the Rail Fence Data Encryption (RFDE) method in a secure cloud environment. The researchers emphasize the importance of utilizing cloud computing technologies to provide access to various healthcare resources while addressing data confidentiality and security issues. The article analyzes a range of important studies related to password protection and data confidentiality in the healthcare sector when using cloud services. They compare the advantages and disadvantages of various methods of safeguarding physical access to data. Additionally, the article proposes a combined authentication procedure based on RFDE models. As a result of the research, the authors assert that their algorithm performs significantly better than previous methods [6].

The article “A study on service-oriented smart medical systems combined with key algorithms in the IoT environment” addresses the issue of improving the efficiency of medical resource utilization and enhancing the diagnostic process through the proposed architecture of an information system for smart medical services using Internet of Things (IoT) technologies. The authors also investigate the data presentation processes in various models, multi-terminal data aggregation algorithms, and resource discovery, the latter of which is based on the hidden factor model. The proposed architecture of the smart medical services information system can contribute to the digitization, intellectualization, and precision of healthcare. The information system aims to improve the utilization of medical resources and make the diagnostic process more efficient, especially in complex business scenarios involving IoT [7].

In the publication titled “Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain” the authors analyze a developed Electronic Health Records (EHR) system that is based on cloud technologies, utilizing an attribute-based cryptosystem and blockchain technology to ensure data security.

Strengths of the publication:

- Relevance of the Problem: Considering the widespread adoption of cloud technologies and electronic health records, the issue of medical data security has become increasingly critical.
- Innovative Approach: The authors employ an attribute-based cryptosystem and blockchain to safeguard data, enabling a high level of security and access control.
- Detailed System Description: The publication provides a clear explanation of the information system's architecture, as well as the principles of operation of the attribute-based cryptosystem and blockchain technology.

However, the publication exhibits certain limitations:

- Practical Application Constraints: The authors do not provide specific examples of how their system can be implemented in real-world scenarios or integrated with existing medical systems.
- Lack of Effectiveness Evaluation: While the authors claim that their approach ensures high-level security, they do not furnish evidence or statistical data to substantiate their assertions.
- Comparison with Alternative Solutions: The publication does not conduct an analysis of other possible technologies and approaches for ensuring medical data security, thereby preventing readers from assessing the advantages of the proposed solution compared to others.

In summary, the publication presents an intriguing and innovative approach to securing electronic medical records using attribute-based cryptography and blockchain technology. However, the article lacks information regarding the scalability of the information system. We consider such an approach relevant for implementation in our own system development, as it would facilitate adaptation to varying levels of complexity in medical systems and user volume [8].

The publication titled "A Comparative study on Securing Electronic Health Records (EHR) in Cloud Computing" is dedicated to comparing various methods of ensuring the security of electronic health records (EHRs) in a cloud environment. The authors focus on analyzing and contrasting various cryptographic techniques and access mechanisms for safeguarding EHRs when utilizing cloud services.

Strengths of the publication:

- Relevance of the Topic: The storage and processing of medical data in cloud environments are becoming increasingly prevalent, leading to a growing need for data protection. The authors' research addresses this pertinent issue.
- Detailed Analysis: The authors conduct a thorough analysis of different cryptographic methods and access mechanisms, examining their advantages and disadvantages.
- Comparative Approach: The application of a comparative analysis allows the authors to identify the most effective methods for securing EHRs in the context of cloud services.

Overall, the publication "Comparative Study of Electronic Health Record (EHR) Security in Cloud Computing" constitutes a significant contribution to the field of medical data protection in cloud environments. The authors provide a detailed comparative analysis of various cryptographic methods and access mechanisms that can be employed to ensure the security of EHRs [9].

In the publication titled "Smart healthcare systems on improving the efficiency of healthcare services" the implementation of smart healthcare systems for improving the efficiency of medical services is discussed. The authors explore contemporary trends, challenges, and potential solutions in this domain, leveraging technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and mobile applications.

The article analyzes approaches to addressing a critical issue – the enhancement of medical service efficiency, which is a pertinent concern in the modern world. The authors examine the possibilities offered by different "smart healthcare" information systems, including the use of IoT, AI, and mobile applications, contributing to the coverage of a wide spectrum of technologies and solutions. The article provides several practical examples of utilizing "smart healthcare systems", illustrating their potential benefits when implemented in real-world scenarios [10].

Product requirements

The Quality Management System (QMS) for medical services is a set of procedures aimed at systematic control and evaluation of the quality of provided medical services. This system allows healthcare institutions to monitor compliance with quality standards, identify ways to improve them, and detect and rectify issues that arise during the provision of medical services.

At the core of the QMS is the establishment of a culture of continuous quality improvement in medical services. This means that every healthcare professional, from doctors to laboratory technicians, considers it their duty to actively seek ways to enhance the quality of the services provided.

The use of QMS facilitates the implementation of systematic management procedures to enhance the quality of healthcare services. This includes processes for staff training and motivation, the implementation of control and assessment mechanisms, and the provision of feedback for continuous improvement of service delivery mechanisms through the use of information technologies and systems.

The proposed information system for the healthcare sector will be based on the utilization of QMS and should be developed as a Software as a Service (SaaS) product, taking into account the specific features of healthcare institutions in Ukraine and adhering to the concept of Minimal Viable Product (MVP), which allows focusing on its key functional features.

Structurally, the information system should consist of two main components: the Front End and the Back End. The Front End, responsible for user interaction, will be implemented in TypeScript using the React library to quickly create an intuitive and user-friendly interface.

The Back End, responsible for data processing and database interaction, will be developed in Ruby programming language using the popular Ruby On Rails framework. This framework ensures rapid and convenient development and enjoys strong support from the developer community.

The information system is planned to be deployed on a dedicated server from the cloud service provider Digital Ocean, with the following system parameters: 1 vCPU, 2GB of RAM, and 50 GB of disk space. It will use the Ubuntu server operating system, the latest stable version, to ensure reliability and stability.

The primary data storage solution for the information system should be a PostgreSQL database, which efficiently handles large volumes of information. For file storage, Amazon S3, an object storage service, is intended for storing and protecting necessary data volumes, including data lakes, cloud technologies, and mobile applications.

As a cloud service, the information system should provide global access to its resources, allowing users to access it from anywhere with internet connectivity.

Medical facility staff work with confidential medical data and patient personal information, and their storage and security are top priorities of the information system. To ensure secure connections, the system will use the Secure Sockets Layer (SSL) protocol from the automated certificate authority Let's Encrypt, which provides free SSL certificates for websites. SSL certificates establish encrypted connections between the user's web browser and the server, enhancing data transmission confidentiality.

A crucial requirement for the designed medical system is to ensure a reliable user authentication and authorization mechanism. This process will be realized by assigning a unique login and password to each user, granting access to the information system upon their input. This authentication process involves multiple critical security elements, which will be analyzed in more detail later.

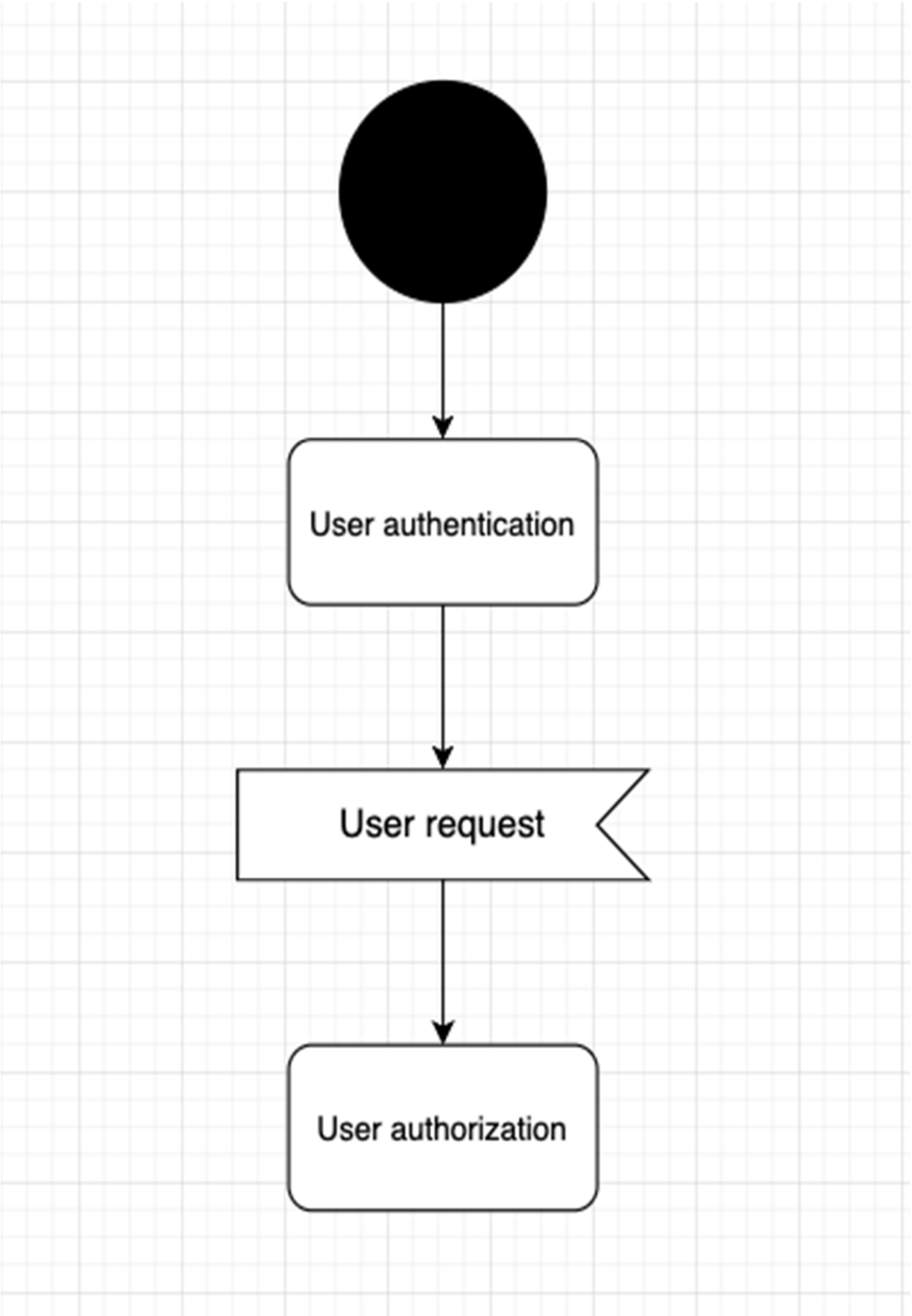

Fig. 1. User Authentication and Authorization

First and foremost, it is imperative to note that the user-entered password must be stored in the system not in plain text but in an encrypted form, significantly enhancing the security of the information system. The utilization of BCrypt for generating an encrypted password hash is a recognized cybersecurity practice. BCrypt is a reliable hashing algorithm that offers a high level of protection against various types of attacks, including rainbow table attacks.

When a user performs the login algorithm in the information system, the password entered by them is encrypted using BCrypt and compared with the already stored encrypted password in the database. This approach ensures that information about the user’s original password does not leak from the system, and the password remains inaccessible to potential attackers.

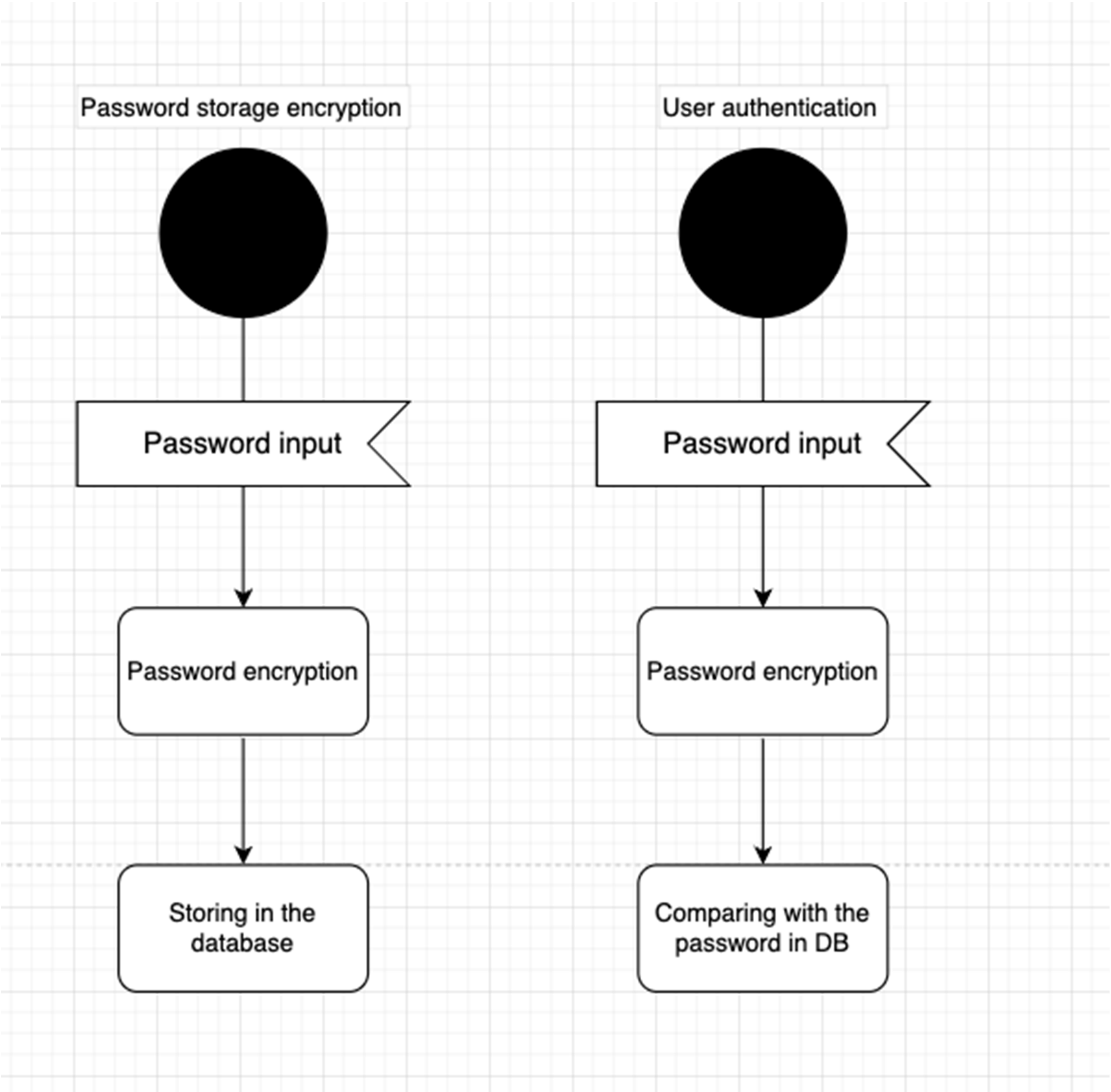

Fig. 2. Password encryption

However, it should be noted that the presence of a reliable authentication mechanism is just one element of the overall security strategy for the designed information system. Other important factors include secure data storage, access control, and regular security audits. The combination of these factors forms a multi-layered security system that contributes to robust protection against potential cyber threats.

Another equally important aspect of secure user authentication in the designed information system is the regular updating of encryption algorithms and authentication mechanisms. Since cybercriminals are constantly developing new techniques and attack methods, it is necessary to continually enhance security mechanisms to guard against the latest threats. The information system should support up-to-date security procedures, including the periodic updating of encryption algorithms and authentication strategies.

Authentication is just one of the stages of user service. After successful authentication, proper authorization must be ensured to grant users access only to resources and services permitted for them. This process includes access control to various parts of the information system based on user roles and privileges.

The information system’s security procedure relies on the use of tokens to prevent Cross-Site Request Forgery (CSRF) attacks. This token serves as a crucial protective measure to prevent forged requests from other sites. After successfully authenticating the user, the system generates a temporary CSRF token, which is returned to the user and used for authenticating their subsequent requests to the server.

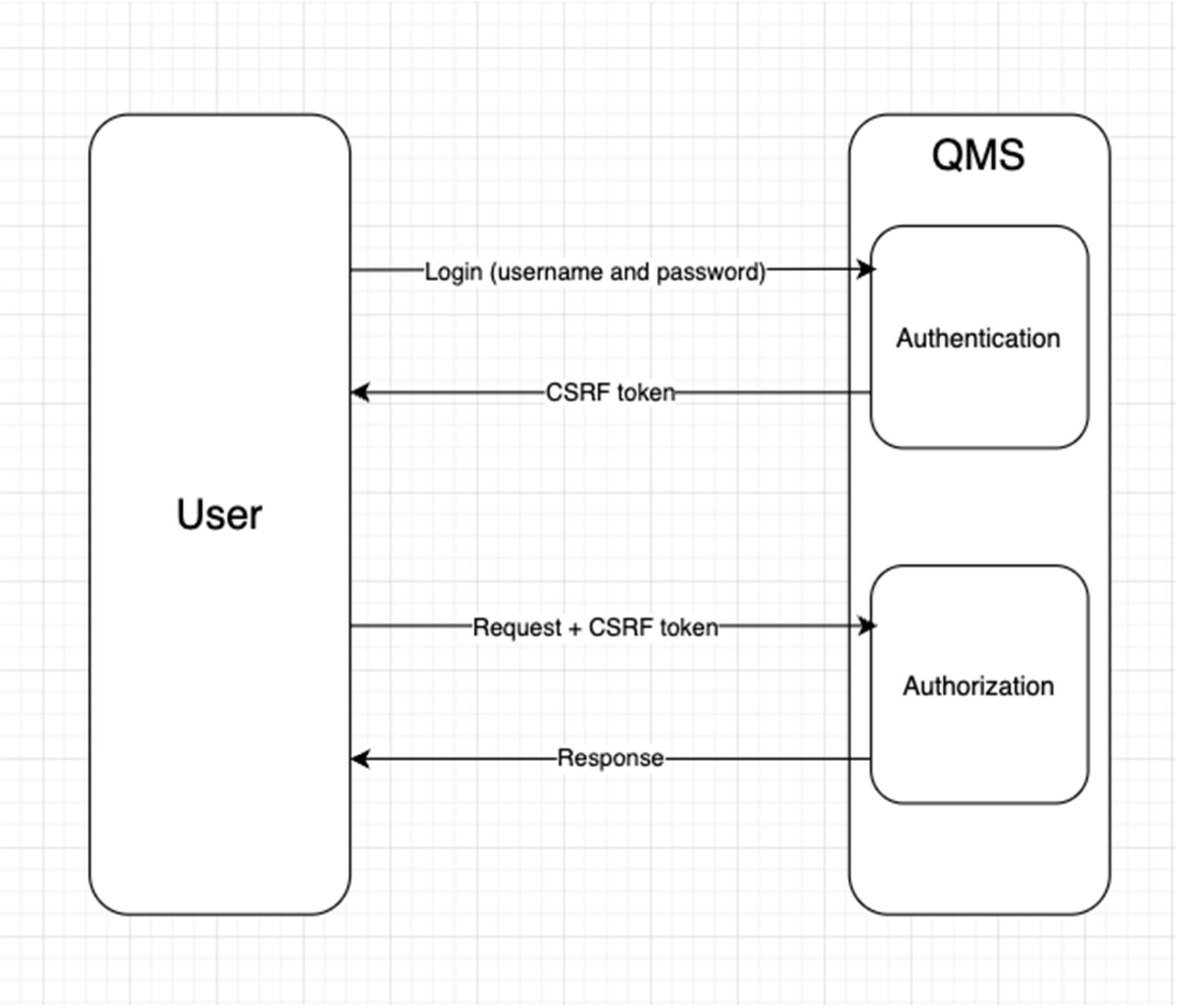

Fig. 3. The operating principle of CSRF authentication tokens

The use of CSRF tokens entails that each request sent to the server contains this unique token, which the server identifies for executing that specific request. Even if an attacker manages to steal a user’s session identifier, they will still be unable to cause harm without the corresponding CSRF token. The token is continuously validated for temporality, providing an additional level of security, including protection against “session hijacking” and “replay attacks”.

This allows users to safely utilize the services of the information system without having to enter their credentials (login and password) with each new request to the server. Instead, the system associates their session with the appropriate CSRF token, which is sent in every request to the server. CSRF tokens have a temporary nature and are refreshed after a certain period of time or after the user's session expires. This serves as an additional protective measure against potential CSRF attacks.

The operation of the information system is centered around ensuring security in the field of information technologies. Regular system updates, including package updates, programming language version updates, and other components, assist in adhering to the latest security standards. These measures are aimed not only at ensuring the reliability of the system's operation but also at preventing possible attacks that could be provoked by vulnerabilities in older versions of the software.

In addition to protecting patients' data from external intrusions, the foundation of the system's reliability lies in ensuring the integrity and availability of data. Various information technologies and architectural solutions are used for this purpose, enhancing the system's resilience to failures and ensuring its stable operation. For instance, to ensure high data availability, database backup and recovery mechanisms are employed to prevent data loss in the event of technical failures or critical situations. The operation of the medical information system stands out due to the need for strict access control levels for data. Based on the principle of "least privilege", each user or group of users has access only to the data necessary for performing their duties. This not only helps maintain information confidentiality but also reduces the risk of unintentional data distortion or destruction.

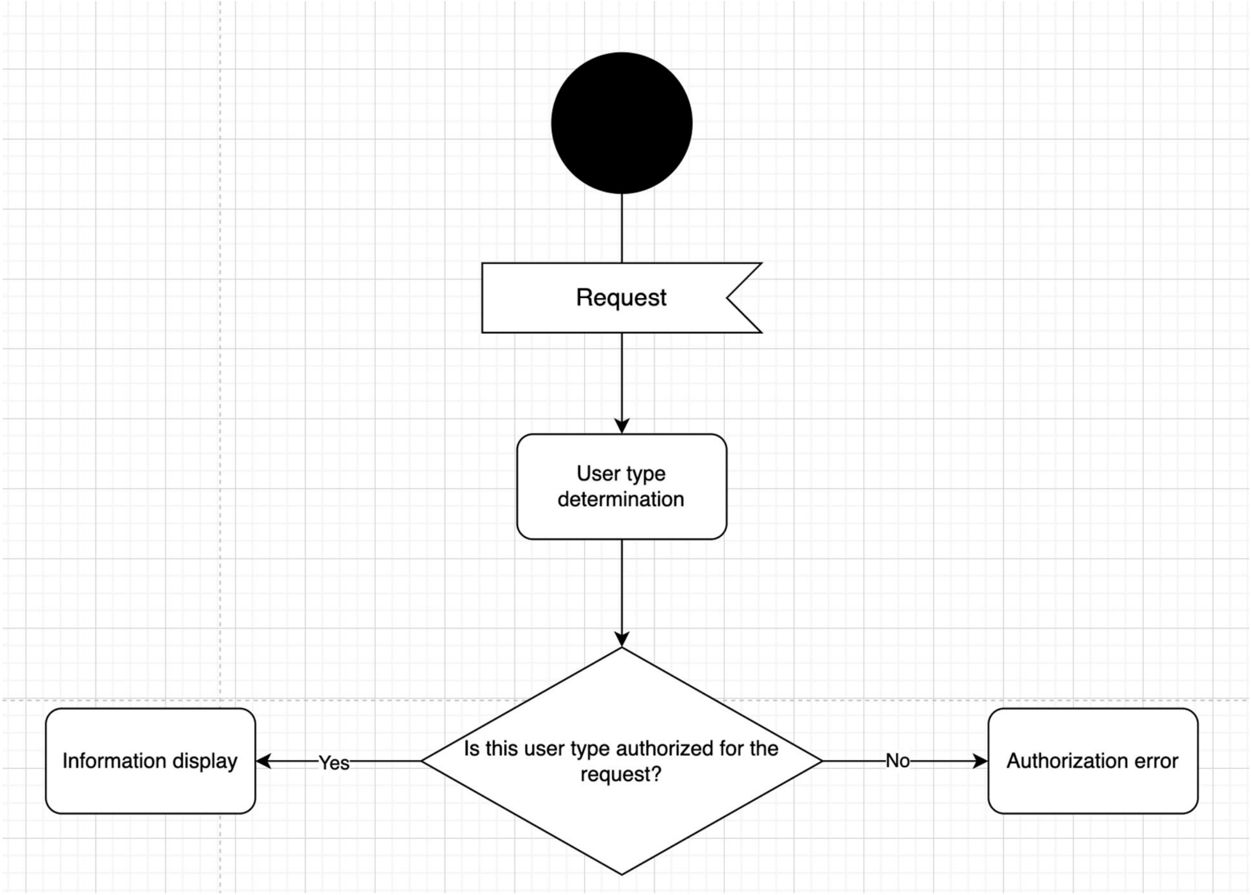

Fig. 4. User-type-based authorization

All these measures contribute to maintaining a secure environment for users, ensuring the confidentiality and integrity of their personal and medical data.

The development and maintenance of secure information systems, especially in the medical field, require continuous improvement and investments. The designed information system will adhere to the best practices and standards in cybersecurity to ensure the security of users and their data.

The overall architecture of QMS and external services

In the process of creating the information system, we actively employed the Minimal Viable Product (MVP) principle, which is based on a limited core of functional capabilities that can be used to test key hypotheses and validate ideas. This approach allowed us to focus resources on addressing the key issues of the target audience and expedite the market research process.

A significant portion of the development of the information system is directed towards integration with various existing market services. This decision was driven by several factors:

Firstly, it enables us to concentrate on the core aspects of the information system, delegating the resolution of more standard tasks to third-party services, such as email distribution, server configuration for the application, analytics collection, error tracking, and file storage.

Secondly, many third-party services offer scalable solutions, allowing for easy adaptation to the growing needs of users.

One example of such delegation is the choice of a virtual server. We concluded that it is cost-effective to use a paid service, as it provides confidence in reliability and stability. The price of such a service is reasonable and justifiable given the value it offers. This service includes additional features, such as automated data backup and server settings snapshots, access to monitoring functionality, and many others that can be easily implemented as the software product expands and develops.

Services that provide data storage, device monitoring, payment transaction processing, marketing, and analytics can be seamlessly integrated into the designed information system. This significantly reduces development time and allows us to use ready-made solutions with guaranteed reliability and efficiency.

An essential aspect of managing the information system is ensuring its continuous operation and stability. To achieve this, various mechanisms of automated control and recovery have been implemented. For instance, automatic data backup creation and server settings are not only safeguards against data loss due to unexpected failures or errors but also enable rapid system restoration to normalcy after such events.

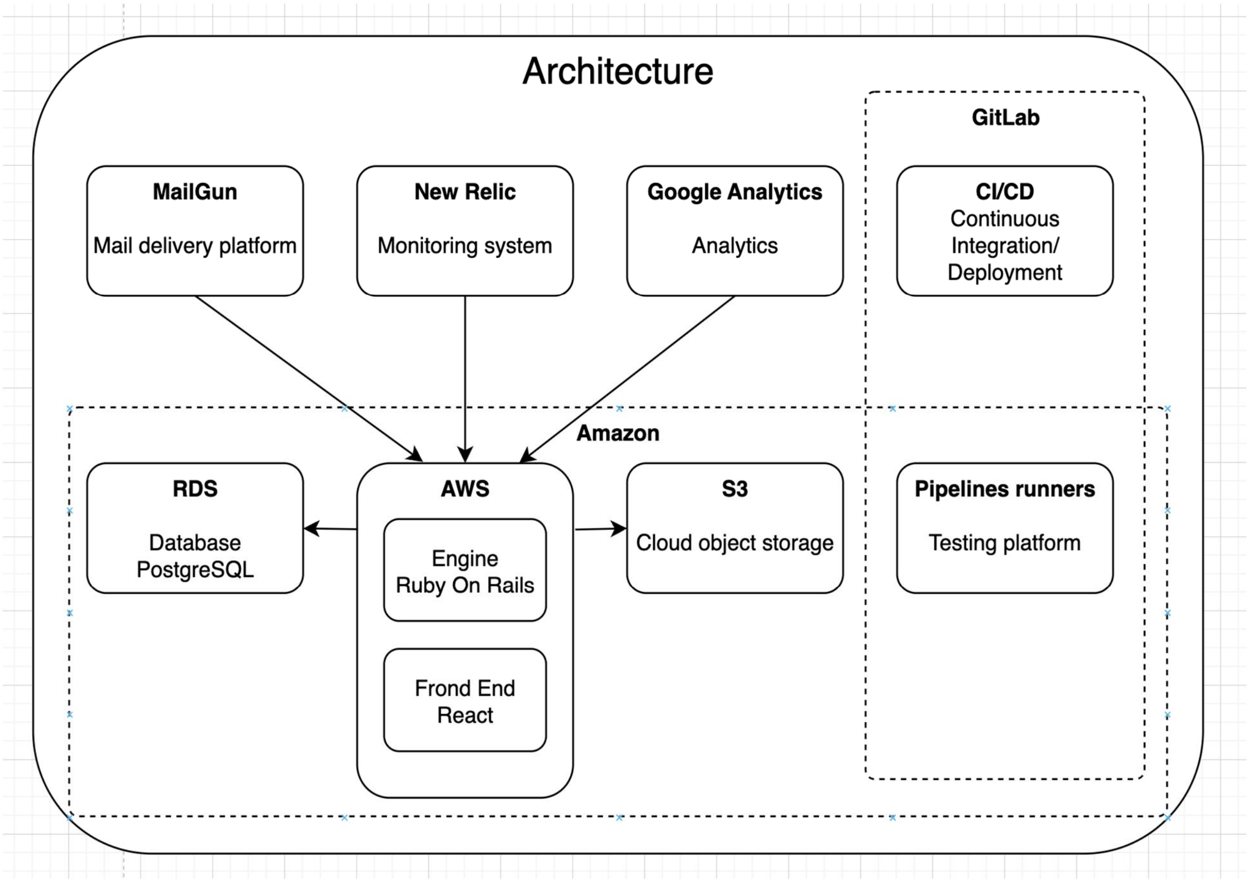

Fig. 5. General Architecture of the Information System

The development of a proprietary email system can be costly and time-consuming, especially when the need for a high level of security, confidentiality, and message delivery reliability is paramount. Since communication with users is a vital component of the healthcare quality management system, the decision was made to utilize a specialized service for email message processing – MailGun.

MailGun is a scalable email service that provides powerful APIs for sending, receiving, and tracking email messages. This solution allows us to perform all necessary tasks related to email without the need to create and maintain our own email server.

By using MailGun, we can send email notifications for various actions, such as user registration, password changes, important system updates, and other critical events. Additionally, MailGun provides detailed reports on email deliveries, including tracking of opens, bounces, and more, which helps us analyze and improve the effectiveness of our communication.

The importance of effective monitoring in the field of digital service provision cannot be overstated. Frequent errors, high peak loads, or any deviations from the normal operation of the information system can significantly undermine the user experience and affect the service's reputation. In this context, tools for monitoring and diagnostics that provide real-time observation of system activity become indispensable for optimizing service performance and maintaining its quality at an appropriate level.

In the designed information system, we utilize the web application New Relic, one of the most powerful monitoring systems on the market. It offers a comprehensive toolkit for tracking various parameters of the information system's operation, including server load, response time, and errors.

An essential component of the web application is the section displaying error statistics, which includes information about the most frequently occurring errors, each accompanied by a detailed description. This enables the identification and resolution of issues in the functioning of the information system at an early stage, enhancing its stability and ultimately improving user convenience.

The use of New Relic software on cloud platforms as a "software as a service" principle helps to maintain the quality of the information system at a high level. It also allows for forecasting and addressing potential problems before they impact user experience.

Google Analytics is a globally recognized service that provides advanced analytical capabilities for monitoring websites and applications. This tool is widely used by cloud system developers to collect user data and analyze their behavior.

One key aspect of Google Analytics is its ability to gather geographical information about users, including their country and city of residence. This information helps understand the geographic distribution of users, which is essential for effective marketing campaign planning and strategic development.

Google Analytics provides detailed data on session duration and visited pages. This enables the study of user behavior patterns and the identification of the most attractive parts of our product. This approach allows the identification of weaknesses in the information system and potential opportunities for improvement.

The compiled and analyzed data provided by Google Analytics is highly valuable for the marketing department. It allows for a deeper understanding of target users, optimizing marketing strategies, adapting content to user needs, and ultimately ensuring more effective user engagement and satisfaction with the service.

GitLab, as a Git web repository that offers both free open and private repositories, serves as the primary code repository for our project, providing centralized and organized storage for all code versions. This significantly simplifies the version management process, as it provides clear structures for tracking code changes, thereby helping to avoid conflicts between processes of different developers.

An important feature of GitLab is its support for the procedure of transferring functionality from one branch to another (merge requests), enabling developers to work in parallel on the code without conflicting with the code of other team members. This ensures comfortable and efficient collaboration among developers.

Moreover, by utilizing Continuous Integration (CI), we can automate the code verification process before integration. The CI system continuously performs various code testing processes, including vulnerability assessment, ensuring the reliability and security of our product.

In combination with Continuous Delivery (CD), which automates the process of delivering changes to the production environment, these approaches allow for the rapid and reliable deployment of new versions of the developed software product. This guarantees that any changes or enhancements made to the code are quickly implemented into the final software product, improving its quality and ensuring timely bug fixes and feature additions.

Conclusions

The emergence of private healthcare in Ukraine has become a significant factor in the substantial improvement of medical services, associated with the utilization of modern equipment and information technologies. These changes have had a positive impact on the development of state medical institutions, prompting the renovation of infrastructure to attract patients seeking high-quality medical services.

The development of an information system, grounded in the management of the quality of medical services and the use of cloud technologies, contributes to the enhancement of technological processes supporting the delivery of medical services and the improvement of their quality. The functionality of the designed information system allows for a meticulous analysis of the procedures for delivering medical services, tracking errors in real-time for prompt correction, and facilitating the planning and management of medical services. During the development of the system, considerable attention has been focused on ensuring the protection of user personal data and medical information.

One of the essential features of the information project is its ability to provide tangible value to its users and stakeholders. This value may manifest as more efficient service delivery, reduced time and resource expenditures, or improved service quality. In the modern world, where boundaries are becoming less visible, projects demand global access to their resources. This implies that the system should be accessible to users from anywhere globally, provided they have internet connectivity.

A crucial characteristic for ensuring secure system operation is the use of SSL connections, which help secure the transmission of data between the client and server. Additionally, a reliable mechanism for user authentication and authorization is essential, ensuring individual access to system resources.

Furthermore, the encryption of user passwords helps protect personal data from unauthorized access, while the use of CSRF tokens ensures secure user session maintenance, eliminating the possibility of cross-site request forgery.

Regular system updates, including package updates, programming language version updates, and other components, aid in maintaining system stability, security, and performance. Ensuring high data availability through database backup and restoration is a critical aspect of any system, especially in the context of critical medical data.

The Quality Management System (QMS) has successfully met these requirements, creating a reliable and secure information system through intensive integration with various third-party services. This integration has allowed QMS to focus its efforts on key aspects of the system, delegating the resolution of more standard tasks to third-party services. Consequently, QMS provides high-quality service, ensuring rapid scalability and adaptation to the growing needs of users.

References

1. Sharma, D. K., Boddu, R. S. K., Bhasin, N. K., Nisha, S. S., Jain, V., & Mohiddin, M. K. (2021). Cloud Computing in Medicine: Current Trends and Possibilities. https://doi.org/10.1109/ICAECA52838.2021.9675730

2. Sarwar, M. A., Bashir, T., Shahzad, O., & Abbas, A. (2019). Cloud-Based Architecture to Implement Electronic Health Record (EHR) System in Pakistan. https://doi.org/10.1109/MITP.2018.2882437

3. Souiki, S., Hadjila, M., Moussaoui, D., Ferdi, S., & Rais, S. (2020). M-Health Application for Managing a Patient’s Medical Record based on the Cloud: Design and Implementation. https://doi.org/10.1109/IHSH51661.2021.9378744

4. Lin, G., Chen, J., Guo, K., & Xu, S. (2021). Application of Computer Big Data Technology in Chinese Medicine Based on Ancient Record Database and Cloud Computing. https://doi.org/10.1109/ICDSCA53499.2021.9650075

5. Su, H., Yao, L., Hou, D., Sun, M., Hou, J., Ying, J., Feng, H.-Y., Chen, P.-Y., & Hou, R. (2021). Cloud Computing Management Architecture for Digital Health Remote Patient Monitoring. https://doi.org/10.1109/SMARTCOMP52413.2021.00049

6. Bhardwaj, S., Baskar, S., Marakala, V., D, P., Gangodkar, D., & Dhole, S. V. (2022). Privacy Preserving-Based Personal Health Records Sharing Using Rail Fence Data Encryption (RFDE) for Secure Cloud Environment. https://doi.org/10.1109/IIHC55949.2022.10060226

7. Lu, S., Wang, A., Jing, S., Shan, T., Zhang, X., Guo, Y., & Liu, Y. (2019). A Study on Service-Oriented Smart Medical Systems Combined with Key Algorithms in the IoT Environment. https://doi.org/10.23919/JCC.2019.09.018

8. Wang, H., & Song, Y. (2018). A Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. https://doi.org/10.1007/s10916-018-0994-6

9. Ishaq, A., Qadeer, B., Shah, M. A., & Bari, N. (2021). A Comparative Study on Securing Electronic Health Records (EHR) in Cloud Computing. https://doi.org/10.23919/ICAC50006.2021.9594178

10. Poorejbari, S., & Mansoor, W. (2019). Smart Healthcare Systems on Improving the Efficiency of Healthcare Services. https://doi.org/10.1109/ICSPIS48135.2019.9045894

Список літератури

1. Sharma, D. K., Boddu, R. S. K., Bhasin, N. K., Nisha, S. S., Jain, V., & Mohiddin, M. K. (2021). Cloud Computing in Medicine: Current Trends and Possibilities. https://doi.org/10.1109/ICAECA52838.2021.9675730

2. Sarwar, M. A., Bashir, T., Shahzad, O., & Abbas, A. (2019). Cloud-Based Architecture to Implement Electronic Health Record (EHR) System in Pakistan. https://doi.org/10.1109/MITP.2018.2882437

3. Souiki, S., Hadjila, M., Moussaoui, D., Ferdi, S., & Rais, S. (2020). M-Health Application for Managing a Patient's Medical Record based on the Cloud: Design and Implementation. https://doi.org/10.1109/IHSH51661.2021.9378744

4. Lin, G., Chen, J., Guo, K., & Xu, S. (2021). Application of Computer Big Data Technology in Chinese Medicine Based on Ancient Record Database and Cloud Computing. https://doi.org/10.1109/ICDSCA53499.2021.9650075

5. Su, H., Yao, L., Hou, D., Sun, M., Hou, J., Ying, J., Feng, H.-Y., Chen, P.-Y., & Hou, R. (2021). Cloud Computing Management Architecture for Digital Health Remote Patient Monitoring. https://doi.org/10.1109/SMARTCOMP52413.2021.00049

6. Bhardwaj, S., Baskar, S., Marakala, V., D., P., Gangodkar, D., & Dhole, S. V. (2022). Privacy Preserving-Based Personal Health Records Sharing Using Rail Fence Data Encryption (RFDE) for Secure Cloud Environment. https://doi.org/10.1109/IIHC55949.2022.10060226

7. Lu, S., Wang, A., Jing, S., Shan, T., Zhang, X., Guo, Y., & Liu, Y. (2019). A Study on Service-Oriented Smart Medical Systems Combined with Key Algorithms in the IoT Environment. https://doi.org/10.23919/JCC.2019.09.018

8. Wang, H., & Song, Y. (2018). A Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. https://doi.org/10.1007/s10916-018-0994-6

9. Ishaq, A., Qadeer, B., Shah, M. A., & Bari, N. (2021). A Comparative Study on Securing Electronic Health Records (EHR) in Cloud Computing. https://doi.org/10.23919/ICAC50006.2021.9594178

10. Poorejbari, S., & Mansoor, W. (2019). Smart Healthcare Systems on Improving the Efficiency of Healthcare Services. https://doi.org/10.1109/ICSPIS48135.2019.9045894

ВИМОГИ ДО БЕЗПЕКИ ДАНИХ МЕДИЧНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Ігор Павлів[1], Наталія Кунанець [2]

[1] xneelo (Pty) Ltd, SA
[2] Національний університет “Львівська політехніка”,
кафедри інформаційних систем та мереж,
ву. С. Бандери, 12, Львів, Україна
[1] Email: ihor.i.pavliv@lpnu.ua, ORCID: 0009-0003-0957-0843
[2] Email: nataliia.e.kunanets@lpnu.ua, ORCID: 0000-0003-3007-2462

Висвітлено підсумки та висновки щодо вимог до проєкту інформаційної системи та безпекової компоненти в контексті хмарних технологій і проєкту QMS, який акцентує на значущих факторах, що сприяють успіху проєкту, і використанні сучасних технологій безпеки. Документ розглядає роль таких аспектів, як SSL-з'єднання, надійні механізми аутентифікації та авторизації, шифрування паролів та CSRF-токени. Увагу зосереджено також на важливості постійних оновлень системи та високої доступності даних. Аналізуючи реалізацію цих вимог у системі управління якістю медичних послуг (QMS), документ висвітлює, як завдяки інтенсивній інтеграції з різноманітними сторонніми сервісами QMS успішно вирішила визначені проблеми, забезпечивши високоякісний, масштабований та адаптивний сервіс.

Ключові слова: програмне забезпечення; хмарні технології; приватна медицина; безпека хмарних застосунків; якість медичних послуг.