Data Security Mechanisms of the Health E-learning System: Case Study

Lidia BĂJENARU[1,2], Claudiu GURA[3] Ion SMEUREANU[4]
[1] National University of Science and Technology Politehnica Bucharest, Bucharest, Romania
[2] National Institute for Research and Development in Informatics - ICI Bucharest, Romania
[3] Enterprise Architecture, Raiffeisen Bank, Bucharest, Romania
[4] Bucharest University of Economic Studies, Romania
lidia.bajenaru@ici.ro, claudiu.gura@gmail.com, ion.smeureanu@csie.ase.ro

Abstract: E-learning platforms have become a popular solution for education, providing access to high-quality educational content from any place where there are Internet connections. However, these platforms are also the target of cyber attacks as they may contain sensitive data. Security is a critical issue, especially for highly interactive applications based on heterogeneous distributed architectures. The security mechanisms of e-learning systems are primarily meant to protect against illegal access to information so that confidentiality and integrity can be guaranteed. This paper highlights some key security aspects that must be considered in the development and use of an e-learning platform, while proposing a holistic approach to security systems. An ontology-based e-learning platform for health management professionals is presented along with its architectural components, with an accent on the security component and its role in ensuring the optimal and safe use of a system.
Keywords: Data Security, Cyber Attacks, E-learning, Health, Management, Ontology.

INTRODUCTION

E-learning platforms have become a popular solution for education, providing access to high-quality educational content from any place where there are Internet connections. However, these platforms are also the target of cyber attacks as they may contain sensitive data such as the personal information of students, teachers and other participants .

Cyber security threats and attacks are increasing every day, as such, the damage caused by cybercrime is also growing. As a response to these problems but also due to a host of other issues such as the increasingly large volume of data that requires processing and protection, security has evolved a lot in recent years and numerous protection methods have been developed specifically to the field in which they will be applied.

https://doi.org/10.54851/v5i2y202310

Most of these attacks are carried out for direct financial gain (Scheau, 2018; Mihai et al., 2020).

Any security system should comply with CIA concepts (confidentiality, integrity and availability) (Mihai et al., 2020; Anghel et al., 2020; Banciu et al., 2023). Starting from these concepts, a solid foundation can be ensured for the applications that would be developed. Following this model, it can be ensured that authorized persons can only access the data, the services are available and have not been compromised. The most popular attacks are those that target the availability of a service, attacks that affect these services and systems to the point where resources are no longer accessible, thereby affecting normal traffic that leads to applications refusing to respond to real user requests.

A cyber-attack is a type of malevolent action which targets a computer system. There are a number of cyber attacks in today's world and they are categorized by both the target and the methods in which they act (Vevera & Albescu, 2018). There are several types of attacks that target different components of an application, such as authentication security, architecture security, database security, etc. (Gavrila et al., 2020).

One of the emerging technologies that provide security to various systems is blockchain (Chen et al., 2018). Mainly used for cryptocurrencies (Nakamoto, 2008), blockchain technology offers insight into many sectors in addition to the financial and commercial one, such as healthcare, government and education. According to some researchers (Chen et al., 2018; Nikola, 2021) blockchain technology has only found a few use cases in education. Thus, the blockchain can be used primarily for the storage and management of information about degrees, i.e. in credentials. This will make certificates more secure and easier to verify. There are already a number of blockchain-based eLearning solutions that are evolving in this direction. One example is Credly, a platform that offers blockchain-based digital certificates. Also, the University of Nicosia was the first school to manage student certificates obtained from online courses, while MIT and the UK Open University took steps in the same direction with blockchain-based projects.

Using blockchain to create peer-to-peer learning mechanisms allows students to buy and sell courses and teaching materials to their peers in a secure space.

Blockchain has the potential to significantly improve e-learning solutions, offering a number of advantages such as transparency, security and reliability. As blockchain technology continues to develop, a number of new functionalities and improvements are likely to emerge in the architecture of blockchain-based eLearning solutions.

The security of e-learning platforms is essential to protect user data and educational content. E-learning platforms that do not implement security mechanisms are vulnerable to cyber-attacks, which can lead to data theft, content sabotage, or service disruption.

This paper presents among the most frequent attacks on e-learning systems, and ONTO e-learning platform along with its architecture components, with an accent on the security component and its role in ensuring the optimal and safe use of the system, the architecture, and the security components used in its development.

This paper is structured as follows. First it presents an overview of the main types of cyber attacks and a holistic approach to security. The second it sets forth an ontology-based e-learning solution designed for medical management professionals, namely its architectural components, along with some steps the user follows in the learning process are presented, with an emphasis on the authentication and authorization process. The last section concludes the paper.

BASIC SECURITY REQUIREMENTS

The definition of e-learning includes certain basic elements such as: it is an application that runs on a server; the content of the learning system; the network, through which the student will access the learning system, the Internet; the user's system, a computer or a mobile device. Internet access is an essential

component of the e-learning system, which makes it vulnerable, i.e. exposed to information security and privacy threats.

E-learning platforms should ensure the following security aspects: authenticity, access control, confidentiality, integrity, and availability.

Previous studies have shown that learners have expressed privacy concerns related to using online learning environments. The acceleration of the use of emerging digital technologies such as artificial intelligence in education has led to an international trend of using and analyzing data from learning processes. In this sense, UNESCO draws the attention of the international educational community to data privacy in education. Rules and protocols are needed to protect students and teachers not only in national policies but also internationally (UNESCO, 2022).

The concern regarding information security and confidentiality, often neglected by institutions providing online education, became acute with the COVID-19 pandemic and the restrictions in the education system (UNESCO, 2022; Nikou & Maslov, 2021). The studies of (Almaiah et al., 2020; Abbasi et al., 2020) have identified challenges related to e-learning that appear as a result of COVID-19, related to such factors as system use, the attitude of users, and ensuring data security.

The studies that evaluated the security aspects of the most used e-learning software systems such as Moodle, Chamilo, and Ilias identified some aspects related to the security vulnerabilities. Also, they identified how COVID-19 may affect the prevalence of these security vulnerabilities, what fixes are available for current vulnerabilities, and what future enhancements may be considered (Akacha & Awad, 2023). Among the recommendations resulting from this analysis, it is important to mention:

- Implementing secure coding practices and using established software development frameworks;
- Integrating security at every stage; establishment of vulnerability disclosure and reporting mechanisms;
- Timely security updates and patches and guidance on the updating process;
- Accessible security documentation to help users implement and maintain secure configurations;
- Periodic security testing, including penetration testing, vulnerability scanning and code audits;
- Promoting a community of users to contribute to reporting errors.

Defence Against Cyber Attacks

Defence against cyber attacks is an essential part of the security of any e-learning platform. E-learning platforms are the target of cyber attacks because they may contain sensitive data such as personal information of students or instructors.

In general, cyber attacks on e-learning platforms can be classified into the following categories:

1. **Phishing attacks:** Attackers send fake emails or text messages that appear to be from a trusted source, such as an educational institution. These emails or text messages often contain infected links or attachments that can install malware on the victim's computer.
2. **Malware attacks:** These are attacks that attempt to infect e-learning platforms with malware programs such as viruses or spyware. These programs can be used to steal information or to take control of the system.
3. **Denial of service (DoS) attack:** Targets the system resources and as such it overwhelms the system so that the targeted service cannot respond to any other request. A good analogy here will be that of a student that permanently keeps the teacher busy and as such he will not be able to handle the other students at all (Yu, 2014).
4. **Distributed denial of service (DDoS):** The attacks that attempt to block access to e-learning platforms by flooding servers with fake traffic. This type of attack can be very dangerous as it can lead users. A DDoS

attack is launched from a greater number of machines that the attacker controls (for example by using a botnet). Going forward with the same analogy, in a DDoS attack there will be multiple students with malevolent intentions that will keep the teacher extremely busy and as such he will not be able to focus on anything else (Singh & Gupta, 2022; Yu, 2014).

5. **SQL injection attacks:** The attacks that attempt to exploit vulnerabilities in the databases of e-learning platforms to obtain confidential information. This type of attack occurs when a malicious entity successfully executes a SQL query to the database using the input data from the client. For example, in a login form instead of just typing the username it will type a SQL query that (if there are no measures taken against it) will be executed on the server/database (Clarke, 2012).
6. **Cross-site scripting (XSS) attacks:** The attacks that attempt to inject malicious code into the web pages of e-learning platforms to obtain confidential information or to take control of the system. An XSS attack uses third party resources to run code (scripts) in the victim browser. This means that the attack usually inserts a malicious JavaScript payload into the database and that payload is furthermore delivered to other victims/users. For example, if a person is able to create an account with a runnable javascript code as his/her biography, all of the users who will later view his/her profile will be victims to his/her code/script (Fogie et al., 2017).
7. **Man in the middle attack:** A type of attack that happens when the attacker has access to the communications between a client and a server and inserts itself in that stream. One of the most popular attack is session hijacking. In this particular attack, the attacker hijacks a session between a client and a server. For web applications that mostly means stealing cookies that are used to authenticate the client.

Holistic Approach to Security

To ensure maximum security, e-learning platforms, including the one presented in this study, should adopt a holistic approach to security. This means implementing a combination of security measures such as those listed above. It is also important to create a security culture within the organization so that users are highly aware of cyber risks and adopt safe security practices.

A holistic approach to security is an approach that considers all aspects of security, including technology, people, and processes. This approach is essential for ensuring the maximum security of e-learning platforms.

Here are some of the important benefits of a holistic approach to security:

- Increase security: A holistic approach to security can help identify and remediate vulnerabilities in all aspects of an e-learning platform.
- Reduce costs: A holistic approach to security can help reduce security costs by avoiding the implementation of redundant or ineffective security measures.
- Improve efficiency: A holistic approach to security can help improve the efficiency of security operations by centralizing processes and resources.

By implementing a holistic approach to security, eLearning platforms can help protect user data and platform content from cyber attacks.

As a starting point in the implementation of a holistic approach to security:

- Developing a security plan that takes into account all aspects of security.
- Implementation of appropriate security measures.
- Creating a culture of security within the organization.
- Monitoring and regularly evaluating the security of the e-learning platform.

E-LEARNING SECURITY CASE STUDY – ONTO PLATFORM

In this section, the ONTO e-learning platform is presented, along with the components of its architecture, with the aim of highlighting the security component and its role in ensuring the optimal and safe use of the system. The security component is responsible for authenticating participants, based on the student's name and password, but also for authorizing and controlling access to resources, depending on the student's role and context.

The e-learning system uses ontologies both for modeling the learning process, and the domain of interest health resources management (HRM), and for organizing and updating specific learning resources (for example: student profile, learning path, and learning objects). It also integrates information from different sources (learning objects, links, websites) to fulfil the requirements of students correlated with their profile. The method used in the design of the system leads to the modeling and automation of the learning environment.

The prototype system offers learning techniques that ensure a structured organization of knowledge, use, and retrieval of the necessary information, as well as new methods of data extraction from the web.

The system proposes the implementation of the personalization concept by taking into account the following aspects that define/ identify the student's profile: knowledge, learning style, learning objective, training level, objective, and context. Also, the personalization process offers solutions for the formalization of knowledge, the evaluation of skills, and the level of training, as well as for feedback.

The e-learning system helps to verify and update knowledge, depending on the student's profile, with notions imposed by the requirements of his professional position. The knowledge offered to students is represented by basic concepts of HRM and information specific to the health system (Băjenaru, 2018; Băjenaru et al., 2016).

The architecture of the ONTO e-learning system

The architecture of the intelligent educational system based on web technologies is a three-layer client-server architecture. The block diagram of this system can be seen in Figure 1.

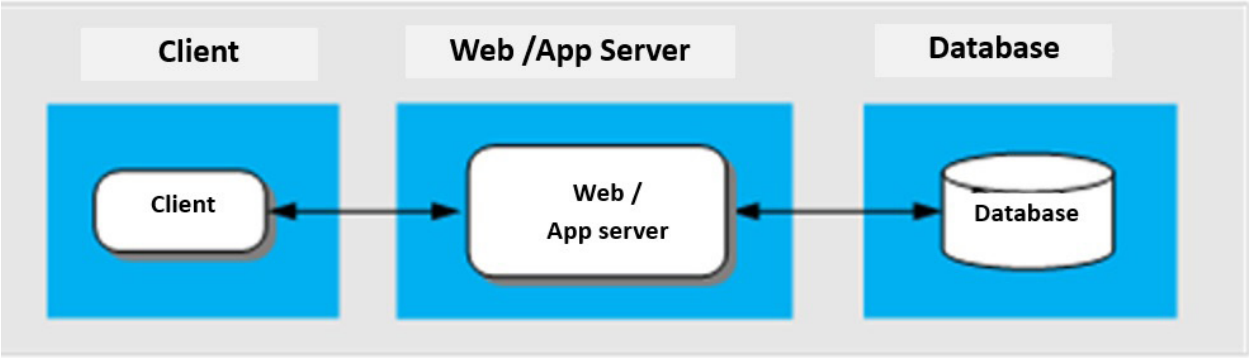

Figure 1. *Block diagram of the system*

The logical architecture integrates:

- The web server that provides the interface with the students and their access to the database;
- The application programs through which the main functions of the system are carried out, providing the necessary capabilities of the training platform;
- The database server that hosts the system's database (educational content, student profiles, and portfolios) and ensures the storage and retrieval of the data necessary to run a course.

The main elements of the logical architecture are the following:

- **Client** – the component used by the student to access the system through a browser;
- **Presentation Level** – ensures the interface with the student but also with the processes corresponding to the student interface;
- **Application Level** – ensures integration with the Presentation and Data levels, running the central logic of the web-based semantic system, specific validations and management of the proposed training model;
- **Data Level** – offers the possibility of integration with data sources and performs data conversions;
- **Data source** – is represented by the system's database with the role of ensuring the persistence of information between participants' training sessions;
- **Security** – ensures the security of participants' access to system resources
- **Operational Management** – offers the possibility to administer and operate the system, through specific „Administrator" type consoles.

The System Components

At the system architecture level, which is the basis for the implementation of the solution proposed in this project, two main blocks are identified, which communicate via the HTTP protocol, using the Internet: the client and the server. Additionally, at the server level, the database server is highlighted with the role of ensuring the persistence of information in the system, communication with it being carried out through the similar ODBC (Open Database Connectivity) protocol. The components of the system are illustrated in Figure 2.

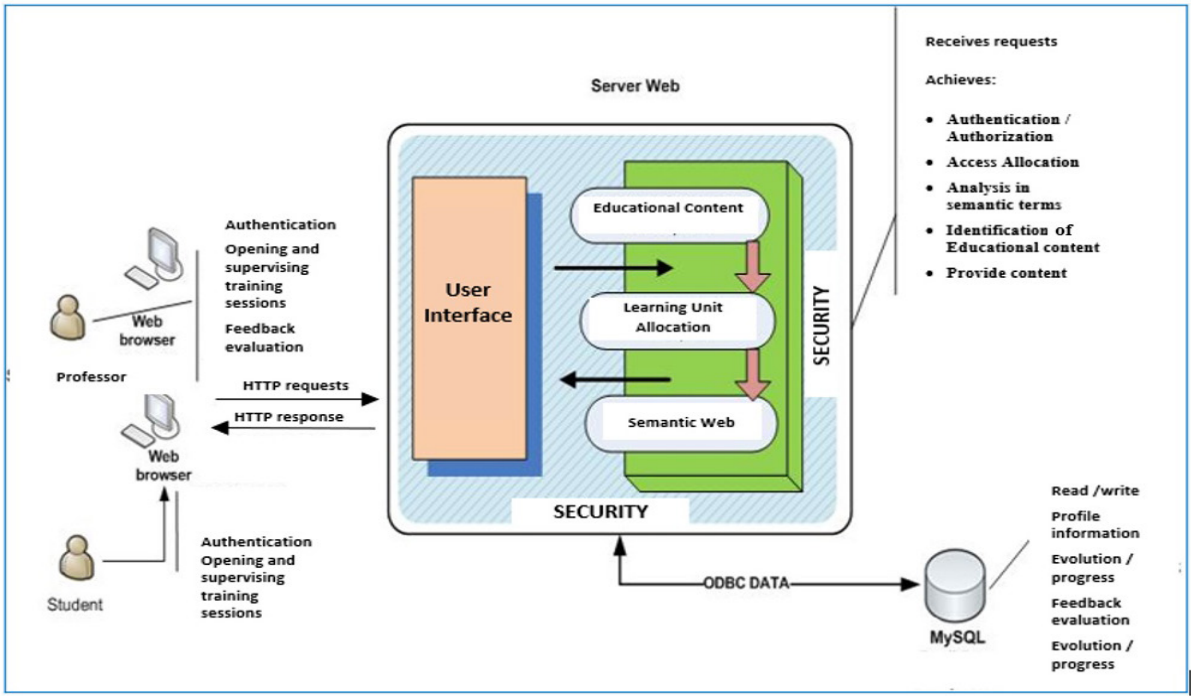

Figure 2. *General system architecture diagram*

Clients are represented by modern browsers, the recommended ones being Microsoft Edge, Google Chrome or Mozilla Firefox. The server is built on an open-source Linux framework.

The main argument for using this operating system is related to the high flexibility specific to open-source components, increased security, and last but not least, the absence of license costs.

MySQL is the relational database used to store profile information, target group member evolution, and student assurance feedback.

The components of the system are presented below:

- **User Interface** (A) is a client component, through which the student requests a URL and then selects the work option (for example, selects the desired section of the course material). All these operations are performed through a browser, all requests being sent to the Web Server component, which after specific processing at the server level will send the response back to the student;
- The **Application Interface** (Front-end) (B) is a component of the server that interacts with clients. It receives requests from the client via the HTTP protocol, forwards the request for internal processing, waits and sends back to the client the response in a specific web page format, so that it can be displayed in the browser;
- The **Security Component** (C) has the role of ensuring the optimal and safe use of the system. The component is responsible for authenticating participants, based on student name and password, but also for authorizing and controlling access to resources, depending on the role of the student and the context;
- The **Learning Unit Allocation Component** (D) together with the semantic web engine (E) analyzes, from the moment of authentication in the system, the specific context of each member of the target group and, using an internal algorithm based on the data model and student attributes, determines the best-personalized training path for the student to follow, to maximize the degree of assimilation of knowledge;
- The **Semantic Web component** (E) is custom-built around a Semantic Web engine. The Semantic Web component is able to process RDF / OWL formatted documents and information based on the training model presented, creating optimal links between specific resources, adapting to the student profile, and having a supporting role for components (D) and (F). Due to its extensibility, the Semantic Web Engine is able to provide flexibility in handling RDF / OWL schemas;
- **Content Generation** (F) is the component responsible for processing and generating optimal customized educational content using the developed student model. This component together with (D) and (E) works to ultimately provide a highly personalized course;
- The **Database Server** (G) represents the storage component that keeps the persistent information of the system, respectively the specific information of each student who accesses the platform, profile information, as well as information about the activities performed by him and his progress in training.

The security components of the ONTO e-learning platform are presented below.

Authentication and Authorization

The e-learning platform uses strong authentication methods, in the future two-factor authentication (2FA) could be considered to prevent unauthorized access.

Authentication is the process of identifying a user. Through authentication, the e-learning platform confirms that the user is „identified".

There are several authentication methods considered:

- **Username and Password:** This method is the most common authentication method. The user enters the username and password in the corresponding fields - an option available since the pilot stage.

- **Two-Factor Authentication (2FA):** This method provides an additional level of security by requiring users to also enter a verification code generated by a physical device or mobile app. This method is considered for later versions.
- **Facial or fingerprint identification:** This authentication method uses facial or fingerprint recognition technology to identify the user. It is an option in the exploration stage for a comparative analysis in relation to two-factor authentication (2FA).

Through the authorization process, the e-learning platform controls the type of access to resources or services once authenticated.

Authorization is based on the roles and permissions assigned to each user. Roles are categories of users, such as teachers, mentors, students or administrators. Permissions are the tasks or actions that users with a specific role can perform.

Thus, a teacher can have permission to create courses, assess students, and access course content. A student can have permission to view courses, participate in assessments, and download educational materials and resources.

To ensure maximum security, the e-learning platform implements strong authentication and authorization methods. These methods are adapted to the specific risks of the e-learning platform.

To improve the security of authentication and authorization in the e-learning platform, the following aspects were considered:

- Use of strong authentication methods in the next version, such as two-factor authentication.
- Periodic reminder to users to create strong passwords and change them with a certain frequency.
- Defining roles and permissions for each actor relevant to the platform.
- Implementation of security measures to further protect the system against cyber-attacks.

The e-learning platform allows users to create strong passwords and change them periodically. The implementation of „assistant" functions is considered to help users remember complex passwords. In order to maintain a high password complexity, the use of password managers is recommended. Password managers store passwords in a safe place and encrypt them so users don't have to remember them. In order to maintain a high password complexity, the use of password managers is recommended.

Access Control

The e-learning platform offers control over access to content and resources. Administrators can define roles and permissions for each user so that users can access only the resources they are entitled to.

Access control is a process of determining who has access to which resources or services. It is an essential part of the security of any e-learning platform.

To ensure maximum security, the e-learning platform implements granular access control. This means that it should be possible to define specific permissions for each role.

Here are some of the benefits of granular access control:

- Use of strong authentication methods in the next version, such as two-factor authentication.
- Increases security: Granular access control can help prevent unauthorized access to resources and services.
- Simplifies user management: Granular access control can make it easier for administrators to manage user access.
- Provides greater flexibility: Granular access control can be used to give users only the access they need, without „giving them too much".

To implement granular access control, the following aspects were taken into account:

- Defining specific roles and permissions for each user;
- Periodic review of roles and permissions to ensure they are still relevant;

- Implementation of security measures to protect user data.

Granular access control is an effective way to improve the security of e-learning platforms. By defining specific permissions for each role, administrators can help prevent unauthorized access to resources and services.

The e-learning platform is protected against cyber attacks such as phishing attacks, brute force attacks and DDoS attacks. Administrators consider implementing security measures such as up-to-date software updates, spam or content/proxy filters, and firewalls.

To protect against cyber-attacks, the e-learning platform operates with the following security measures:

- Implementation of up-to-date software updates: Software updates often include security patches that can help prevent the exploitation of vulnerabilities related to the software components, both server-side (database, application server) and client-side ones (JavaScript libraries used to display and operate the content in the web interface from the browser);
- Use of a firewall: A firewall that helps block unauthorized traffic from accessing the e-learning platform;
- Implementing spam and content filters: Spam filters help block fake emails and text messages that may contain malware;
- Awareness of cyber risks: Administrators and users must be aware of cyber risks and adopt safe security practices.

By implementing appropriate security measures, the e-learning platform is protected from cyber attacks by users and the content of the platform.

The ONTO E-Learning Platform

From among the number of mechanisms mentioned above to assure the security of e-learning platforms, the initial implementation is focusing more on Authentication and authorization, Access control and Auditing, as follows.

Authentication and authorization: Users should be required to authenticate themselves before accessing the platform, and they should only be authorized to access the resources that they need. This can be done using a variety of methods, such as passwords for the initial implementation, but two-factor authentication, and biometric authentication are also considered on the roadmap.

Access control: Access to the platform and its resources should be controlled to ensure that only authorized users can access them. This can be done using a variety of methods, but for the initial implementation role-based access control (RBAC) is considered.

Auditing: The platform should be audited regularly to identify and address any potential security vulnerabilities. This includes auditing user activity, system logs, and security configuration.

In addition to these technical measures, it is also important to implement security policies and procedures for the platform. This includes things like user education, password management, and vulnerability management.

Figure 3 illusttrates the diagram of the security architecture for the ONTO e-learning platform.

As it can be seen in the diagram, the ONTO Security Layer is vertical, taking action at all the platform levels. These components should be interconnected in a way that provides a comprehensive and layered security posture. For example, the authentication and authorization components should be integrated with the policy and rules component to ensure that only authorized users can access the platform.

For a higher clarity on the implementation process, the essential components related to the security aspects considered are:

- Load balancer (LB): Distributes secured https traffic across multiple servers to improve performance and reliability – platform external component;
- Authentication engine: Authenticates users and provides them with access tokens;
- Authorization engine: Authorizes users to access specific resources on the platform;
- ONTO eLearning Core: Host the e-learning applications and business logic;

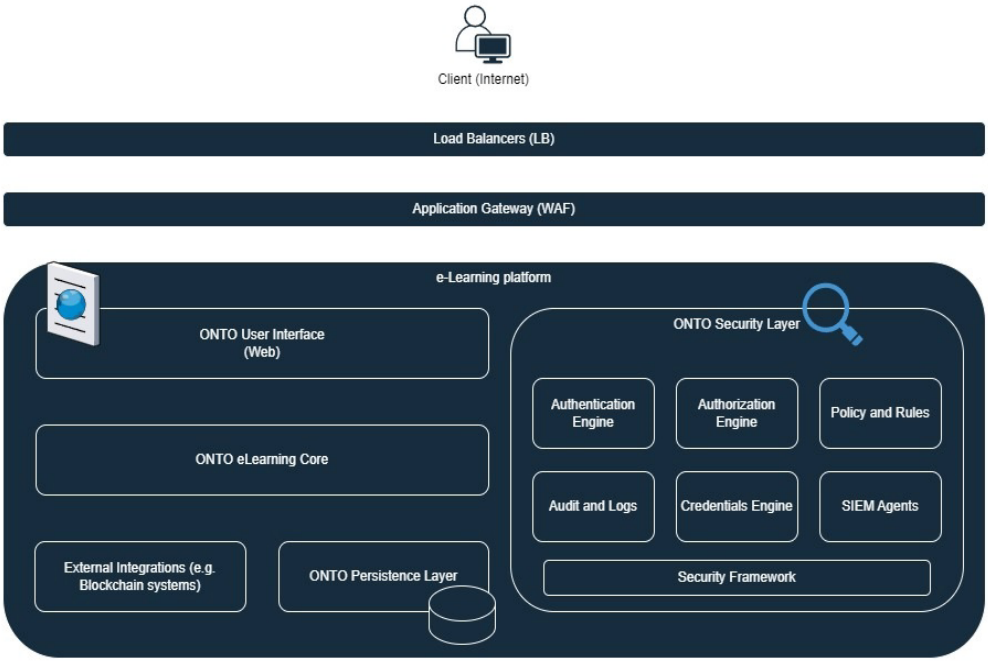

Figure 3. *Diagram of the security architecture for the ONTO platform*

- ONTO Persistence Layer: Stores the platform's data.
- Audit and Logs: Collects and stores logs from all platform components;
- SIEM Agents: Collect relevant data and forward it to a SIEM - Security information and event management - system that aggregates and analyses logs from all platform components to detect security threats and incidents.

Further on, some steps the learner follows in the learning process are presented, with an emphasis on the authentication and authorization process.

To implement the e-learning process on a real platform, an open-source web-based learning management system (LMS) was chosen. The e-learning platform based on semantic web technology offers the necessary tools (e-learning) to implement a new mechanism for obtaining relevant information from the Internet, thereby providing the possibility of using the advantage offered by semantic web content and multimedia materials (materials in electronic format, links, images, animations, sounds, movies, etc.) (Băjenaru, 2018; Băjenaru & Smeureanu, 2018).

Depending on the profile and his/her job in the managerial team, the student will have access to the e-learning platform, in order to obtain a personalized learning program based on a specific ontology, as well as to obtain bibliographies that meet his/her learning requirements.

A training sequence, represented by specific platform screenshots for a student applying for the position of hospital manager and who has an advanced level of knowledge, is presented below.

The student has logged onto the platform based on a username and password received from the administrator and is accessing it for the first time. On the main page of the platform, a wizard-like sequence opens, which ultimately has the role of determining the optimal educational content, personalized for the student.

In step 1, the desired position should be selected, namely Hospital Manager (manager de spital), and the student proceed to the next step, as it is shown in Figure 4.

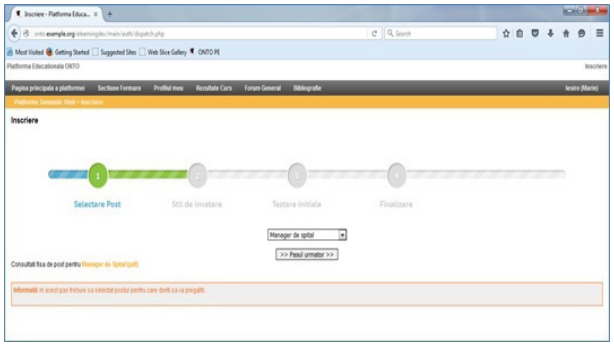

Figure 4. *Step 1 – position selection*

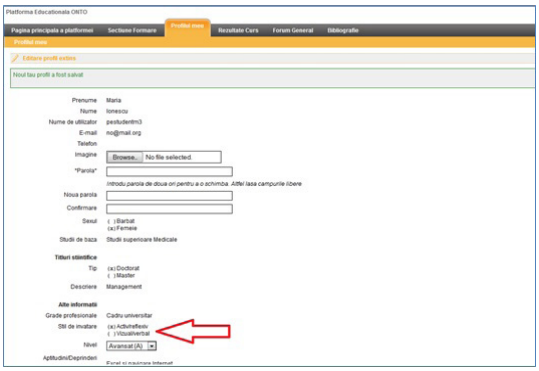

Figure 5. *Participant profile page*

The determination of the student's visual/verbal or active/reflective learning style was achieved by two methods: (1) by interpreting the text entered by the student in a defined area in the platform and (2) by using a questionnaire.

The RDF / OWL engine loads the OWL source to be able to perform the automatic student learning style determination. The active/reflective learning style is automatically determined, and it is saved in the participant's profile (Figure 5).

After returning to the wizard sequence, the initial testing takes place to determine the student's level of knowledge, and the process of defining the student profile is completed (Figure 6). In the last step, the Allocation of the learning unit is carried out, by associating an appropriate training content, personalized according to the test score, with the student's profile, the learning style, and other information related to his/her profile (Figure 7).

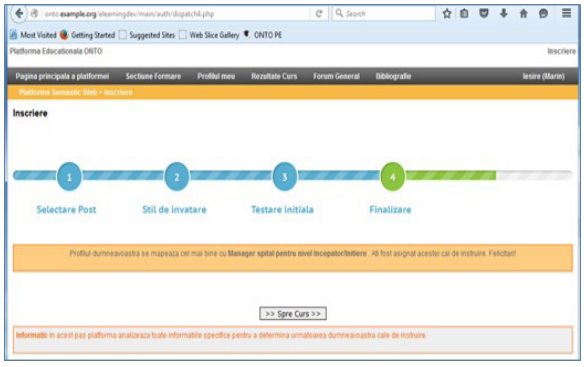

Figure 6. *Step 4 - Completion of registration*

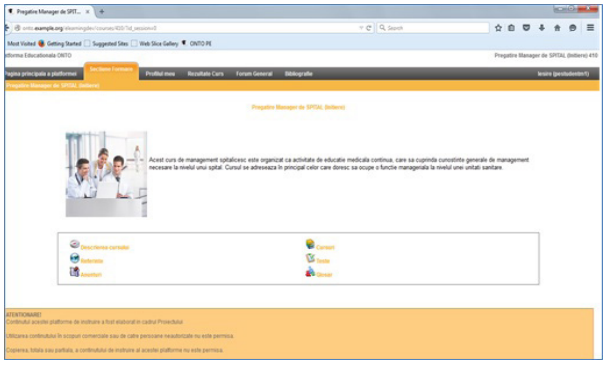

Figure 7. *Training section – home page*

The student has access to the training section, respectively to the training section for the position of hospital manager, with the following profile: graduate medical studies, advanced level of training, active/reflective learning style, initial test - grade 5 and other information related to his/her profile (Figure 7). The security system intervenes in the act of user authentication and before providing access to personal data on an e-learning platform by verifying the user's identity and ensuring data confidentiality. First, the security system checks if the user is „who he says he is". This is done through an authentication process, which may include entering a username and a password, and also a code, which is specific to „2FA" authentication. Second, the Security system checks the user's authorization to prevent unauthorized access to the educational content and ensures the confidentiality of the data from the training process.

CONCLUSION

Cyber attacks on e-learning platforms can have serious consequences, such as the loss of personal data and confidential information, as well as credentials and certifications. They can also lead to the unavailability of the platform for users, which can negatively affect the learning process.

In this regard, a case study is presented, an ontology-based e-learning platform for professionals in the healthcare management domain. The security and user access components are essential for the proposed e-learning platform based on semantic technologies. By implementing appropriate security measures, the e-learning platform can protect user data and platform resources from cyber-attacks.

To ensure maximum security, e-learning platforms should take a holistic approach to security that considers all aspects of security, including technology, people, and processes. It is also important to create a security culture within the organization so that users are highly aware of cyber risks and adopt safe security practices.

REFERENCE LIST

Abbasi, S., Ayoob, T., Malik, A. & Memon, S. I. (2020) Perceptions of students regarding E-learning during Covid-19 at a private medical college. *Pakistan Journal of Medical Sciences*. 36, S57-S61. doi: 10.12669/pjms.36.COVID19-S4.2766.

Akacha, S. A.-L. & Awad, A. I. (2023). Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders. *Sustainability*. 15(19), 14132. doi: 10.3390/su151914132.

Almaiah, M. A., Al-Khasawneh, A. & Althunibat, A. (2020) Exploring the critical challenges and factors influencing the e-learning system usage during COVID-19 pandemic. *Education and Information Technologies*. 25(6), 5261-5280. doi: 10.1007/s10639-020-10219-y.

Anghel, M., Perețeanu, G. C. & Cîrnu, C. E. (2020) Emerging Trends in Elearning and Mlearning from a Byod Perspective and Cyber Security Policies. In: *Proceedings of the 16th International Scientific Conference eLearning & Software for Education (vol. I), 30 April - 1 May 2020, Bucharest, Romania*. Bucharest, University Publishing House. pp. 444-452.

Banciu, D., Vevera, A. V. & Popa, I. (2023) Digital Transformation Impact on Organization Management and Several Necessary Protective Actions. *Studies in Informatics and Control*. 32(1), 49-56. doi: 10.24846/v32i1y202305.

Băjenaru, L., Smeureanu, I. & Balog, A. (2016) An Ontology-Based E-Learning Framework for Healthcare Human Resource Management. *Studies in Informatics and Control*. 25(1), 99-108. doi: 10.24846/v25i1y201611.

Băjenaru, L & Smeureanu, I. (2018). Learning Styles in an Ontology-Based E-Learning System. In: Silaghi, G. C., Buchmann, R. A. & Boja, C. (eds.) *Informatics in Economy*. 15th International Conference, IE 2016. (*Lecture Notes in Business Information Processing*, 273). Cham, Switzerland, Springer, pp. 115-129.

Băjenaru, L. (2018) *Ontologii informatice în învățământul online (Computer Ontologies in Online Education*). Bucharest, ASE Bucharest Publishing House.

Chen, G., Xu, B., Lu, M. & Chen, N.-S. (2018) Exploring blockchain technology and its potential applications for education. *Smart Learning Environments*. 5(1), 1-10. doi: 10.1186/s40561-017-0050-x.

Clarke, J. (2012) *SQL Injection Attacks and Defense*. Rockland, Syngress Publishing.

Fogie, S., Grossman, J., Hansen R., Rager, A. & Petkov, P. D. (2007) *XSS Attacks: Cross Site Scripting Exploits and Defense,* Syngress, Massachusetts.

Gavrilă, V., Băjenaru. L, Tomescu, M. & Dobre, C. (2020) Security Measures Analysis Related to Intellit Platform. In: *13th International Conference on Communications (COMM), 18-20 June 2020, Bucharest, Romania*. pp. 93-96. doi: 10.1109/COMM48946.2020.9141977.

Mihai, I. C., Ciuchi, C. & Petrică, G. (coord.). (2020) *Securitatea Cibernetică - Provocări și Perspective în Educație*. București, Editura Sitech. doi: 10.19107/CYBERSEC-EDU.2020.RO.

Nakamoto, S. (2008) *Bitcoin: A peer-to-peer electronic cash system.* [Acccesed October 2nd 2023]. https://bitcoin.org/bitcoin.pdf

Nikola, D., & Milena, B. (2021) Applying Blockchain Technology in eLearning systems: Overview, Analysis and Potential Solutions. In: *Proceedings of the 11th International Conference on Information Society and Technology, 7-10 March 2021, Kopaonik, Serbia.*

Nikou, S. & Maslov, I. (2021) An analysis of students' perspectives on e-learning participation - the case of COVID-19 pandemic. *International Journal of Information and Learning Technology.* 38(3), 299-315. doi: 10.1108/IJILT-12-2020-0220.

Scheau, M. C. (2018) *Criminalitatea informatica privind transferurile financiare*. București, Editura Economica.

Singh, A. & Gupta, B. B. (2022) Distributed Denial-of-Service (DDoS) Attacks and Defense Mechanisms in Various Web-Enabled Computing Platforms: Issues, Challenges, and Future Research Directions. *International Journal on Semantic Web and Information Systems (IJSWIS)*. 18(1), 1-43. doi: 10.4018/IJSWIS.297143.

UNESCO. (2022) *Minding the data: protecting learners' privacy and security*, United Nations Educational, Scientific and Cultural Organization.

Vevera, A.V. & Albescu, A.R. (2018) Human resource vs. cyber security. *Romanian Journal of Information Technology and Automatic Contro*l. 28(4), 67-74.

Yu, S. (2014) *Distributed Denial of Service Attack and Defense*. New York, Springer.