Hindawi
Scientific Programming
Volume 2019, Article ID 9313571, 16 pages
https://doi.org/10.1155/2019/9313571

Research Article

Towards the Construction of a User Unique Authentication Mechanism on LMS Platforms through Model-Driven Engineering (MDE)

Jhon Francined Herrera-Cubides, Paulo Alonso Gaona-García, and Geiner Alexis Salcedo-Salgado

Facultad de Ingeniería, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia

Correspondence should be addressed to Jhon Francined Herrera-Cubides; jfherrerac@udistrital.edu.co

Received 20 October 2018; Accepted 26 December 2018; Published 11 March 2019

Guest Editor: Vicente García-Díaz

In LOD, authentication is a key factor in the security dimension of linked data quality models. This is the case of (a) LMS that manages open educational resources (OERs), in training process, and (b) LMS integrated platforms, which also require authenticating users. Authentication tackles a range of problems such as users forgetting passwords and time consumption in repetitive logins in different applications. In the context of linked OERs that are developed in LMS, it is necessary to design guidelines in order to carry out the authentication process. This process authorizes access to different linked resources platforms. Therefore, to provide abstraction methods for this authentication process, it is proposed to work with model-driven architecture (MDA) approach. This paper proposes a security abstraction model on LMS, based on MDA. The proposed metamodel seeks to provide a set of guidelines on how to carry out unified authentication, establishing a common dialogue among stakeholders. Conclusion and future work are proposed in order to generate authentication instances that allow access to resources managed in different platforms.

1. Introduction

Model-driven engineering (MDE) [1–5] has as one of its first phases the search for the understanding of the problem to be addressed, that is, the knowledge of the problem domain. From this knowledge, an initial abstraction is constructed, using model schemes. These models are intended to be essential components for communication between the problem domain experts and software developers.

Based on the principle that the fundamental artifacts of development software are the models and not the programs, MDE proposes model-driven software development (MDD) based on the models that are generated from the most abstract to the most concrete through transformation or refinements steps, until arriving at the code applying a last transformation. Taking into account the above, the model-driven architecture (MDA), a concept promoted by object management group (OMG), is configured as an architecture that provides a set of guidelines to structure specifications expressed as models, following the MDD process [6]. On the other hand, linked open data (LOD) is a strategy to link open data licensed under one of the several open licenses that allow reuse [7]. In order to verify the linkage process, in addition to carry out different studies about the status of the data web [8–12], different linked data quality models have been proposed in LOD. These models define a dimensions and metrics set, such as those proposed by Zaveri et al. [13]. Within these dimensions, security has been considered, as a measure in which data access can be restricted and, therefore, protected against its alteration and misuse.

The security priority level depends on whether the data should be protected and whether there is a cost to the data that is unwittingly available. It should be noted that, although in the case of open data, the security aspect is often

not very developed given that the data are freely accessible under a specific license. However, today's students want to access the training at their own time rhythm and place, which has motivated them to implement LMS to join students' personalized needs who seek an online learning with resources in mobile and dynamic environments. For this reason, LMS platforms, and their integration with other applications, pose a security challenge in aspects such as (a) user authentication, which consumes linked resources in these applications; (b) the management and remembrance of multiple users and passwords; (c) continuous calls to reset passwords; (d) time consumption by continuous logins in different platforms; and (e) managing different authentication schemes according to the platforms or applications used, among other factors [14, 15]. With the purpose of analyzing and establishing criteria about the integration of security as a quality dimension in the linked open educational resources, the question arises about How to structure a metamodel that provides an authentication abstraction process for linked open educational resources, supported on linked data quality dimensions? To address this research question, the use of MDA is proposed, in order to design a metamodel, which allows the generation of authentication instances for the linked open educational resources, supported by quality dimensions.

In Section 2, the background about the research subject is described. Subsequently, the methodological approach is presented in Section 3. The methodological development used for the metamodel approach is described in Section 4. In section 5, the results obtained and the discussion about them are exposed. Conclusion and future work are presented in Section 6.

2. Related Work

The main references that support the theoretical foundations used in this research are described below.

2.1. Identification and Authentication. As described in [16–18], when a user connects to a computer system, he/she must provide

(i) User name or identification: identification is the ability to identify a user of a system or an application that is running in the system [19]

(ii) Password or authentication

Authentication is the ability to demonstrate that a user or an application is really who the said person or application claims to be [19]. To carry out this identity verification process, there are different proposals such as [17, 20, 21]

(i) Something that is known (e.g., password): the most basic authentication model is to decide if a user proves he is who he says he is. In this case, it is possible to use a knowledge test that only that user can answer.

(ii) Something you have (e.g., badge, token, and smart card): an example of these are smart cards, which have a chip embedded in the card itself that can implement an encrypted file system and cryptographic functions and can also detect actively invalid attempts to access stored information.

(iii) Something that one is (e.g., fingerprint, DNA, and iris): for example, the so-called biometric systems based on the physical characteristics of the user to be identified.

(iv) Where you are (e.g., using a particular terminal).

To carry out authentication, the steps of (a) obtaining the authentication information of an entity, (b) analyzing the data, and (c) determining whether the authentication information is effectively associated with the entity are carried out [16]. For this process, there are authentication mechanisms such as passwords, challenge-response, alternative mechanisms (information, tags, cards, biometrics, signatures, etc.), and multiple methods, among others [22].

2.2. Linked Data Quality. As discussed in [23], published data may suffer from different problems given the heterogeneity of the data source, such as redundancy, inconsistencies, or may be incomplete. Therefore, queries made by applications that consume LOD may be inaccurate, ambiguous, or unreliable. Different authors [24–28] have proposed models and metrics to evaluate LOD instances published on the Web. Some of the criteria worked on in these proposals are oriented to provenance, content, RDF structure, and links, among other factors. It is important to note that in most of the references, a treatment of the proposed quality dimensions is identified, on the data instances already published on the Web.

On the other hand, some of these authors emphasize that quality must not only operate in the resource construction but also in the metadata itself, in order to seek the interoperability of said resources [29]. For the work in this investigation, the model proposed by Zaveri et al. [30] is proposed as a fundamental basis. This model qualitatively analyzes 30 main approaches to quality assurance and 12 tools using a set of attributes. As a result of this review, data quality dimensions and metrics model in LOD are proposed by the authors. Dimensions of (a) accessibility, (b) representation, (c) contextual, (d) intrinsic, (e) trust, and (f) dataset dynamicity are identified in this model.

2.3. MDE-MDA. MDE is a software development approach focused on the model generation to describe the elements of a system. Its main objective is the separation of the system design both from the architecture and from the construction technologies, facilitating that design and architecture can be modified independently. In this section, it is important to present some essential concepts in MDE [31–36]:

(i) Meta-metamodel describes the proposed metamodels, generating a supremely high degree of abstraction in which all models coincide.

(ii) Metamodel is a general structure in which entities are managed but not instances of them. The metamodel guides the model construction, through the description of the basic structure to follow, in addition to showing

the interaction rules between defined entities. In summary, they are tools (rules, restrictions, models, and theories) that allow the model construction.

(iii) Model is the application of the metamodel in a particular case, in other words, a structure in which general entities are not managed, but rather with specific instances of them. In general, it is a description (simplified representation) of one or more domain elements or real world.

As for MDA, this architecture provides a set of guidelines for structuring specifications expressed as models [5]. MDA focuses on the following three principles:

(i) Direct representation focuses on the ideas and concepts of the problem domain and decreases the distance between the domain semantics and its representation, applies principles of abstraction, and separates relevant aspects from the problem domain of technology decisions

(ii) Automation promotes the use of functionalities such as the exchange of models, the management of metamodels, the verification of consistency, and the transformation of models

(iii) The use of open standards: the purpose is to achieve the interoperability in different tools and platforms, promoting the applications development

Metamodels in the context of MDA are expressed using meta-object facility (MOF), which proposes a 4-layer scheme: M0 (instances), M1 (the model), M2 (the metamodel), which define the elements of the model, and M3 (the meta-metamodel), which defines concepts, attributes, and relationships for the elements. Now, MDA adds to the model-driven approach the inclusion of several levels of abstraction (CIM, computation independent model; PIM, platform independent model; PSM, platform specific model) and several transformations between levels, thus carrying out system descriptions to several levels [2, 4, 35]. The development steps proposed in MDA are as follows [6]:

(a) The system requirements are presented in a CIM model, which describes the situation in which the system will be used

(b) The CIM model is transformed into a PIM model that describes the system, but does not show the details of its use in a particular technological platform

(c) After obtaining the PIM model, another transformation is made to the PSM model, which contains the necessary detail to use the technological platform in which the system will operate

(d) Finally, having the PSM model, a transformation is performed which results in the generation of code to achieve a solution or executable model

3. Methodological Approach

This research works on a quasiexperimental methodology. This design, as an empirical method, allows the analysis of the properties resulting from the application of the technological process, to obtain an analysis of the proposed variables. Considering that metamodels in the context of MDA are expressed in a 4-layer scheme, for this research process, M0: the instances; M1: the model; and M2: the metamodel layers are considered. From this perspective, the need to carry out a quasiexperimental design was proposed, in order to conceptually consider the abstraction process of the security dimension in the context of linked open educational resources, based on metamodels. This methodology is shown in Figure 1.

To develop this proposal, a methodological design structured in phases was defined, which allows to determine the processes that led to this research. In order to carry out the proposed design, the following phases are described succinctly:

(a) Context approach: in this phase, in order to identify the theoretical elements of the research, the following question was designed to guide the research process: How to structure a metamodel that provides an authentication abstraction process for the linked open educational resources, supported on linked data quality dimensions?

Based on the design of a metamodel for the abstraction of the authentication process for the linked open educational resources, it is important to take into account aspects of model-driven engineering and linked data quality, as key elements for the metamodel design, which allows generating guidelines for the construction of this abstraction.

(b) LMS authentication: in this phase, the research problem and the strategies identification used for the authentication in LMS are proposed, as the main axis in the abstraction process of the knowledge domain. In the same way, the key requirements are defined, to feed the build process of the proposed metamodel.

(c) Metamodel layers definition: after the requirements definition, the identification of the proposed layers for the elaboration of the conceptual design that will guide the metamodel implementation is carried out.

(d) Verification example design: in this phase, the verification example is carried out that will show the follow-up to the conceptual design that will guide the metamodel implementation.

(e) Results analysis: with the abstraction of the protocol to be followed and the corresponding application in the case of study, the proposed design is evaluated.

4. Methodological Development

4.1. LMS Authentication. In general, information is stored in an authentication process to carry out this process, such as user and password. As described in [37], in order to authenticate itself, a user generally provides at least two elements: (a) its identifier that allows its definition and (b) one or more elements that guarantee the authentication itself.

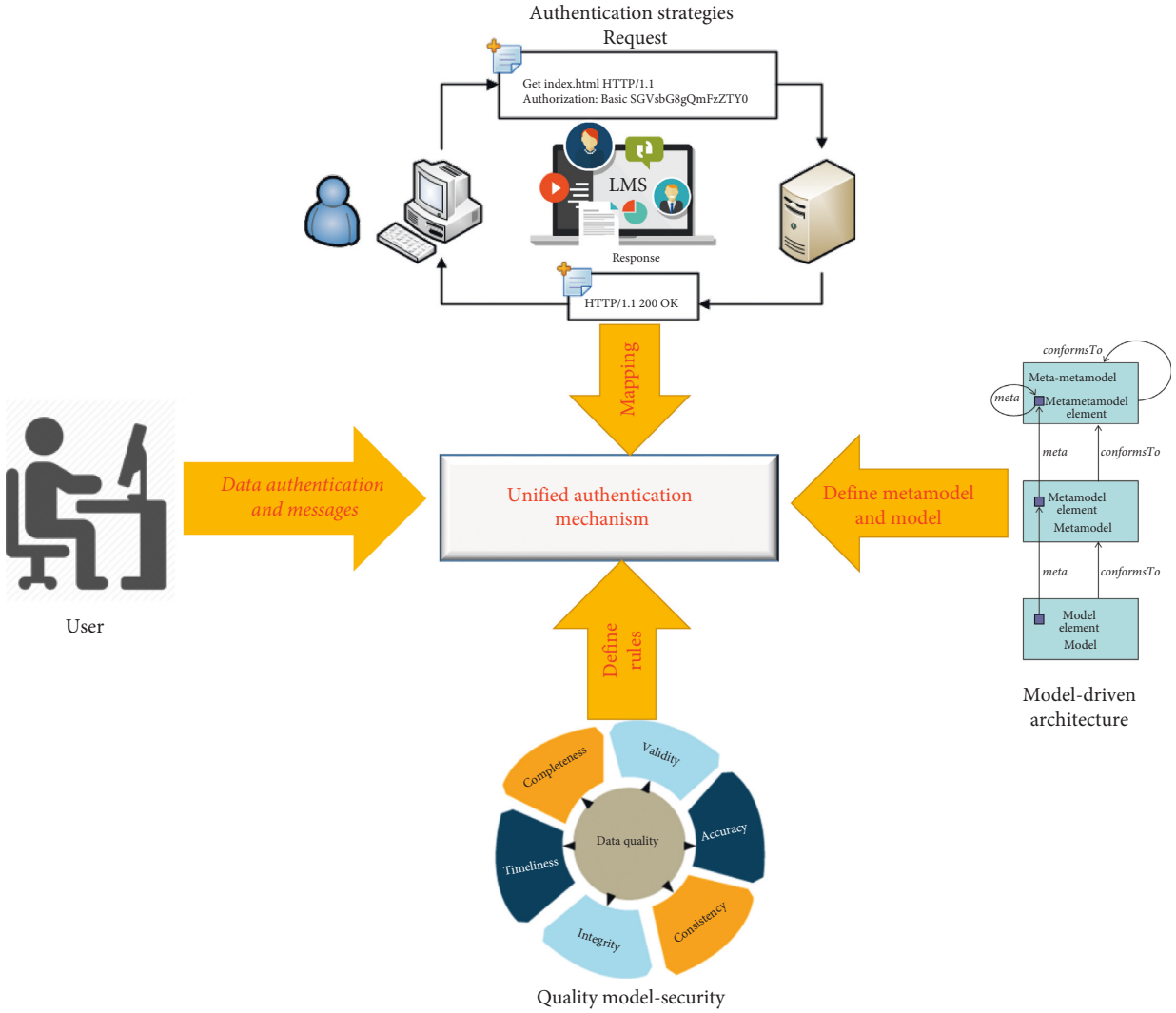


Figure 1: Methodological approach.

Thus, independent of the mechanism, the same elements are found in different forms, for example,

(i) Identifier and password.

(ii) PKI certificates on smart card or USB token: identifier is a public certificate that is signed and consequently guaranteed by a recognized certification authority. The user must provide a secret element to be able to use the different cryptographic elements, for example, "PIN code of your card or your USB key."

(iii) Identifier and password on a smart card.

(iv) Authentication by biometrics is based on the verification of an element of the user's body (usually the fingerprint).

(v) In multifactor authentication, different combinations such as smart card + PIN code, smart card + biometric, and biometric + password, among others, can be registered.

As for the learning management systems (LMSs), these are systems whose main function corresponds to providing sufficient support for the mediation of appropriation of knowledge and its administration, access to didactic and communication tools, and reuse of contents, among others. To carry out their objective, LMS must provide services and tools such as authentication. For such purpose, LMS must have an infrastructure to guarantee the users authentication [38]. In LMS such as Moodle, different authentication mechanisms through modules are developed, which allow easy integration with existing systems. Within these mechanisms are the following [39]:

(i) Standard method of e-mail registration: students can create their own access accounts. The e-mail address is verified by confirmation.

(ii) Lightweight Directory Access Protocol (LDAP) method: access accounts can be verified on an LDAP server. The administrator can specify which fields to use.

(iii) Internet Message Access Protocol (IMAP), Post Office Protocol (POP3), and Network News Transport Protocol (NNTP): access accounts are

verified against a mail or news server (news). Supports secure sockets layer (SSL) certificates and transport layer security (TLS).

(iv) External database: any database, which contains at least two fields, can be used as an external authentication source.

An example of user authentication interfaces which access different applications of the District University (Academic Management and LMS) is shown in Figure 2. Each of them has an independent authentication mechanism.

4.2. Metamodel Layers Definition. According to the layer scheme defined for the metamodels in the MDA context, layers below were proposed to work on the framework project: (a) M0 (the authentication), (b) M1 (the authentication model), and (c) M2 (the metamodel). The structure of the meta-object facility (MOF) proposed for the project is shown in Figure 3. In this architecture, the following is proposed:

(i) A metamodel that defines restrictions, rules, and theories set must be followed by the representations made about it. This layer will define requirements and restrictions, which must be met in any authentication process.

(ii) A model that characterizes both the defined authentication strategy, supported on the quality dimension, and the requirements definition that these must meet in their design.

(iii) A model instance, which represents the abstraction made of the knowledge domain, adjusted under metamodel constraints, in an own domain of linked data quality.

4.3. Verification Example Design. For the verification example design, the metamodel requirements must be identified in the first instance.

Case study: "A digital educational resources bank is connected to several institutional repositories. When a user enters the resource bank, after logging in, he should be able to access the different LMSs that manage the resources there related, even more so when said LMS corresponds to different providers. This single access provides the user with a username and password for each of the repositories, in order to access and consume the resources published there."

For this problem context, metadata or data model requirements are not handled. The domains used correspond to security and LMS.

4.3.1. Knowledge Domain. The knowledge domain for the problem posed presents the following knowledge instances:

(a) *Quality Dimension*. For this verification exercise, the security dimension was worked on, grouped in the accessibility category, based on the quality model proposed by Zaveri et al. [13]. According to the authors, this aspect describes the following:

(i) Accessibility: the dimensions that belong to this category involve aspects related to the access and retrieval of data to obtain all or part of the data for a particular use case. There are five dimensions that are part of this group, which are availability, licensing, interconnection, security, and performance.

(ii) Security: security is the metrics to which data access can be restricted and, therefore, protected against its alteration and misuse. Security is measured according to whether the data have an owner or require web security techniques (e.g., SSL or SSH) for accessing, acquiring, or reusing the data by users. The importance of security depends on whether the data should be protected and whether there is a cost of data that is unwittingly available. For open data, security is often not very developed since the data are freely accessible under a specific license.

(b) *Digital Repositories*. As described in [41], a learning object repository (ROA) is a software system that stores educational resources and their metadata (or, only, the latter) and provides some type of resource search interface, either for interaction with humans or with other software systems. Additionally, there are learning management systems (LMSs), which allow designing courses based on the reuse and integration of learning objects. These resources have been searched and previously selected in repositories. Regarding authentication, an LMS must have an infrastructure to guarantee the authentication of its users.

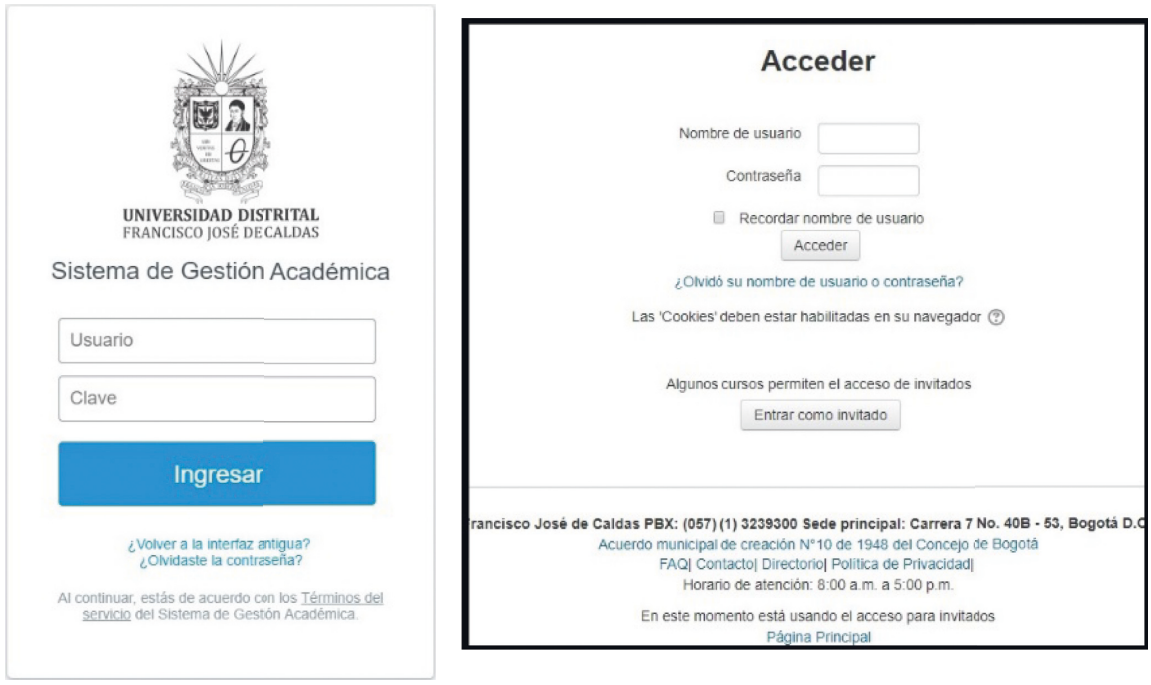
(c) *Identification and Authentication*. Identification is the ability to uniquely identify a system user or an application that is running on the system. Authentication is the ability to demonstrate that a user or an application is really who the said person or application claims to be [16].

(d) *Single Sign-On*. It is an authentication mechanism [42], which allows users to access different systems through a single identification instance. In other words, single sign-on (SSO) is a concept to delegate the authentication of an end-user on a service provider (SP) to a third party, the so-called identity provider (IdP) [43]. The behavior proposed by single sign-on is shown in Figure 4.

In SSO, there are common configurations:

(i) Enterprise single sign-on (E-SSO): It operates as a primary authentication and intercepts the login requirements that are required by the secondary applications in order to complete the user and password fields. For the correct operation of E-SSO, it is necessary that the underlying applications allow to disable the login interface.

(ii) Web-based single sign-on (Web-SSO): this type of solution operates only with applications and



(a) (b)

Figure 2: Examples of authentication interfaces. (a) Academic management system. (b) LMS system. Source: [40].

resources that are accessed through the web. The access data are intercepted through a proxy, a component on the server, or the portion of software running on the client. Users, who have not been authenticated yet, are redirected to an authentication service from which they must return with a token or successful access.

(iii) Kerberos: users register on a server and obtain a ticket (TGT: ticket-granting ticket), which is used by client applications to gain access.

(iv) Federated identity: it corresponds to an identity management solution or identity management, which allows using the credentials available in one authentication system in others, either from the same organization or even from other companies. The above is done with standards that define mechanisms to share information between domains.

After a review, different SSO implementations were identified. These *related works* are shown below:

(i) Web-SSO is a used technique to allow users to easily register and sign-in to websites with the use of social media accounts. These websites can be associated with new applications downloaded from Apple's App Store, Android's Google Play store, or even accessing website accounts [45].

(ii) In Austria, most public sector applications use an open-source identity provider called MOA-ID. However, due to the sectorial identity management, MOA-ID has not been single sign-on capable. A security architecture that enables single sign-on between different governmental applications using MOA-ID as identity provider while meeting the requirements for sectorial data privacy protection at the same time is presented in [46]. This research achieves this by transforming unique sectorial identifiers of users with the help of an additional trusted attribute provider.

(iii) A system which wants to integrate information systems by using web services should provide a unified identity authentication single sign-on scheme for heterogeneous platforms. This research introduces the characteristics of Kerberos-based single sign-on and SAML-based single sign-on [47].

(iv) Federated access control schemes such as SAML and OpenID for authentication or OAuth for authorization enable secure, cross-domain single sign-on for web and mobile applications regardless of where users are located or what device they are using to start the authentication or authorization flows. Using federated schemes allow users to avoid managing as many user names and passwords as services they want to interact with. Instead, they ask for a token at some kind of identity provider or verifier and all services participating in the federation trust these tokens to solve authentication and/or authorization [48].

(v) OpenID Connect is the OAuth 2.0-based replacement for OpenID 2.0 (OpenID) and one of the most important single sign-on (SSO) protocols used for delegated authentication. It is used by companies like Amazon, Google, Microsoft, and PayPal [43].

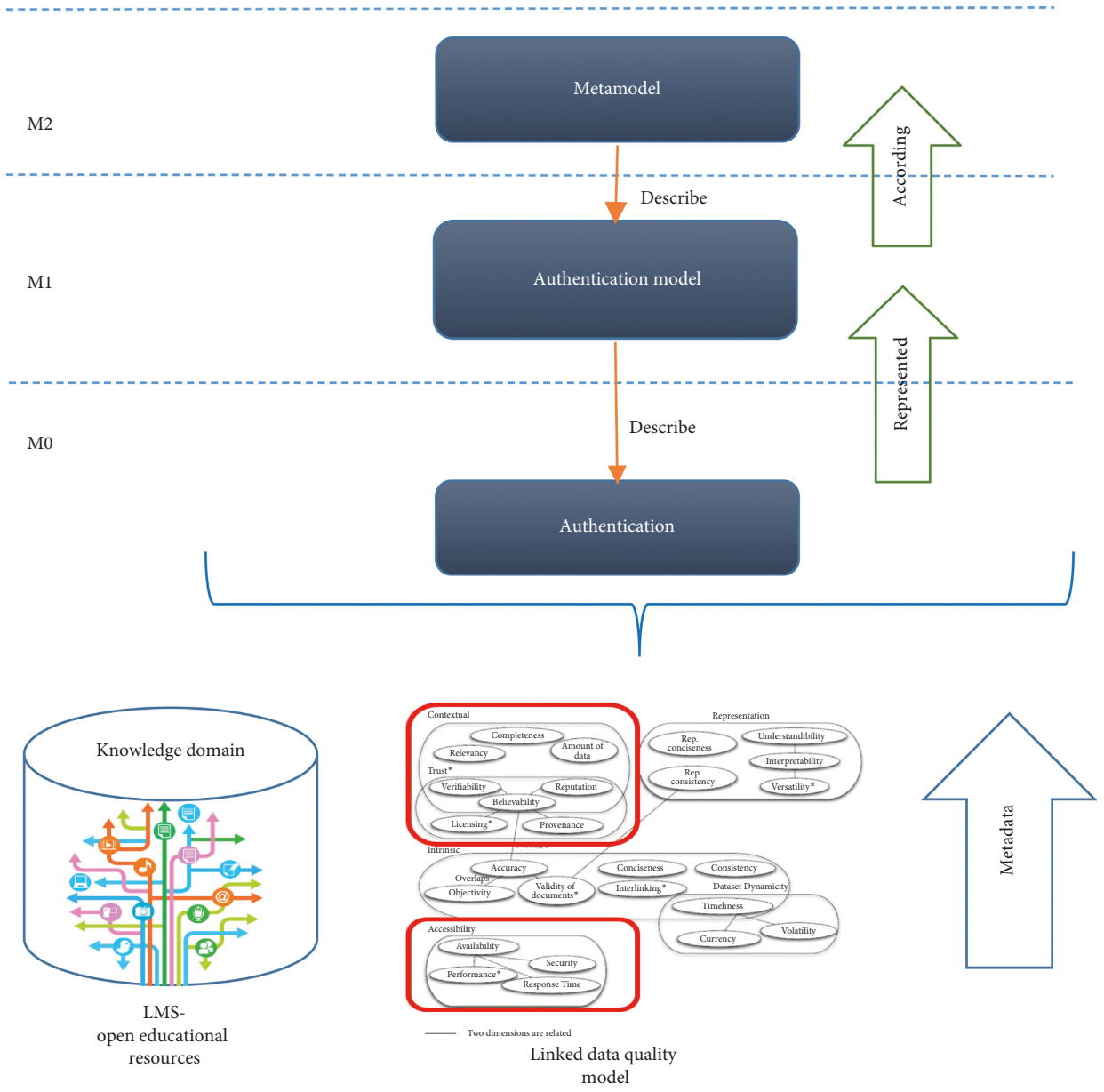


Figure 3: Project MOF.

5. Results and Discussion

5.1. Requirements. Identified requirements are as follows:

(i) Requirement R1 provides a security mechanism for accessing users and acquiring or reusing data.

(ii) Requirement R2 provides an authentication mechanism that allows a user to access the LMS instances, where resources are managed.

5.2. Metamodel. Taking into account the above requirements, it is necessary to consider some situations described below, in order to build the metamodel:

(a) Accessibility in a secure way to different LMSs, using the same access point, involves an authentication layer, which allows authenticating the access of consumers to exposed digital resources in each LMS.

(b) In addition to the accessibility to different LMSs, it is possible to integrate the LMS with other tools, such as customer relationship management (CRM), electronic commerce, or any other application. This authentication scheme in different applications should also have a single authentication layer.

In other words, the task of this layer is twofold: on the one hand, integrating each authentication scheme from different LMSs, and on the other hand, offering an authentication service to users. Since each integrated LMS has its own authentication model, it is necessary to make an abstraction over multiple authentication models, unifying them under this basic metamodel. The proposed general

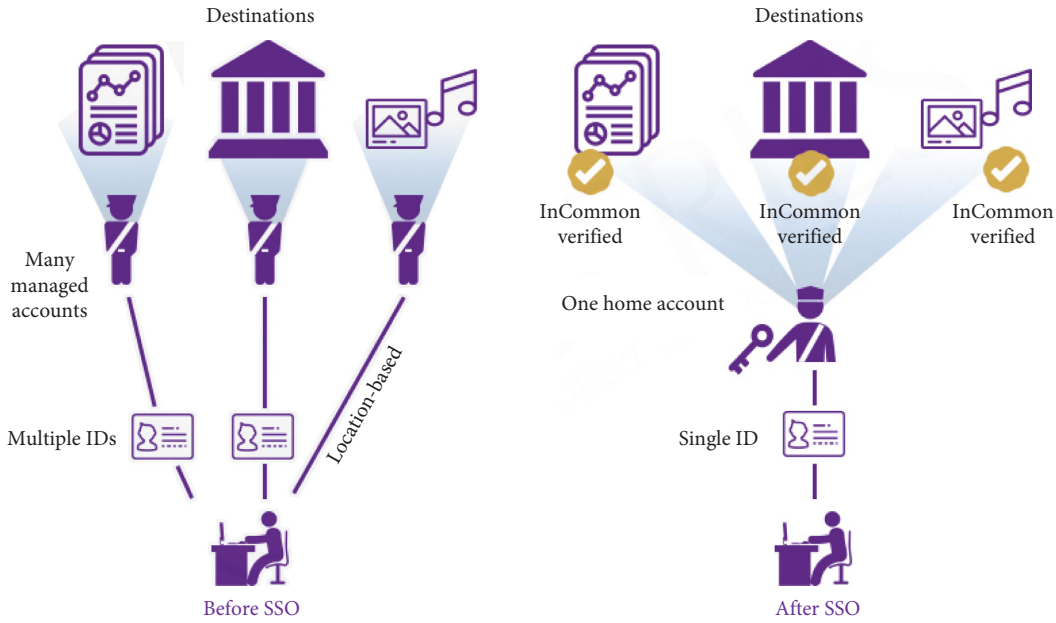


Figure 4: Single sign-on. Source: [44].

metamodel is illustrated in Figure 5. The implementation of this authentication layer uses a metamodel that consists of the following three simple classes:

(i) *Entity*. They are both the user who wishes to carry out the authentication and the authenticating entity, which handles the unified authentication mechanism and which can map the attributes to each LMS authentication scheme or integrated applications.

(ii) *Attribute*. These factors are captured to carry out the identification (e.g., the nick) and the authentication (e.g., the token).

(iii) *Message*. These are the request and response messages made between user and unified authentication system.

The restrictions that the metamodel handles are defined according to the unified authentication factors. As described in [24], different criteria can be configured, which can be taken as factors for authentication. An example of configuring basic criteria for IMAP is shown in Table 1.

According to the characteristics of the LMS authentication modules, the use of an identifier factor and an authenticating factor (pin, biometric, or a simple password) can be abstracted. To specify a little more, the requirements proposed by the domain abstraction, a more detailed metamodel where the entities, attributes, and messages are specified in textual form, are shown in Figure 6.

As seen in Figure 6, after receiving the message from the "User" entity, "Authenticator" entity processes the authentication of the factors submitted as attributes (credentials), generating a response message, either the authorization or the rejection of the user.

5.3. Model. To perform the interaction between entity, attribute, and message, the model design is proposed, which, in addition to responding to the criteria established in the metamodel, encapsulates access to identity management functions and provides a single session on. For this, delegator pattern in [51] is proposed, which allows an independent evolution of the weakly coupled identity management services while providing system availability. The class diagram, which visualizes the unique authentication model implementation based on a delegator pattern, is shown in Figure 7.

With this pattern implementation, the client does not interact directly with identity management service interfaces. The delegate prepares for the single session on, configures security session, looks for the physical security service interfaces, invokes the appropriate security service interfaces, and performs the global logout at the end [51].

5.4. Instances. The proposed model instance is based on single sign-on. An example of the login process in the TalentLms domain, through the SSO service, is shown in Figure 8.

Implementations of SSO in Canvas, WordPress, Atlassian, Jooomla, Drupal, and Magento, among other platforms, are described in [53, 54]. Research on SSO, which is being carried out at the Universidad Distrital Francisco José de Caldas, is shown in Figures 9 and 10. This proposal is based on The OAuth 2.0 Authorization Framework (RFC 6749) [55], a framework based on refresh tokens which are credentials used to obtain access tokens.

The developed interface is shown in Figure 11.

The aim of this research is to integrate academic applications, used at the Universidad Distrital. Subsequently, learning resources repositories will be integrated. For this integration, its metamodel proposes a set of recommendations. These recommendations will allow mapping generated tokens, to each learning objects repositories. This process lets

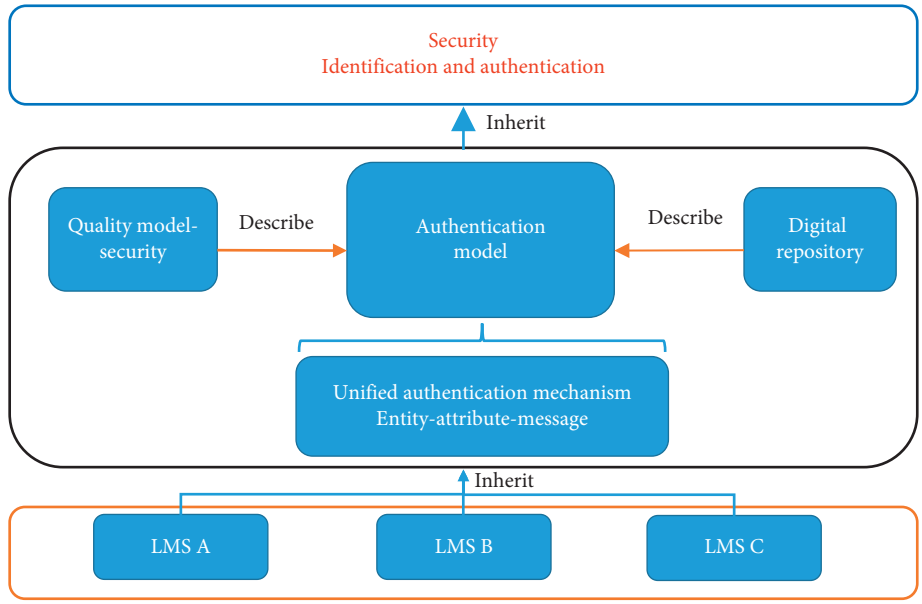


Figure 5: General metamodel proposal.

Table 1: IMAP configuration parameters.

Username	Personal name (e.g., Juan Carlos Pérez)
E-mail	Main address, for example, juan.perez@alumnos.unican.es
Answer	The same
Incoming IMAP mail server	imap.alumnos.unican.es with SSL protocol (port 993)
Outgoing SMTP mail server	smtp.alumnos.unican.es with TLS protocol (port 587)
Account name	username@alumnos.unican.es (e.g., xyz01@alumnos.unican.es)
Password	User password
Other parameters	Enable outbound authentication (SMTP) with the same username and password

Source: [49].

perform respective authentication. In other words, for each authentication model, respectively, instantiated, the unified authentication mechanism will manage tokens for authentication process and according to their validity will allow access to the respective repository.

The proposed model focuses on user authentication and validation process that will allow them to access educational resources. Basic architecture for the credential verification process and after that access for query or management of educational resources is shown in Figure 12. Different points are shown in this model. Some of them are relationship between Web applications that share educational resources and messages passing to access control to resources. Access control is done by credentials, which are validated in SSO.

Token must be sent with each request that is made for queries or management of educational resources. When a request is made in the API manager, validation process starts, taking the token from the request header to query it in the authentication server and grant access permissions and consumption service in the API. By obtaining an educational resources list located in other applications, resource access will be transparent to users, since message flow for access authorization will be managed with the same implicit flow.

This model allows controlling access to educational resources on different applications that require credentials validation. In addition to manage permissions to repositories access, this model allows to edit resource information (if the application allows it). The flow is controlled and is supported through the most used authentication protocols, such as OAuth2.

As a discussion about what is the broad application of the SSO model beyond the case study proposed, a single authentication design has different advantages and disadvantages, which are exposed [39, 43, 45–48, 51, 58, 59]. Among the advantages, the following advantages are identified:

(i) Minimizing the amount of passwords and usernames, which are used in password-based authentication for instance, and the ease in signing up for new websites and apps.

(ii) With a single session record, factors such as the use and possible forgetting of multiple access keys are attacked, as well as reducing the time in different authentication processes.

(iii) Using model implementation patterns, such as delegation, allows to improve the handling of the sessions, since the single sign-on service creates a secure SSO session and delegates the service requests to the relevant security services.

(iv) By avoiding centralized management of users and authorizations, the applications themselves have to implement these mechanisms (it is delegated to the SSO itself), streamlining the process of provisioning user credentials for the different applications, and

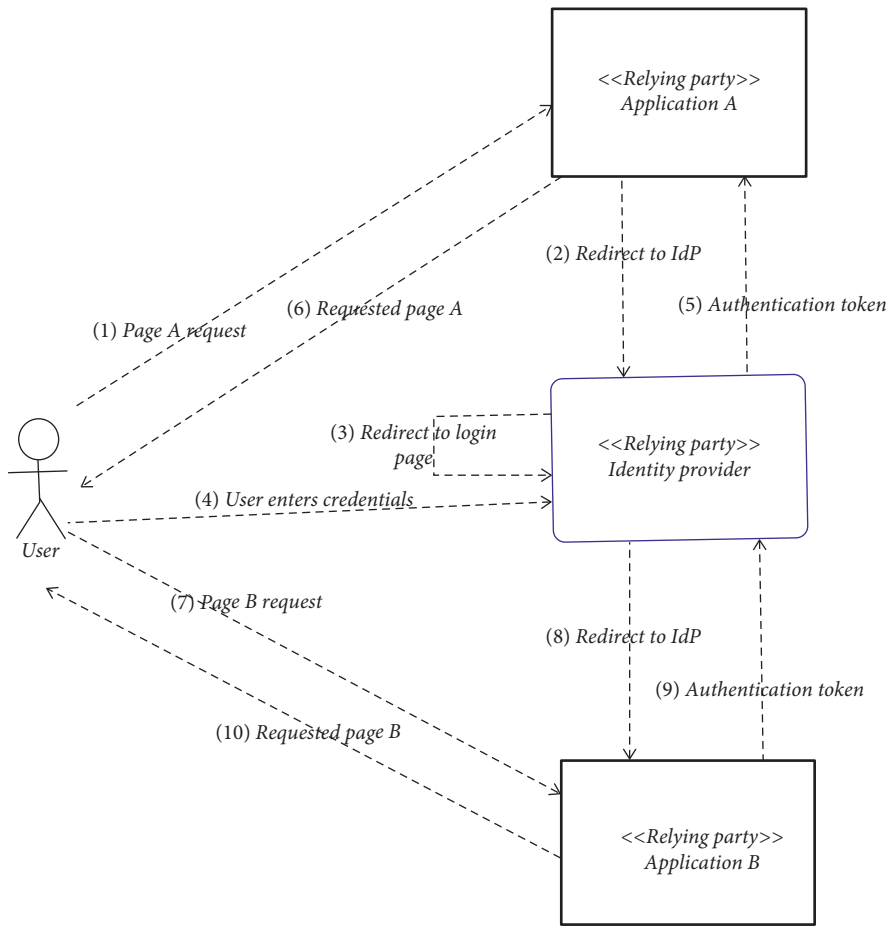


Figure 6: Detailed metamodel proposal. Source: [50].

automating this process considerably reduces the error probability.

(v) Multiplatform system allows the integration of different systems from different manufacturers in a single user authentication mechanism.

Disadvantages are as follows:

(i) The SSO system accessing process allows an intruder to access all the systems covered by the SSO system. This inconvenience is usually mitigated by making the authentication process much stricter than in the usual processes.

(ii) When SSO is implemented, it must be used very carefully. This is especially true if there is not complete control over who is authenticated by the identity provider. Authentication only provides information about the user's identity; for this reason, it should be verified separately in each application what should be visible to him/her.

However, some *contributions and findings* were identified in the review as follows:

(i) Using single sign-on delegator pattern, multiple instances of the remote security services will help improve scalability and support a standards-based single sign-on framework that does not require users to sign-on multiple times [51].

(ii) The SSO process for web applications can use two techniques (a) using passive redirection mechanism: applications that are involved in the process do not communicate directly with each other, but rely on browser's redirection and standard HTTP GET and POST messages. (b) Using "active SSO": when a relying party application talks directly (e.g., via a Web Service) to the identity provider to validate the user's identity and obtain the related security token [50].

(iii) Under a corporate environment, the user needs to remember only one set of credentials to access various resources in and out of the organization's network, in addition to increasing productivity by avoiding reentering your password to authenticate yourself in various resources repeatedly [52].

(iv) Burden on the IT is cut down due to fewer helpdesk requests for password resets. Centralized authentication center and identity management allows quicker and better control over the accesses granted to each user [53].

(v) SSO can be mixed with any of authentication methods (e.g., security questions, mobile authentication, and

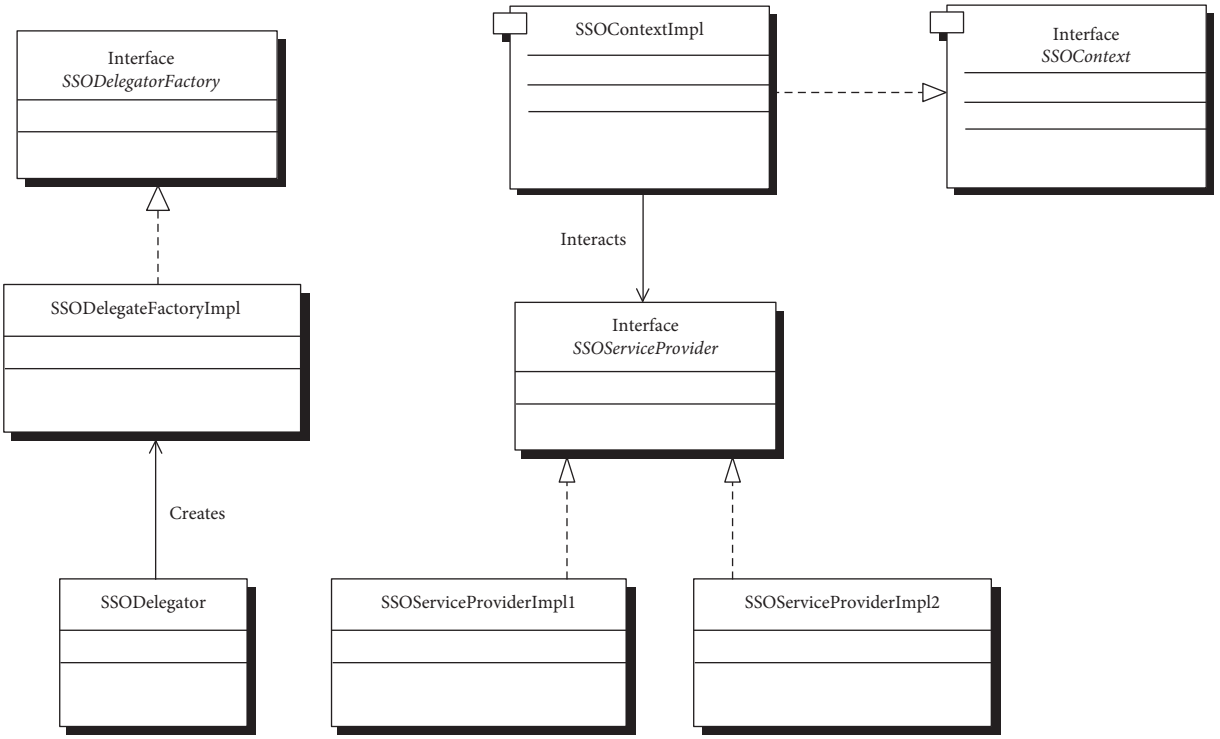


Figure 7: Proposed model class diagram. Source: [51].

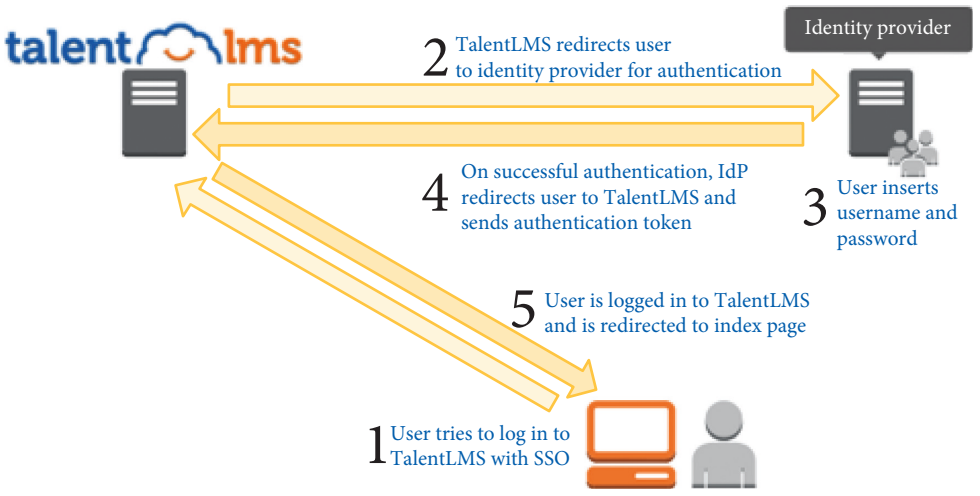


Figure 8: Single sign-on example. Source: [52].

voice authentication) to augment your password-based authentication [54].

Finally, regarding the management of educational resources, which are stored in repositories with access control, SSO implementation guarantees access to these resources, performing a validation process of credentials from a centralized node. In this node, each one of the LMS that wants to query resources is registered. In this registration process, each application requests credentials validation to carry out access to resources. When a user wants to query a resource in a repository (which has valid credentials), one of the following scenarios could happen:

(a) User is logged in into the centralized authentication node: if the user has previously accessed the centralized authentication module, this user will have access credentials for all those applications or repositories registered in the centralized node, so that credentials validation would be transparent to the user, allowing him/her to access to the educational resource.

(b) User is not logged in, but if he/she is registered in centralized authentication node: when user tries to query the educational resource, a credential restriction will not allow him/her to query this

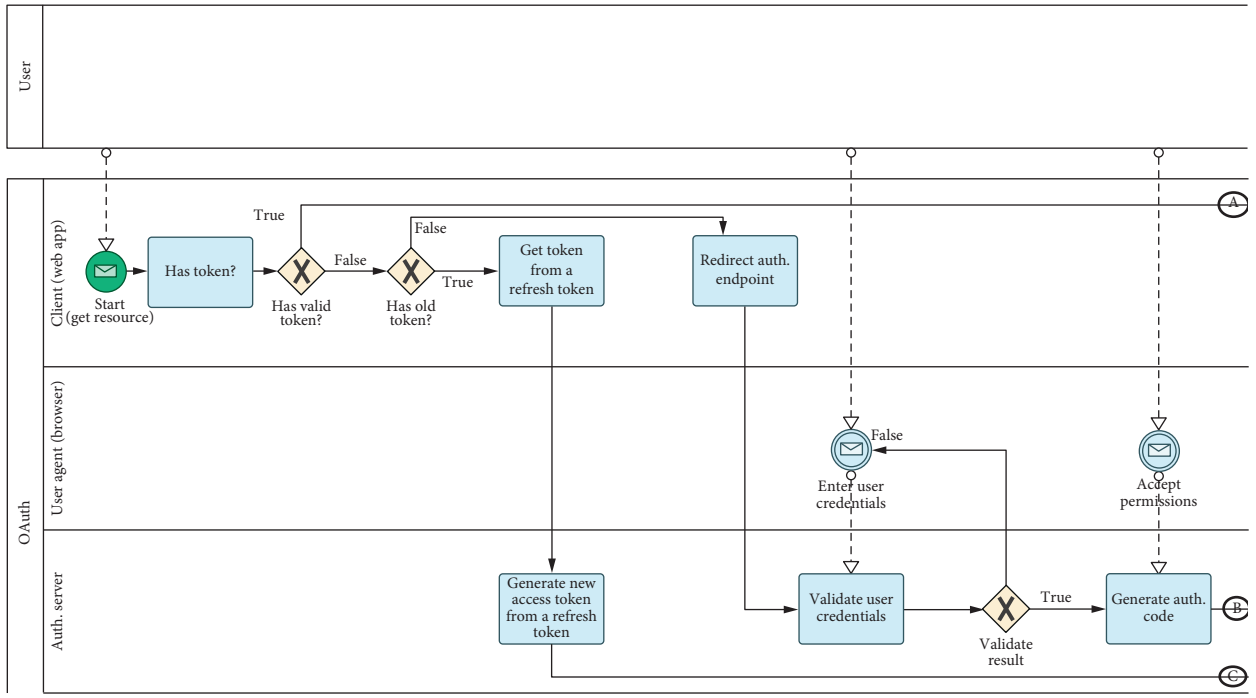


Figure 9: OAuth 2.0 authorization code grant: first part. Source: [55, 56].

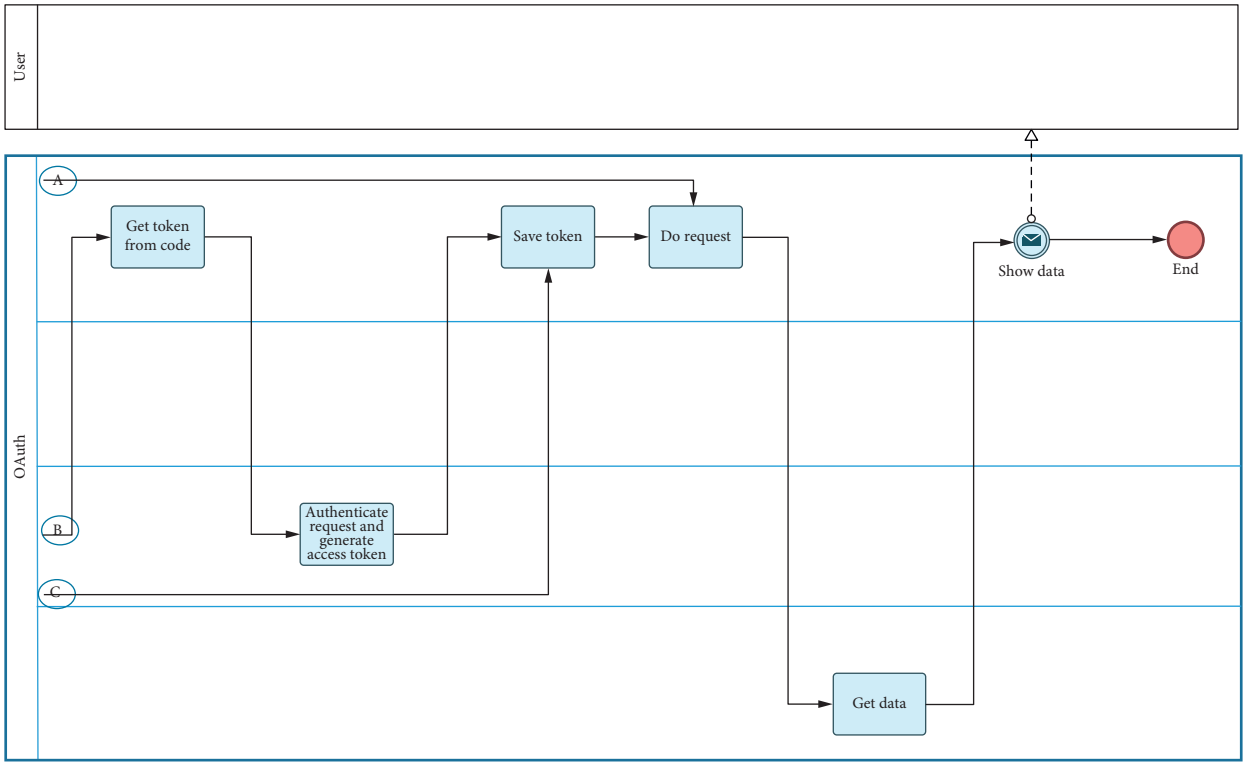


Figure 10: OAuth 2.0 authorization code grant: second part. Source: [55, 56].

resource, unless he/she accesses the application from the centralized node or from the application itself.

(c) User is neither logged nor registered: this case is similar to the previous one; therefore, the process will be the same. Additionally, an option to register and query the educational resources will be offered by the centralized node.

In a nutshell, metamodel design for the security dimension abstraction, and specifically different LMS and

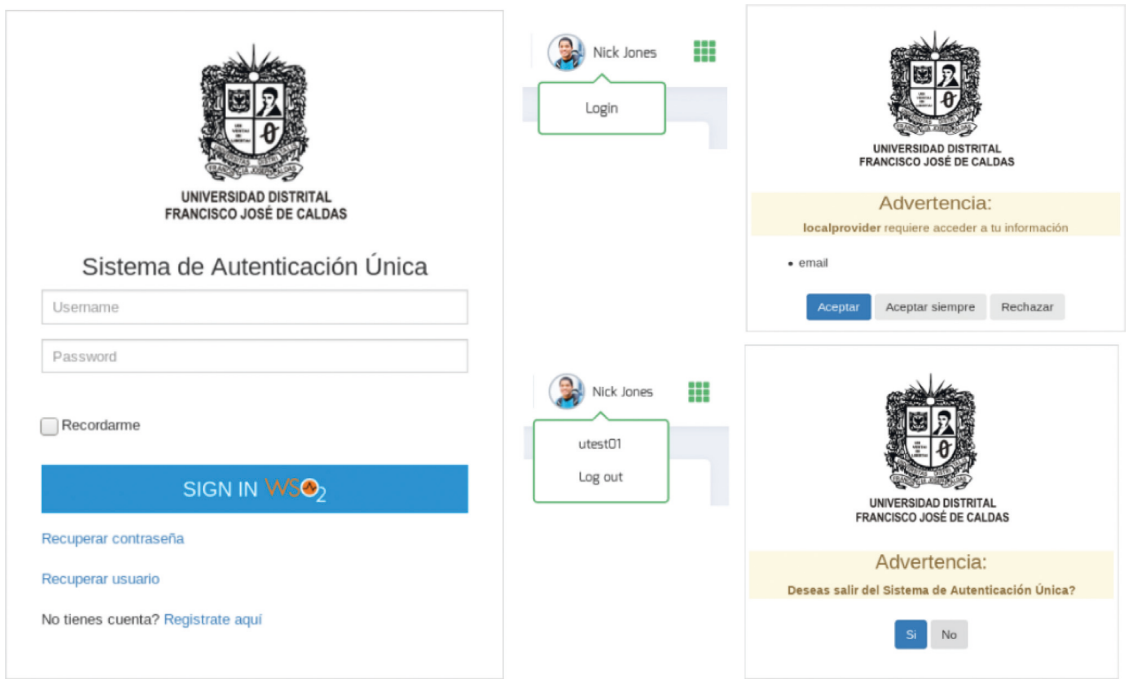


Figure 11: Proposed SSO: UDistrital. Left: login. Right: access authorization (above) and logout confirmation (below). Source: [57].

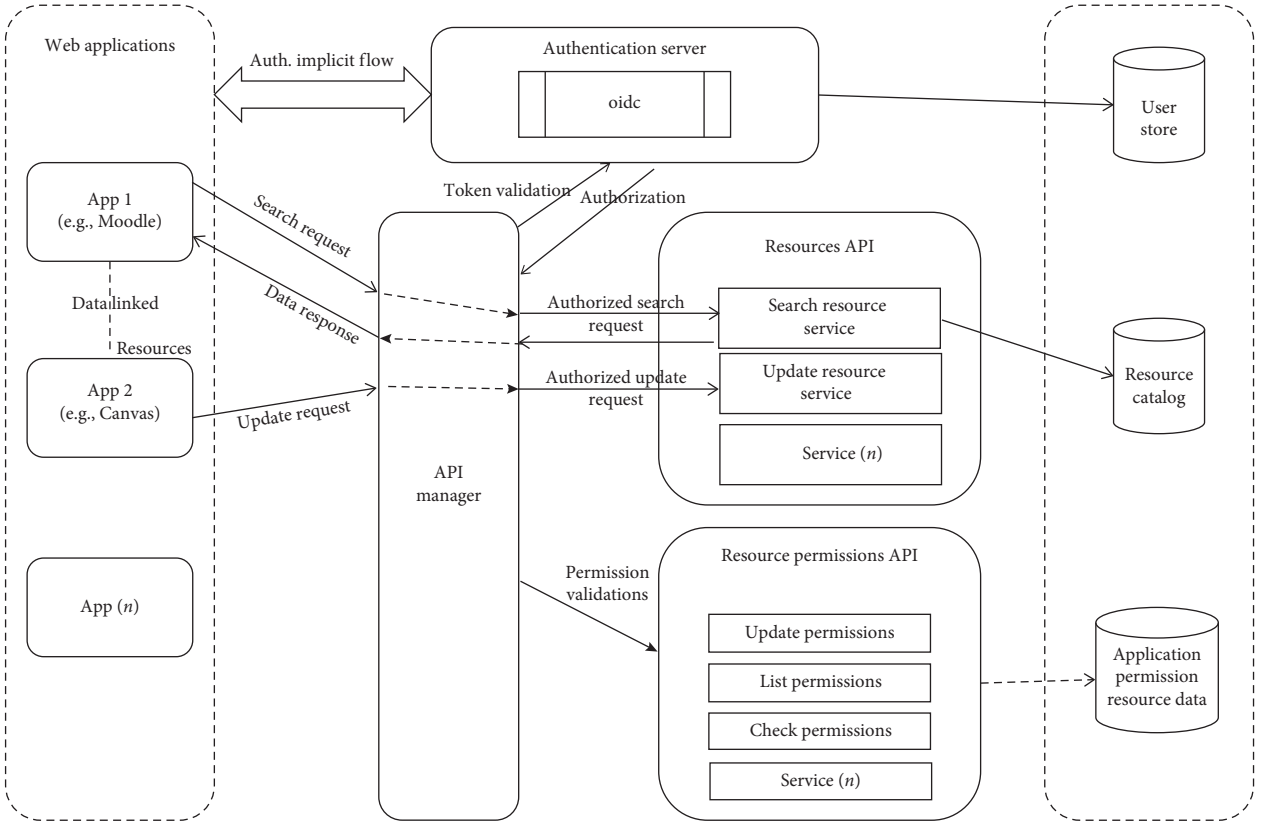


Figure 12: Architecture SSO: UDistrital. Source: authors.

authentication of integrated applications, is configured as a strategy, which provides an authentication unifying model. This model provides users with a single set of authenticating factors, which authorize applications under them authenticated. However, task of integrating each authentication scheme from different LMSs, where each one handles its own authentication model, is configured as restriction basis that metamodel must carefully manage, so that entities, attributes, and messages exposed perform corresponding mapping to each of the authentication instances. Derived

from this, use of design patterns becomes a priority strategy when designing models.

Briefly, abstraction level offered by MDA becomes a useful tool when planning authentication scenarios, not only for access and authorization in LMS, but in different environments where applications are integrated and required to simplify user identification and authentication process.

6. Conclusion and Future Works

MDA, besides raising different abstraction levels, which are represented in models, allows the automatic code generation using built models. For this purpose, MDA makes use of metamodels, which correspond to a set of domain concepts to be modeled and the existing relationships between them, defined in an abstract way. The metamodels allow carrying out a better abstraction of the knowledge domain, through the identification of concepts, rules, restrictions, etc., which operate in the domain, facilitating their understanding.

Regarding the main aspects to be taken into account for the authentication metamodel definition for accessing the LMS, and the use of linked open educational resources, for the model back-end, the metamodel should consider (1) the identification and characterization of the authentication schemes from the different applications that are to be integrated and (2) the authentication factors identification and the mechanisms used to carry out this task. These elements provide relevant criteria and restrictions that are raised in the metamodel. These criteria are implemented in the design of the proposed model, through (a) entities that participate in the authentication process, (b) attributes or authentication factors which are mapped to different schemes, and (c) messages which are sent and received among different entities that participate in model instances.

Regarding the model's front-end, the metamodel must consider the parameterization of restrictions on authentication factors, which are requested from the user. Using this parameterization process, the factors can meet all necessary requirements in order to be mapped, by the integrated authentication unit, with each application authentication scheme, which are integrated into the model.

In the authentication metamodel, the linked educational resources taxonomy, or the metadata provided, is not considered relevant, since at this level what is sought is to provide an access and authorization mechanism to the platforms that manage those resources. In the generation of model instances, considerations such as the following should be taken into account:

(i) With a single authentication point, authentication factors that authorize access and use of resources in different platforms are provided, according to the defined profiles. Therefore, the use of stronger authentication mechanisms should be considered, such as the use of multifactor authentication methods, which prevent unauthorized users from accessing information and resources that only have a password as an authentication factor.

(ii) In the authentication process, only information about the user's identity is provided. Authorizations about what is visible to each user should be verified separately in each application.

Taking into account the above, the use of metamodels for the authentication abstraction is configured as a strategy of the knowledge domain representation, which will allow to define restrictions and necessary components so that an administrator can add new authentication mechanisms, in addition to providing new applications to the model that implements these authentication mechanisms. Future works are proposed (a) to extend the metamodeling process to the other linked data quality dimensions, proposed in the framework research of this project; (b) to design a metamodel for the process of generating data models for linked open educational resources, based on linked data quality dimensions; and (c) to carry out the framework implementation, which allows verification of the proposed metamodel for the linked open educational resources; and finally, to develop a machine learning solution to measure the level of trust in different queried repositories, after validation of access credentials.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Disclosure

The current work has been developed within the doctoral research project framework on Linked Data at the Universidad Distrital Francisco José de Caldas. In the same way, Linked Data is also being worked as a research topic of the GIIRA Research Group.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Kleppe, J. Warmer, and W. Bast, *MDA Explained: The Model Driven Architecture: Practice and Promise*, Addison-esley, Boston, MA, USA, 2003, ISBN: 0-321-19442-X, https://dl.acm.org/citation.cfm?id=829557.

[2] Z. Bizonova, D. Ranc, and M. Drozdova, "Model driven e-learning platform integration," in *Proceedings of CEUR Workshop*, Busan, Korea, November 2007, http://ceur-ws.org/Vol-288/p02.pdf.

[3] V. García-Díaz, J. Tolosa, B. G-Bustelo, E. Palacios-González, O. Sanjuan-Martínez, and R. Crespo, "TALISMAN MDE framework: an architecture for intelligent model-driven engineering," in *Lecture Notes in Computer Science*, vol. 5518, Springer, Berlin, Germany, 2009.

[4] A. Rodrigues da Silva, "Model-driven engineering: a survey supported by the unified conceptual model," *Computer Languages, Systems & Structures*, vol. 43, pp. 139–155, 2015.

[5] D. Orozco, W. Giraldo, and H. Trefftz, *MDE; MDA; Transformaciones y DSLs. Una breve introducción*, Universidad Eafit, Medellín, Colombia, 2013, https://repository.eafit.edu.co/bitstream/handle/10784/5107/Articulo8CCC.pdf?sequence=4&isAllowed=y.

[6] F. Aguillón Martínez and M. Mateus Gómez, *Automatización del desarrollo de aplicaciones web mediante el enfoque MDA-MDE*, Facultad de Ingeniería, Pontificia Universidad Javeriana, Colombia, Bogotá, Colombia, 2014, https://repository.javeriana.edu.co/handle/10554/15572.

[7] B. Hyland, G. Atemezing, M. Pendleton, and B. Srivastava, *Linked Data Glossary*, W3C Working Group, Dublin, Ireland, 2013, https://www.w3.org/TR/ld-glossary/#linked-open-data.

[8] J. Herrera-Cubides, P. Gaona-Garcia, and S. Sánchez-Alonso, "The web of data: past, present and ¿future?," in *Proceedings of XI Latin American Conference on Learning Objects and Technology (LACLO)*, pp. 1–8, San Carlos, AL, Costa Rica, October 2016.

[9] J. Herrera-Cubides, P. Gaona-García, J. Alonso Echeverri, K. R. Vargas, and A. Gómez Acosta, "A Fuzzy logic system to evaluate levels of trust on linked open data resources," *Revista Facultad de Ingeniería*, no. 86, pp. 40–53, 2018.

[10] P. Gaona-García, A. Fermosa-García, and S. Sánchez-Alonso, "Exploring the relevance of europeana digital resources: preliminary ideas on europeana metadata quality," *Revista Interamericana de Bibliotecología*, vol. 40, no. 1, pp. 59–69, 2017.

[11] P. Gaona-Garcia, K. Gordillo, C. Montenegro-Marin, and A. Gómez-Acosta, "Visualizing security principles to access resources based on linked open data: case study DBpedia," *Information: An International Interdisciplinary Journal*, vol. 21, no. 1, pp. 109–122, 2018.

[12] J. Herrera-Cubides, P. Gaona-García, and K. Gordillo-Orjuela, "A view of the web of data. case study: use of services CKAN," *Revista Ingeniería*, vol. 22, no. 1, pp. 111–124, 2017.

[13] A. Zaveri, A. Rula, A. Maurino, R. Pietrobon, J. Lehmann, and S. Auer, "Quality assessment methodologies for linked open data. a systematic literature review and conceptual framework," *Semantic Web Journal*, vol. 7, no. 1, pp. 63–93, 2012.

[14] F. McSweeney, "Five reasons to use single sign-on (SSO) with Workable," Workable, 2018, https://blog.workable.com/use-sso-with-workable/.

[15] E. McKeown, "What is single sign-on (SSO)? Ping identity, 2017, https://www.pingidentity.com/en/company/blog/2017/08/23/what_is_single_sign-on_sso.html.

[16] GSI, "Seguridad informática," Grupo de Seguridad informática, 2018, https://eva.fing.edu.uy/pluginfile.php/58016/mod_resource/content/6/FSI-2018-IAA.pdf.

[17] J. Lanza Calderón and L. Sánchez González, "Seguridad en Redes de Comunicación," in *Grupo de Ingeniería Telemática*, Departamento de Ingeniería de Comunicaciones, Universidad de Cantabria, Santander, Spain, 2015, https://ocw.unican.es/course/view.php?id=28.

[18] Mentor, "Mecanismos básicos de Seguridad," in *Seguridad Informática*, Torrelavega, Spainhttp://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/mecanismos_bsicos_de_seguridad.html.

[19] IBM, *Identificación y Autenticación*, IBM Knowledge Center, New York, NY, USA, 2016, https://www.ibm.com/support/knowledgecenter/es/SSFKSJ_7.5.0/com.ibm.mq.sec.doc/q009740_.htm.

[20] J. Montoya and Z. Restrepo, "Gestión de identidades y control de acceso desde una perspectiva organizacional," *Ingenierías USBMed*, vol. 3, no. 1, pp. 23–34, 2012.

[21] RedIris, *Autenticación de usuarios*, Red Académica y de Investigación Nacional Iris, Madrid, Spain, 2008, https://www.rediris.es/cert/doc/unixsec/node14.html.

[22] Oracle, *Guía de administración del sistema: servicios de seguridad*, Oracle, Redwood City, CA, USA, 2011, https://docs.oracle.com/cd/E24842_01/html/E23286/toc.html.

[23] E. Ruckhaus, M. Vidal, S. Castillo, O. Burguillos, and O. Baldizan, "Analyzing linked data quality with LiQuate," in *The Semantic Web: ESWC 2014, Lecture Notes in Computer Science*, vol. 8798, Springer, Berlin, Germany, 2014.

[24] J. Pattanaphanchai, "DC proposal: evaluating trustworthiness of web content using semantic web technologies," in *Lecture Notes in Computer Science*, vol. 7032, Springer, Berlin, Germany, 2011.

[25] A. Rula and A. Zaveri, "Methodology for assessment of linked data quality," in *Proceedings of LDQ 2014, 1st Workshop on Linked Data Quality*, pp. 1–4, Leipzig, Germany, September 2014, http://ceur-ws.org/Vol-1215/paper-04.pdf.

[26] F. Radulovic, N. Mihindukulasooriya, R. García-Castro, and A. Gómez-Pérez, "A comprehensive quality model for Linked Data," *Semantic Web*, vol. 9, pp. 3–24, 2018.

[27] C. C. T. Di Noia, B. Marcu, and M. Matera, "A quality model for linked data exploration," *Web Engineering, Lecture Notes in Computer Science*, vol. 9671, pp. 397–404, Springer, Berlin, Germany, 2016.

[28] C. Bizer, P. Mendes, Z. Miklos, J. Calbimonte, A. Moraru, and G. Flouris, "D2.1 conceptual model and best practices for high-quality metadata publishing," Technical Report, Planet Data, 2012, https://www.planet-data.eu/results/deliverables.html.

[29] D. Pons, J. Hilera, and C. Pagés, "La estandarización para la calidad en los metadatos de recursos educativos virtuales," in *Proceedings of IV Congresso Internacional sobre Qualidade e Acessibilidade da Formação Virtual*, Leiria, Portugal, July 2013, http://www.esvial.org/wp-content/files/estandarizacionmetadatosPonsHileraPages.pdf.

[30] A. Zaveri, A. Rula, A. Maurino, R. Pietrobon, J. Lehmann, and S. Auer, "Quality assessment for linked data: a survey, a systematic literature review and conceptual framework," 2012, http://www.semantic-web-journal.net/system/files/swj773.pdf.

[31] C. Castro, *Montoya. Configuración de software basada en metamodelos y modelos*, Repositorio Universidad de los Andes, Bogotá, Colombia, 1992, http://repositorio.uniandes.edu.co/xmlui/handle/1992/3991.

[32] V. García Díaz, E. Núñez Valdez, J. Espada, C. Pelayo García, J. Cueva Lovelle, and C. Montenegro Marín, "Introducción breve a la ingeniería dirigida por modelos," *Revista Tecnura*, vol. 18, no. 40, 2014.

[33] V. García Díaz, H. Fernández-Fernández, E. Palacios-González, C. Pelayo, O. Sanjuán-Martínez, and J. Cueva Lovelle, "TALISMAN MDE: mixing MDE principles," *Journal of Systems and Software*, vol. 83, no. 7, pp. 1179–1191, 2010.

[34] V. García Díaz, *MDCI: Model Driven Continuous Integration*, Departamento de Informática, Universidad de Oviedo, Oviedo, Spain, 2011, http://www.tdx.cat/handle/10803/80298.

[35] C. Montenegro Marín, P. Gaona García, J. Cueva Lovelle, and O. Sanjuan Martínez, "Aplicación de ingeniería dirigida por modelos (mda), para la construcción de una herramienta de modelado de dominio específico (dsm) y la creación de módulos en sistemas de gestión de aprendizaje (lms) independientes de la plataforma," *Revista Dyna*, vol. 78, no. 169, 2011, http://www.scielo.org.co/pdf/dyna/v78n169/a05v78n169.pdf.

[36] C. Montenegro, J. Cueva, O. Sanjuán, and P. Gaona, "Desarrollo de un lenguaje de dominio específico para sistemas de gestión de aprendizaje y su herramienta de

implementación KiwiDSM mediante ingeniería dirigida por modelos," *Revista Ingeniería*, vol. 15, no. 2, pp. 67–81, 2010.

[37] Evidian, *Los 7 métodos de autenticación más utilizados*, Evidian, New York, NY, USA, 2015, https://www.evidian.com/pdf/wp-strongauth-es.pdf.

[38] F. Sotelo Gómez and M. Solarte, "Incorporación de recursos web como servicios de e-learning al sistema de gestión de aprendizaje. LRN: una revisión," *Tecnura*, vol. 18, no. 39, pp. 165–180, 2014.

[39] WizHosting, *Soluciones Web enlatadas*, WizHosting InternetServices, London, UK, 2015, http://www.wizhosting.com/e-learning.

[40] UDistrital, *Interfaces de Logueo Sistema Académico y LMS*, UDistrital, Bogotá, Colombia, https://funcionarios.portaloas.udistrital.edu.co/urano/.

[41] M. Rojas, J. Montilva, and M. Hurtado, "Diseño de repositorios de objetos de aprendizaje como estrategia de reutilización e integración de contenidos en modelos de educación virtual," in *Proceedings of 11th LACCEI Latin American and Caribbean Conference for Engineering and Technology*, Cancun, Mexico, August 2013, http://www.laccei.org/LACCEI2013-Cancun/RefereedPapers/RP240.pdf.

[42] Tecnoinver, *Qué es Single Sign-On o Autenticación Única*, Tecnoinver: Cloud, Datacenter y Hosting, Santiago, Chile, 2015, https://www.tecnoinver.cl/que-es-single-sign-on-o-autenticacion-unica/.

[43] C. Mainka, V. Mladenov, J. Schwenk, and T. Wich, "SoK: single sign-on security—an evaluation of openID connect," in *Procedings of 2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 251–266, Paris, France, April 2017.

[44] 9Series, *How Single Sign On Authentication Work?*, 9Series HandCrafted Technology Solutions, Ahmedabad, Gujarat, 2017, https://www.9spl.com/blog/how-single-sign-on-authentication-work/.

[45] C. Scott, D. Wynne, and C. Boonthum-Denecke, "Examining the privacy of login credentials using web-based single sign-on–are we giving up security and privacy for convenience?," in *Proceedings of 2016 Cybersecurity Symposium (CYBERSEC)*, pp. 74–79, Coeur d'Alene, Idaho, USA, April 2016, https://www.computer.org/csdl/proceedings/cybersecsym/2016/5771/00/07942428.pdf.

[46] B. Zwattendorfer, A. Tauber, and T. Zefferer, "A privacy-preserving eID based Single Sign-On solution," in *Proceedings of 2011 5th International Conference on Network and System Security*, pp. 295–299, Milan, Italy, September 2011.

[47] Y. Chen, B. Xia, B. Wu, and L. Shi, "Design of web service single sign-on based on ticket and assertion," in *Proceedings of 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce AIMSEC 2011*, pp. 297–300, Zhengzhou, China, August 2011.

[48] M. Beltrán, M. Calvo, and S. González, "Federated system-to-service authentication and authorization combining PUFs and tokens," in *Proceedings of 2017 12th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC)*, pp. 1–8, Madrid, Spain, July 2017.

[49] UC, *Configuración correo IMAP*, Universidad de Cantabria, Santander, Spain, https://sdei.unican.es/paginas/servicios/correo/manual_imap.aspx.

[50] J. Szczegielniak, *Introducing Single Sign-on to an Existing ASP.NET MVC Application*, RedGate Hub, Cambridge, UK, 2015, https://www.red-gate.com/simple-talk/dotnet/asp-net/introducing-single-sign-on-to-an-existing-asp-net-mvc-application/.

[51] C. Steel, R. Lai, and R. Nagappan, *Core Security Patterns: Securing the Identity--Design Strategies and Best Practices*, InformIT, Pearson, Carmel, Indiana, 2009, http://www.informit.com/articles/article.aspx?p=1398626.

[52] D. Kaplanis and TalentLMS, *Integrating Single Sign-On with your Cloud LMS*, TalentLMS Features & Updates, London, UK, 2014, https://www.talentlms.com/blog/integrating-single-sign-on-with-cloud-lms/.

[53] D. Parr, *LMS SSO with ONELOGIN*, Paradiso Solutions, Maharashtra, India, 2017, https://www.paradisosolutions.com/blog/lms-sso/.

[54] MiniOrange, *Single Sign On (SSO)*, MiniOrange, Maharashtra, India, 2018, https://www.miniorange.com/canvas-single-sign-on-(sso).

[55] D. Hardt, *The OAuth 2.0 Authorization Framework*, RFC 6749. Internet Engineering Task Force (IETF), Fremont, CA, USA, 2012, https://tools.ietf.org/html/rfc6749.

[56] Pradas, *BPMN OAuth 2 0 Authorization Code Grant, GenMyModel*, Pradas, Milan, Italy, 2018, https://repository.genmymodel.com/pradas/BPMN-OAuth.2.0.Authorization.Code.Grant.

[57] G. Salcedo, *Dashboard Proyecto de Investigación SSO*, Universidad Distrital Francisco José de Caldas, Bogotá, Colombia, 2018, https://autenticacion.udistrital.edu.co/dashboard.

[58] J. Martin, *Implantación de un SSO (Single Sign On), Master interuniversitario en Seguridad de las tecnologías de la información y de las Comunicaciones (MISTIC)*, Universidad Oberta de Cataluña, Barcelona, Spain, 2008, http://openaccess.uoc.edu/webapps/o2/bitstream/10609/28021/6/nacho_martinTFM0114memoria.pdf.

[59] P. Sheriff, "Single Sign-On Enterprise Security for Web Applications," *Microsoft Developer Network*, PDSA, Inc., Bristol, UK, 2004, https://msdn.microsoft.com/en-us/library/ms972971.aspx#singlesignon_topic10.