Identity Authentication and Data Access Authorization in Regional Education Informatization

Qi Feng, ZhongLin Chen, FuKe Shen And YuHong Zhu

Abstract—During the procedure of the Region-informatization, there are encountered different types of challenges. Playing the key roles in the construction mechanism, Governments, Universities, and enterprises are building their own information systems that are unable to be interoperable because of lacking interconnection standard. So these systems' effective data-sharing mechanism poses to be a major point of concern. In this paper, from the top design of informatization eco-system, we are going to conduct discussion on the roles played by these participants in addition to the mechanism which these participants' system is to interconnect, so that we could enhance the development of Region-informatization. We consider the Authentication System built in Shanghai Education as an illustration together with showing the process, design, implementation and the current situation comprehensively. The new approaches in this paper is to provide a fusion scheme of Oauth2 and Shibboleth, which combines the advantages of both. And in the maintenance on federation, provide some methods and practices to improve service level

Key words: Authentication; cross-region authentication; Shibboleth; Oauth2

I. INTRODUCTION

In the development of regional informatization, there are encountered three key challenges:
Difficult to Share Information: because of historical reasons, resources of the Government, educational institutes and internal departments mostly develop the exclusive monopoly as well as lack of communication between one another, eventually leading to the difficulty to information sharing.

Difficulties of Data Analysis: owed to the lack of a scientific top-level design, an immaculate coordination and information construction and an independent development of information resources construction in organization, capital and system, the construction remained at a low level that also drove data collection incomplete. These issues brought forth gigantic difficulties in data analysis. Thus, the Big Data analysis in regional education has emerged as an empty slogan.

No Cohesion among Government, Educational Institutes and Enterprises: currently, the main body of the regional education informatization comprises three aspects: government, educational institutes, enterprise. Among them, government provides financial support to multiple independent projects without taking into consideration the data-sharing with one another, leaving behind one another “information islet”; the educational institution also possesses a large number of low level analogous function information systems constructions. Repeated construction, constrained staffing and ineffective system function result into low profits in informatization; despite the fact that enterprises have some participatory enthusiasm, the cooperation between them and educational institutions is quite fossilized under the current strategy. Nonetheless, lots of companies are showing their interests in participating in the cooperation, but they cannot find the entry point to start with.

II. THE TOP-LEVEL DESIGN OF REGIONAL INFORMATIZATION

In the mechanism of regional informatization, it is more than important to clarify the responsibilities of different participants together with making clear the relationships among them. The top-level design of informatization should throw emphasis on the design of the overall framework of the regional information system, as well as the design of information infrastructure that could support multiple construction bodies, for the purpose of developing a regional information ecosystem. Meanwhile, we are required to respect the independence of the main body in addition to making not
interference in the procedure of information planning, management system, etc. The following issues throw emphasis on the relationship between identity management and resource sharing in order to delineate the different responsibilities of educational institutes, governments and enterprises in the top-level design.

Educational Institute: Educational institutes supervised and identified, correspondingly together with supplying functional education resources.

User of education information system is primarily the teachers and the students, whereby their identification is entirely supervised by their respective institutes. The authorization mechanism in cyberspace should constitute the physical world. That is why academic institutes are required to bring forth reasonable solutions, construct effective identity authentication system, and provide authentication services for its users. It also delivers corresponding types of application authorization in respect of different users.

Conversely, each academic institute is inclined towards having a huge amount of characteristic resources, whereby, how to derive the value of these resources must be taken into consideration. The sharing of school resources should throw light on these distinctive applications.

Government: Government is the primary construction body of the information infrastructure that is capable of interconnecting multiple identities and the application resources. Moreover, it helps form a scientific and reasonable sharing mechanism.

It is quite tough to standardize the application of academic information system as a unified product to satisfy all user requirements. Government should put to use this infrastructure along with corresponding stimulus strategy in order to motivate enterprises and educational institutes for delivering topnotch and different personalized service together with making full use of the resources of each application.

Enterprises: Enterprises possess advantages when it comes to producing different applications and resources. Furthermore, they can provide high quality services.

Good educational information ecosystem is unable to perform without the participation of enterprises. Enterprises can bring forth the personalized applications for different users. Enterprises are required to assume the responsibility of the development of academic information ecosystem, share responsibility, in addition to getting reasonable commercial profit.

A sustainable regional education information framework should comprise three key aspects: authentication, authorization and data-sharing.

Authentication: Each user’s authentication has been the responsibility of its own the organization. Each individual should pose the full trust in the results of authentication from other providers in the federation.

Authorization: Authorization can be segregated in two aspects:

On the first place is the Authorization for recourse access, also termed as user authorization. For instance, we can define a user’s access limits that he can only read. Authorization should be based on different individual’s features, for instance, users can be authorized different roles to distinguish between staff and students.

On the second place is the Authorization for different application development participant, also called application authorization, for instance, what kind of application can participate in ecosystem? How much educational resource can be utilized by these application developers? And, what operation they can perform on the data in the infrastructure? All of these proposals should be controlled by application authorization.

Data-sharing: Data builds the base of the information infrastructure. Data-sharing mechanism is quite significant to support the top-level design as well as to supply personalized service to users. A productive educational ecosystem should include user elementary data together with user behavior data.

User elementary Data is associated with the user’s identity and personal information. Elementary data is primarily collected offline. Once the user is transferred to online character, the elementary data will be entered into the online system.

User behavior Data is defined as the data logging user behavior as well as the data produced by operation system.

These two kinds of data contribute towards the bases of Big Data analysis.

Authentication, Authorization and Data-sharing should be encapsulated in different services, together with being openly provided to every participant, with Application Program Interface (API).

For the purpose of supporting several construction participants as well as users from multiple educational institutes, authentication must be accomplished by the organization itself. The authentication findings of multiple organizations are required to be trusted by each other in the regional federation. Shibboleth is an open source and a quite effective solution to this issue.

Shibboleth poses to be standard open source software that allows users to archive login through web, which belongs to the same federation. When a user visits protected resources, Shibboleth provides safe as well as private identity authentication services.

There are three constituents of Shibboleth:

IDP (Identity Provider): IDP Client: The key function of IDP deals with validating users together with providing user’s attribute to resource providers. In accordance with their attributes, the server would response to user’s activities.

SP (Service Provider): SP client: The key role of resource service provider deals with responding to user’s request together with inquiring the attribute of the user from IDP that belongs to it. Thereafter, in accordance with the result of inquiry, SP will decide whether user is allowed to visit the resource or not.

DS (Discovery Service): Discovery Service acquires the responsibility to guide users to go to their own IDP for authentication.

As presented in Figure 1, it represented a logic framework of Shibboleth.
As user’s visit the resources from the Federation, the data flow will go through the following steps, in Figure 2:

A. User makes request to get access to the protected resources.

B. SP judges if the status of user has been authenticated, contrarily, it redirects the data to DS.

C. User chooses the IDP of his own organization on the DS.

D. Requesting authentication to the IDP selected by the user.

E. Authenticating.

F. IDP sends a message containing user’s confirmed identity to SP.

G. SP makes request for user’s attribute from IDP.

H. In accordance with the rules that have already been agreed by federation organizations, IDP sends relevant attributes to SP.

I. Because of user’s attributes, SP finishes procedure of authorization.

SEAC unified authentication center performs the key function of providing distributed authentication, centralized authorization and data-exchange services in dock application market. Application is authorized with the use of the open interface of oauth2, and the cross-organization authentication docking shibboleth for distributed authentication is done during the process of authorization. Through the transmission of users’ attribute data, information in identity authentication center platform SEAC will be integrated as well as cleaned. Thereafter, packaging as a unified standard formation and as an API interface is to be issued for the applications’ calling.

This requires the application of additional work for data data cleansing. But now the work has done by the SP Proxy. For applications, the data returned by the API is always standard.
and consistent, which is more appealing to the developer.

In conclusion, SEAC makes use of an authorization mode, termed as Oauth2, which is the mainstream of the Internet authentication with fast access and conduciveness to promote. In respect to cross-organization authentication user, the authentication data flow through the authentication center, and then redirect to the application that accords an opportunity for SEAC to carry out data cleaning. Moreover, it is conducive to standardize data structures, and also helpful for the promotion of the application docking. So, we are able to construct an open platform for authentication like Google/Facebook/Github through the SEAC Center, and form an ecosystem of regional education informatization.

SEAC is meant to deliver services to the whole society of Shanghai education. Furthermore, it is important to guarantee the reliability of its services. That is how the monitoring of the SEAC is of utmost importance as well. Nonetheless, owed to the multiple participation bodies of federal authentication framework that is quite different from that of single main body, it is quite tough to consider a strong monitoring program in it. We can only make use of different schemes of gathering monitor information in accordance with the distinguished objects in framework, display and alarm to users with the help of a unified monitor platform.

There are two types of monitoring applications in regional informatization authentication framework:

One type is the Applications supported directly by regional informatization administrator, just like that deliver the interface to Oauth2. We can utilize a robust collecting method to these applications. For instance, it is possible to arrange Agent on the server directly for the collection of the status as well as logs of it, in addition to reporting to the monitoring platform.

Secondly, there are Applications supported by regional informatization participators, as IDP delivered by educational institutes. These kinds of applications’ objects are placed in each respective educational institute. This is why we recommend them to utilize a polite technique for the purpose of monitoring the running status, as well as reporting to the platform.

The monitor framework is illustrated by Figure 4

For example, we conduct monitoring of the http status interface of IDP with the help of the platform, check the status of one IDP and then report it to the platform sporadically. If an IDP node is shut down, the collector will receive an error code, and the platform would take the alarm as per requirements.

The following pictures delineate the average latency time for the request of 4 IDP nodes, whereby the unit is milliseconds (ms).

Owed to the fact that the SEAC informatiation administrator extends support to the DS node directly, we are capable of collecting quite detailed information of application. We can not only collect the information of CPU, space, disk IO status, but also the average amounts of authentication requirements through collection and analysis of DS server’s logs. The statistical analysis did away with some worthless requests, so it showcases more accuracy in comparison with the average daily page views.

As presented in the following figure, Shanghai SEAC’s request makes period appearances during the semester, being low in the summer as well as winter holidays. This is owed to the fact that, in the term of weekends, teachers and students have frequent cross-organization communications, thus leading to more uses of wireless communication based on SEAC.

Being a distributed authentication framework adopted by the federal authentication, the quality of user authentication service is dependent on each IDP node whereas the fact suggests that the IDP node service quality can’t be controlled where there is likely to be a very superior quality of IDP together with the existence of services unavailable frequently as well as inability of provision of normal service’s IDP. The congenital loose type federated authentication of alliance architecture poses to be the key cause. Nonetheless, SP is always interested in becoming capable of getting a stable certification experience in accordance with their expectations, for unstable certification experience is difficult to be promoted and dissipated that will become certified resistance for the alliance’s developing. We have tried a variety of ways to
improve the Federation’s Service level:

If the IDP is also important function within a university, more stable operation will be expected. Therefore, we work with vendors which provide identity authentication solution for universities. In the future, we will make federal identity module integrated into the university identity authentication system. Then IDP will be the important function within a university. This cooperation is under negotiation.

For some small, technically weak universities, we provide IDP function as a SaaS (IDaaS), for free. The service has been tested and verified, and will be officially launched in the second half of 2017.

Some universities do not want to use cloud services. We provide remote support services based on Jumpserver. Jumpserver will record all the operations logs. So we can provide them with a safe and controllable idp remote operation and maintenance.

The most important is IDP classification and certification. Incommon assurance has awarded an IDP certification scheme on the bases of security considerations. In addition to the certification scheme, we also believe that we are capable of rating the attributes that have provided responses as per service stability, response Time (such as 5*8, 7*24) and other comprehensives by the IDP. With the help of the evaluation and monitoring by some third party organization, we should award a topnotch certification to those IDPs that deliver exceptional services. In the meantime, the results of evaluation and monitoring displayed online would provide SP with a clear and predictable certification experience. SP can also adjust their service object in accordance with the results of the IDP level analyses, together with promoting and publicizing with a clear target.

IV. PRACTICE IN SHANGHAI

On the bases of Shanghai SEAC, we engineer numerous education applications, docking to current system in addition to providing large amount of state-of-the-art resources. Cross-organization authentication system disseminates in a rapid and broad manner, together with offering a friendly interface to users. Thereafter, we’ll introduce three distinguishing cross-organization applications as hereunder:

1. Shanghai Educational Cross-organization Wi-Fi (SECW)

Shanghai Educational Cross-organization Wi-Fi (SECW) system offer wireless resource sharing. Moreover, this technology is quite identical to the global wireless roaming framework—Eduroam that allows users to visit the sharing resource in any supported college, once his own account gets successfully authenticated.

The technology of Eduroam is based on 802.1x and radius, in addition to fully taking the distributed management that asks for more technology management for those schools that are providing roam services. Nonetheless, SECW is based on web portal that puts to application the management of half-centered and half-distributed that requires comparatively less technology management together with being handier to popularize.

As of December 2016, SECW owned an aggregate of 40 units in order to support Shanghai Educational Wireless roaming that also included 3 Bureau of Education (covering the identity authentication in primary and secondary schools of the bureau). All through the same period, there are 4 colleges that support Eduroam.

2. Cross-organization Education By Universities from Northeast Shanghai

In order to motivate academic resource sharing, Shanghai Municipal Education Commission supports the development of inter-course enrollment system on the bases of SEAC serviced for 12 universities in Shanghai Northeast Region. It allows students from all of the 12 member universities including Fudan University, Tongji University, Shanghai University of Finance and Economics etc. to participate in the short courses run by other colleges. Once a student passes the exams, he would secure the certificate for the same course awarded by the host university. The platform of intercollegiate education by universities from northeast Shanghai(http://www.kxxfx.shec.edu.cn) puts to use the SEAC authentication for the purpose of transferring users’ attribution, while avoiding rebuilding accounts for users, at the same time, bringing convenience to those who would take part in the other college’s minor courses.

3. Construction and Sharing Platform of High Quality Resources in Shanghai Area

Construction and sharing platform of high quality resources in Shanghai area (http://www.kxzy.sh.edu.cn) is a resource sharing project that receives the support from Shanghai Municipal Education Commission, while aiming at the collection of every university’s database, characteristic data and high quality resources. As of now, the platform possesses
integrated 12 colleges’ high quality databases, including Fudan University, Tongji University, Shanghai Normal University, East China Normal University, etc. The databases house a diverse variety of different types of resources, for instance books of Republic of China, ancient books, ordinary reading material, teachers’ guides, degree thesis, etc. The platform possesses more than 300 thousand documents, whereby 85% of it offers the whole text of the original paper and 15% of the recourses offer the copies of documents. The entire authentication for the resources is based on SEAC.

4. Eastern Airlines Campus Promotions

Eastern Airlines Campus Promotions is one of the promotion activities that aim at educating the users, allowing the education users to purchase preferential tickets in APP once they’ve been authenticated. Actually, a large number of enterprises possess their own promotion policies in respect to educators, but it is not that convenient in auditing, together with encountering several issues in safety. Nonetheless, Eastern Airlines Campus Promotions is based on SEAC whereby the successful practice has earned bundles of compliments.

5. Shanghai Massive Intelligent Learning Environment (SMILE)

SMILE poses to be a platform that docked the third part providers with the use of oauth2.0 technology as based on SEAC technology. The platform aims to providing distinguished academic services, including relevant recourses, study materials, and numerous kinds of online courses that are also popular as “WeShare Science & Technology”.

With Oauth2 technology, WeShare Platform allowed users to login using numerous ways, for instance WeChat, QQ by Tencent, SEAC, etc. Being a SEAC user, the academic attribute of his own is likely to extend great support for the promotion of WeShare Platform, together with enhancing the quality of its’ service. The composition of login is presented as hereunder:

V. CONCLUSION AND PROSPECTION

The fundamental objective pursued by regional informatization is resource-sharing. As every participant is capable of living up to its potential together with letting each of the various organizations perform its own functions in the educational informatization ecosystem, government must offer prerequisite infrastructure as well as corresponding policies for the development of education resource prosperity through multi-agent participation. SEAC appears to be an exceptional technique. Based on the technology of cross-organization authentication, we carried out several trials on the sharing of Wi-Fi resource (SECW), learning resources and library resources that all exhibited unparalleled effects. In the meantime, in the practice of resource sharing, we have distributed to some extent its proposed standard specification and Identity Authentication System, and both of them attained great results.

In the future, we will put further efforts in three aspects. As regards the access as well as promotion of applications, we should benefit from SEAC Certification for its efforts on three aspects. In respect to the access and the promotion, the applicant should be deployed in a more simple and easy manner. In respect to the access and promotion of users, those pilot projects are expected to bring more high-qualified applications to the open platform. Positive feedback from users and their usage could be driven by applications. In respect to the stability and security of the system, it is the consolidated supervisory console that performs monitoring of the status of authentication nodes and applications. As for those nodes and applications are concerned, that lack system maintenance and are unwilling to keep maintenance, we should consent to their withdrawal as regards the enhancement of the platform, its service and the potential of supporting.

REFERENCES

[3] Xiong C.P. et al., 2010. Study on the development and application of educational information resources “regional co construction and sharing” [J]. Open Education Research, 2010(01)


Qi Feng Male, engineer at Information Technology Services Center of East China Normal University. Member of the authentication center in Shanghai Education Construction Team, major technology support in cross-organization certification of Shanghai municipal education. Research direction: infrastructure operation and maintenance monitoring, SSO, cross-organization authentication).

ZhongLin Chen Male, engineer at Information Technology Services Center of East China Normal University, major in software testing, services of campus informatization. Fuccous on trouble shooting in verity operation systems and school applications' management.

FuKe Shen Male, Professor, Senior Engineer in East China Normal University, director of the China Higher Education Information Acamy, member of Shanghai education and research computer network expert committee, vice chairman of Shanghai Association of Higher Education, director of Shanghai Education Science Network IPv6 Laboratory (ECNU) Research Center. Research direction: communication and network technology (network architecture, the next generation network protocol and implementation principle of network traffic monitoring and management), educational informatization / digital campus (SSO, cross domain authentication, e-learning, smart, campus). Corresponding author of this article.

YuHong Zhu Female, senior engineer, chief engineer of the information center of Shanghai Municipal Education Commission, engaged in the work of educational informationization, responsible for the technical management of Shanghai construction and application. And participated in a number of issues in the development of Informationization Education Research, including the evaluation index system of university informatization in Shanghai, Shanghai educational informatization planning and development research and cross-organization authentication system, etc..