SECURITATEA SISTEMELOR DE BIBLIOTECI VIRTUALE ÎN CONTEXTUL COLABORĂRII ÎN SPAȚIULUI EUROPEAN

Mihai Doinea

mihai.doinea@ie.ase.ro

Biblioteca Academiei Române

Rezumat: Articolul prezintă colaborarea ca fiind un proces de partajare de resurse. Sunt discutate aspecte principale care influențează procesele de partajare. Este expus conceptul de colaborare în sistemele de biblioteci virtuale şi propus un model de sistem colaborativ pentru partajarea de resurse digitale între mai multe entități de biblioteci virtuale din spațiul european. Sunt analizate caracteristicile principale ale securității, ținând cont de natura proceselor ce se desfăşoară în astfel de sisteme care partajează resursele digitale.

Cuvinte cheie: securitate, biblioteci virtuale, colaborare, sisteme.

Abstract: The paper presents the collaborative concept as being a process of sharing resources. The main aspects that are having a huge influence on these types of processes are debated. The concept of collaborativity in the context of virtual library systems is presented and a model of collaborative system for sharing resources between different virtual library entities from European area is proposed. The main security characteristics are analyzed keeping in mind the collaborative nature of the undergoing processes which manages the electronic resources.

Keywords: security, virtual libraries, colaborativity, systems.

1. Partajare şi colaborare

Partajarea reprezintă metoda prin care resursele unui sistem integrat de bibliotecă, denumit şi sistem care partajează, sunt utilizate de mai multe entități, fie acestea procese sau utilizatori, pe baza unui set de restricții, norme, ce reflectă felul în care acestea urmează să fie întrebuințate. Partajarea trebuie să țină cont de o serie de elemente ce definesc atât resursele, cât şi entitățile care le folosesc, precum:

- dimensiunea mulțimii partajate; după dimensiunea resurselor se poate discuta de următoarele tipuri de partajări:
  - partajare de tip 1 la n: aceeaşi resursă la mai mulți utilizatori; partajarea unei resurse la mai mulți utilizatori implică mecanisme specifice care să gestioneze accesul concurent la aceasta precum şi tehnici de înregistrare a operațiilor şi crearea unui jurnal al tuturor acțiunilor care au avut loc la nivelul acesteia;
  - partajare de tip n la n: mai multe resurse la mai mulți utilizatori presupune existența unui sistem pe baza căruia să fie alocate aceste resurse fără a crea dependențe între procesele de alocare;
- natura resurselor partajate; natura acestora determină modalități diferite de partajare, după cum partajarea unui obiect digital, stocat în cadrul unei biblioteci virtuale, este diferită de partajarea zonei de memorie din cadrul unui sistem informatic sau de cea a procesorului utilizat pentru efectuarea calculelor în două procese distincte.

Colaborarea este descrisă în [1] ca fiind procesul prin care un sistem are capacitatea de a gestiona un număr important de utilizatori care lucrează împreună pentru atingerea aceluiaşi obiectiv, folosind resurse proprii; o astfel de abordare se bazează pe un sistem complex de management al documentelor şi al proceselor distribuite. Colaborarea reprezintă un proces de partajare de resurse cu un nivel suplimentar de restricții care să specifice felul în care aceste resurse sunt partajate.

În cadrul unui proces colaborativ entitățile care utilizează setul de resurse lucrează pentru atingerea aceluiaşi obiectiv, fiecare procesare a resursei fiind direct dependentă de o alta, apriorică, cu excepția primei procesări.

În cadrul sistemelor integrate de bibliotecă, mecanismul de partajare şi colaborare sunt bine definite, întrucât intersecţia utilizatorilor şi a proceselor ce folosesc resursele generează o matrice a drepturilor de acces foarte complexă, [2]. Această complexitate poate fi tratată doar dacă la nivelul sistemului integrat de bibliotecă sunt prevăzute măsuri prin care resursele acestuia sunt utilizate corespunzător.

Un exemplu de partajare de resurse, în cadrul unui sistem integrat de bibliotecă, îl reprezintă felul în care fişele bibliografice sunt utilizate de către utilizatorii de sistem cu roluri diferite, funcţie de specificul activităţii acestora. Începând de la momentul creării unei fişe bibliografice, la nivelul serviciului de achiziţie, continuând cu completarea acesteia de către serviciul de catalogare şi până la momentul în care fişa intră în gestiunea serviciului de prezervare digitală, o fişă bibliografică suferă o serie de transformări menite să îmbogăţească patrimoniul cultural. Aceste modificări aduse de fiecare grup de utilizatori, respectiv de procesele care rulează în mod automat în plan secund, în cadrul sistemului integrat de bibliotecă cu rolul de a elimina redundanţele sau de a omogeniza conţinutul, trebuie să păstreze caracteristicile de bază ale informaţiei stocate la nivelul fişei bibliografice, fără a denatura în vreun fel calitatea expusă de aceasta.

Partajarea resurselor în sistemele integrate de bibliotecă este tratată diferenţiat la următoarele niveluri logice, toate componentele fiind perfect sincronizate pentru a nu periclita integritatea resurselor gestionate:

- baza de date în care sunt stocate obiectele bibliotecii virtuale; înregistrările stocate la nivelul bazei de date sunt protejate de mecanisme specifice de blocare a accesului în momentul în care sunt în curs de editare; astfel se evită suprascrierile nedorite în momentul în care mai mulţi utilizatori doresc să acceseze aceeaşi resursă cu scopul de a o modifica;
- aplicaţia distribuită în arhitectură client-server care permite utilizatorilor să utilizeze resursele; înregistrările sunt marcate la acest nivel prin permisiuni de editare ierarhizate pe niveluri de prioritate astfel încât odată ce nivelul de prioritate creşte, grupurile de utilizatori cu valori sub nivelul curent să nu mai poată realiza modificări asupra conţinutului decât prin solicitări justificate şi aprobate de către un utilizator autorizat;
- serverul web care accesează resursele web gestionate de sistemul integrat de bibliotecă; la acest nivel înregistrările sunt mai puţin vulnerabile deoarece accesul la resurse se realizează mai mult în modul consultare; la acest nivel sunt utilizate mecanisme de actualizare corespunzătoare astfel încât conţinutul afişat utilizatorilor să fie în permanenţă corelat cu ceea ce se află stocat în baza de date a bibliotecii virtuale.

2. Colaborarea în sistemele de biblioteci virtuale

La nivel naţional, geopolitic, cultural sau teritorial se impune o sincronizare a tuturor sistemelor de biblioteci virtuale pentru eliminarea redundanţei şi pentru a eficientiza procesul de catalogare şi digitizare în scopul creării de conţinut digital unitar, ca element valoric al patrimoniului cultural. Această armonizare între mai multe instituţii culturale care gestionează cataloagele unor biblioteci virtuale presupune utilizarea unor protocoale standardizate de partajare a conţinutului digital precum Z39.50 sau OAI-PMH. Standardul internaţional ISO 23950, [3], care referă protocolul Z39.50 are rolul de a putea lansa cereri de regăsire către sistemele integrate de bibliotecă fără a cunoaşte sintaxa de căutare specifică acelui sistem. Protocolul returnează o listă cu rezultate care au legătură cu termenii cheie utilizaţi în cererea de regăsire trimisă spre procesare. Protocolul OAI-PMH, [4], folosit pentru partajarea resursele în mediul online, este foarte eficient întrucât utilizează un set restrâns de expresii, denumite verbe, pentru a lansa cereri de regăsire în cadrul depozitelor de date care publică la rândul lor meta-date tot prin intermediul acestui protocol. Partajarea resurselor prin OAI-PMH implică doi actori:

- furnizori de date – sistemele care au implementat protocolul OAI-PMH cu scopul de a publica meta-date şi de a răspunde cererilor de regăsire primite de la clienţi;
- furnizori de servicii – reprezintă clienţii care lansează cererile de regăsire către furnizorii de date cu scopul de a colecta meta-date din cadrul depozitelor de date.

În cadrul protocolului OAI-PMH se disting trei entităţi cu roluri diferite în managementul meta-datelor stocate în aceste depozite, precum se observă în figura 1.

Figura 1. Structura depozitului de date din perspectiva OAI-PMH

Protocolul OAI-PMH utilizat pentru partajarea resurselor între diverse instituţii culturale dispune de mecanisme de transfer de meta-date de tip unidirecţional, dinspre furnizorii de date spre clienţii care lansează cererile de regăsire. Acest tip de protocol nu permite implementarea unor mecanisme de colaborare în mod implicit. Pentru implementarea unor procese de colaborare între mai mulţi actanţi culturali este necesară asigurarea unei relaţii de transfer de meta-date bidirecţionale astfel încât fiecare să poată prelua, modifica, apoi publica versiuni actualizate ale meta-datelor iniţiale, model de partajare în medii eterogene prezentat în [5]. Pe lângă această relaţie bidirecţională este utilă şi implementarea unei funcţii care să anunţe toţi furnizorii de servicii, dezvoltatori de colecţii, de îndată ce un nou furnizor de date este disponibil, precum este descris în [5].

Colaborarea între sistemele integrate de bibliotecă, la nivelul instituţiilor culturale europene, are rolul de a construi progresiv patrimoniul cultural al spaţiului european, asigurând durabilitatea formelor digitale precum şi conservarea formelor printate a căror expunere este cu mult diminuată.

Modelul colaborativ propus este format din următorii actanţi care participă activ la schimbul de resurse electronice pentru a construi un depozit central la care să aibă acces toţi utilizatorii spaţiului virtual. Componentele modelului sunt prezentate în figura 2.

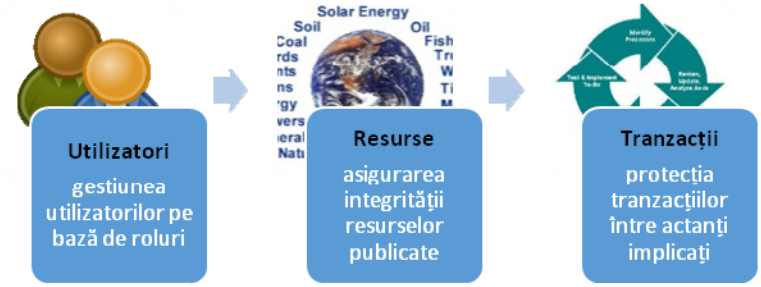

Figura 2. Componentele modelului colaborativ şi caracteristicile fiecărui grup

La nivelul acestor componente este necesară derularea unor procese de sincronizare şi management al versiunilor conţinutului electronic partajat astfel încât utilizatorilor să li se ofere în permanenţă cele mai bune rezultate pentru cererile de regăsire trimise cu ajutorul protocolului Z39.50.

3. Securitatea unui proces colaborativ în sistemele de biblioteci virtuale

În scopul implementării unui proces colaborativ pe baza protocolului OAI-PMH, între diferite sisteme integrate de bibliotecă ale instituţiilor culturale deţinătoare de biblioteci virtuale, următoarele premise de lucru trebuie asigurate:

- fiecare actant trebuie să fie în acelaşi timp atât furnizor de date cât şi consumator de servicii de meta-date;
- existenţa unui mecanism de notificare cu privire la actualizările efectuate la nivelul furnizorilor de meta-date;

- implementarea unui model de gestiune a versiunilor pentru înregistrările care suferă modificări la nivelul oricărui actant.

Securitatea unor procese colaborative prezintă o serie de caracteristici particulare datorită modului în care se desfăşoară acestea în raport cu resursele pe care le antrenează în sistem. Colaborarea într-un sistem, după cum este menționat în [7], poate servi unor scopuri distincte, după cum securitatea în astfel de sisteme pune accentul pe elemente diferite, funcție de contextul colaborativ, precum:

- informare – permit mai multor utilizatori să publice conținut digital în acelaşi spațiu informatic cu scop informativ; ex. rețeaua Facebook;
- negociere – permit desfăşurarea unor procese de licitație online, având la bază obiecte digitale; ex. rețeaua Bidson sau rețele de tranzacționare Forex;
- conlucrare – permit lucrul în echipă pentru atingerea aceluiaşi obiectiv, fiecare utilizator folosind însă resurse individuale; ex. Microsoft Project;
- cooperare – permit utilizarea aceleiaşi resurse de către mai mulți utilizatori pentru îndeplinirea unor obiective comune; ex. Google Documents; rețeaua Dropbox.

Modelul colaborativ asigură un nivel de partajare de meta-date de tip bidirecțional, care presupune dezvoltarea incrementală a unui patrimoniu cultural european. În figura 3 este prezentată o diagramă SWOT cu principalii factori pentru un astfel de sistem.

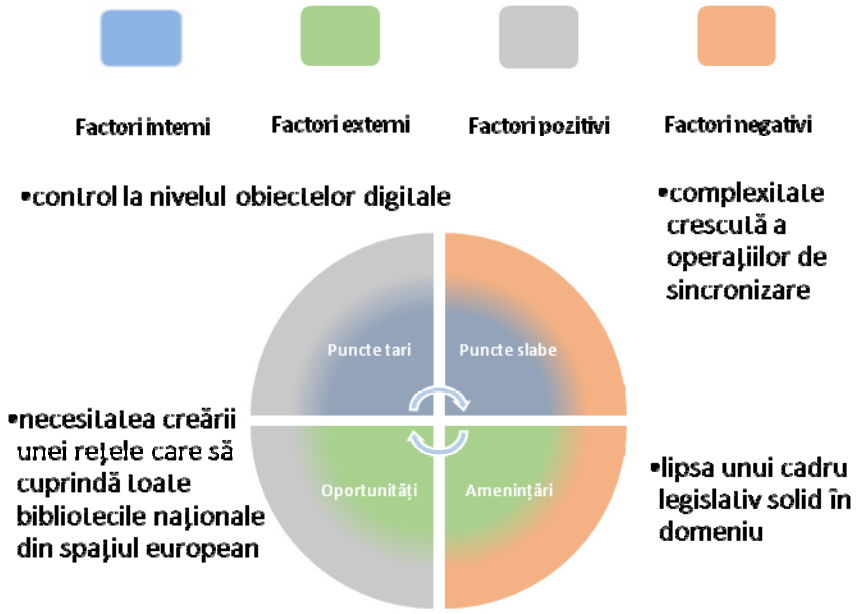

Figura 3. Diagrama SWOT a modelului colaborativ la nivelul bibliotecilor virtuale

Funcție de aceste aspecte pe care le vizează un proces colaborativ, securitatea ridică diferite probleme care trebuie avute în vedere. Natura unui proces colaborativ este decisivă atunci când se analizează securitatea acestuia, [8], după cum urmează:

- securitatea sistemelor care facilitează colaborarea şi pun accentul pe publicare de conținut digital cu rol de informare trebuie să urmărească disponibilitatea acestora; astfel de sisteme nu permit existența unor timpi de inoperabilitate, fiind necesară prezența unor sisteme cu copii de rezervă sau a unor sisteme care să preia sarcinile celor care nu mai sunt funcționale;
- în cazul sistemelor care facilitează colaborarea şi care au ca principală activitate negocierea, securitatea trebuie să vizeze aspectele temporale ale tranzacțiilor precum şi confidențialitatea acestora; în astfel de sisteme este foarte important să se cunoască cu o

precizie la nivel de milisecunde când a fost efectuată o tranzacție, iar detaliile acesteia să fie cunoscute doar de persoanele autorizate;

- sistemele colaborative al căror principal obiectiv este partajarea de către mai mulți utilizatori a unor resurse divizibile şi independente au ca principală caracteristică a securității, integritatea conținutului sub toate aspectele acestuia: al transferului pe canalele de comunicație; al stocării în baze sau depozite de date; al publicării pe paginile de internet;
- în sistemele în care se utilizează tehnici de partajare a aceleiaşi resurse de către mai mulți utilizatori, pentru obținerea aceluiaşi obiectiv, caracteristica de bază a securității, vitală în acest context, este aceea de non-repudiere; fiecărui utilizator trebuie să-i fie foarte bine atribuite operațiile care au fost efectuate în sistem pentru o cât mai bună urmărire a evoluției procesului colaborativ.

În cadrul unui model colaborativ implementat între mai multe sisteme de biblioteci virtuale toate aceste aspecte ale colaborării sunt prezente, iar securitatea trebuie asigurată la următoarele niveluri de lucru:

- utilizatori – din perspectiva acestora, securitatea trebuie să asigure principiul funcționării pe bază de roluri, implementarea unei politici pe bază de roluri de acces; un astfel de model este descris în [9]; rolurile trebuie definite după o analiză minuțioasă a operațiilor din sistem şi a necesarului de resurse; trebuie cunoscut exact cine are acces şi la ce resurse are acces, pentru a păstra o imagine clară asupra modificărilor aduse acestora în urma proceselor de colaborare care le accesează;
- resurse – în vederea unei manipulări corecte a resurselor, măsurile de securitate trebuie să asigure integritatea acestora la nivelurile unde acestea sunt utilizate; măsurile de integritate la nivelul stocării sunt asigurate de sistemele de gestiune a bazelor de date; transmiterea datelor prin rețea are implementate mecanisme la nivelul stivei de protocoale TCP/IP pe bază de sume de control, [10], care asigură transmiterea corectă a pachetelor; tot la nivelul resurselor se impune implementarea de măsuri pentru crearea copiilor de siguranță în cazul avariilor de orice natură ce pot apărea;
- tranzacții inter/intra biblioteci – acestea sunt cele mai sensibile elemente ale sistemului pentru că pot altera conținutul de o manieră ireversibilă; din perspectiva securității, tranzacțiile efectuate între diferite instituții trebuie să aibă un caracter confidențial, eliminând orice posibilitate de a capta informația vehiculată între acestea; în acest scop pot fi implementate sisteme de criptare pe bază de chei publice precum Diffie–Hellman sau RSA, [11], bazat pe standardul PKCS#1 sau sisteme simetrice cu chei private precum AES sau DES, [12].

4. Concluzii

Ideea unui model colaborativ folosit pentru a partaja resursele între mai multe instituții culturale de tip biblioteci virtuale ale spațiului european, îşi găseşte justificarea în necesitatea de a crea un patrimoniu durabil care să cuprindă forme digitale de cultură europeană, uşor accesibilă cititorilor acestei zone. Modelul propus se bazează pe standarde actuale bine definite care permit partajarea într-un singur sens a informației digitale. Aspectele de securitate ce vizează caracteristica de colaborare a unor procese care se desfăşoară într-un astfel de model prezintă o particularitate care nu trebuie neglijată când se doreşte protecția datelor vehiculate.

* * *

Această lucrare a fost realizată în cadrul proiectului "Cultura română şi modele culturale europene: cercetare, sincronizare, durabilitate", cofinanțat de Uniunea Europeană şi Guvernul României din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013, contractul de finanțare nr. POSDRU/159/1.5/S/136077.

BIBLIOGRAFIE

1. **MICAN, D.; TOMAI, N.; COCOS, R.:** Web Content Management Systems, a Collaborative Environment in the Information Society. Revista de Informatică Economică, 13(2), 2009, pp. 20-31.
2. **SÁNCHEZ, M.; JIMÉNEZ, B.; GUTIÈRREZ, F. L.; PADEREWSKI, P.; ISLA, J. L.:** Access control model for collaborative business processes. În: Engineering the User Interface: From Research to Practice. s.l.:Springer London, 2009, pp. 117-132.
3. Standard ISO, 1998/2014. Information and documentation -- Information retrieval (Z39.50) -- Application service definition and protocol specification. s.l.:ISO/TC 46/SC
4. **LAGOZE, C.; VAN DE SOMPEL, H.; NELSON, M.; WARNER, S.:** Open Archives. [Interactiv], 2015. Available at: https://www.openarchives.org/OAI/openarchivesprotocol.html
5. **HOUSSOS, N.; STAMATIS, K.; KOUTSOURAKIS, P.; KAPIDAKIS, S.; GAROUFALLOU, E.; KOULOURIS, A.**, Enhanced oai-pmh services for metadata sharing in heterogeneous environments. Library Review, 63(6-7), 2014, pp. 465-489.
6. **GOEBERT, S.; HARRIEHAUSEN-MÜHLBAUER, B.; FURNELL, S.:** Towards a unified OAI-PMH registry. s.l., Society for Imaging Science and Technology , 2014, pp. 97-100.
7. **DOINEA, M.; VAN OSCH, W.:** Collaborative Systems: Defining and Measuring Quality Characteristics. Journal of Applied Collaborative Systems, 2(1), 2010, pp. 50-61.
8. **CARMINATI, B.; FERRARI, E.:** Trust-based information sharing in collaborative communities: Issues and challenges. s.l., Vieweg+Teubner, 2009, pp. 83-92.
9. **DEMURJIAN, S.; REN, H.; BERHE, S.; DEVINENI, M.; VEGAD, S.; POLINENI, K.:** Improving the information security of collaborative Web portals via fine-grained role-based access control. În: Handbook of Research on Web 2.0, 3.0, and X.0: Technologies, Business, and Social Applications. s.l.:IGI Global, 2009, pp. 430-448.
10. **STONE, J.; PARTRIDGE, C.:** When the CRC and TCP checksum disagree, 2000, Stockholm, s.n.
11. **TAO, J.; MA, J.; KERANEN, M.; MAYO, J.; SHENE, C.; WANG, C.:** RSAvisual: A visualization tool for the RSA cipher. s.l., Association for Computing Machinery, 2014, pp. 635-640.
12. **DAMJANOVIĆ, B.; SIMIĆ, D.:** Performance evaluation of aes algorithm under linux operating system. roceedings of the Romanian Academy Series A - Mathematics Physics Technical Sciences Information Science, 14(2), 2013, pp. 177-183.