Economie teoretică şi aplicată
Volumul XVIII (2011), No. 8(561), pp. 29-52

Tipuri de utilizatori în aplicații online

Ion IVAN
Academia de Studii Economice, Bucureşti
ionivan@ase.ro
Dragoş PALAGHITA
Academia de Studii Economice, Bucureşti
mail@dragospalaghita.ro
Sorin VINTURIS
Academia de Studii Economice, Bucureşti
sorinvintturis@ie.ase.ro

Rezumat. *Se prezintă aplicațiile online în contextul societății informaționale. Sunt analizate particularitățile aplicațiilor online. Se prezintă caracteristici de calitate în raport cu utilizatorii aplicațiilor online. Sunt prezentate tipurile de utilizatori din aplicația AVIO. Se identifică cazurile de utilizare ale aplicației AVIO. Se definesc restricțiile de utilizare ale aplicației AVIO. Se identifică tipuri de utilizatori în aplicații online. Se construieşte matricea tridimensională de acces la resursele aplicației online. Se structurează baza de date orientată spre tipurile de utilizatori. Se analizează modalitățile de gestionare a accesului la câmpurile asociate tabelelor din baza de date. Se realizează clasificarea utilizatorilor în aplicații online.*

Cuvinte-cheie: aplicație online; utilizator; acces; metrică; securitate.

Cod JEL: C88.
Cod REL: 10J

Aplicații online

În literatura de specialitate (Roşca et al., 2006) se prezintă coordonatele societății informaționale care constau în:

- crearea informației prin trecerea de la active fixe la active informaționale, prin dezvoltarea sistemelor de calcul, realizarea bibliotecilor digitale, prin realizarea de portaluri informaționale;
- distribuția informației se realizează prin dezvoltarea rețelelor de calculatoare şi a internetului; accesul la informație este mult mai rapid şi mai eficient datorită motoarelor de căutare online sau în rețea;
- difuzarea informației prin intermediul internetului, mijloacelor media sau email;
- utilizarea informației de fiecare dată când este nevoie folosind calculatoarele personale sau terminalele de acces public pentru a rezolva problemele cetățenilor sau pentru a îmbunătăți procesele de afaceri;
- integrarea informației în sisteme complexe de gestiune a informației ce permit regăsirea facilă după chei de căutare;
- gestionarea informației prin optimizarea proceselor de acces la date oferind cetățenilor modalități eficiente şi simple de acces la informații.

Aplicația informatică este un produs software dezvoltat pentru a fi operat de pe un calculator şi a servi soluționării de probleme complexe.

Sistemul distribuit este reprezentat de un număr de calculatoare autonome ce comunică prin intermediul unei rețele. Un sistem distribuit este realizat pentru a rezolva o singura problemă comună tuturor unităților de procesare sau pentru a rezolva o serie de probleme specifice fiecărei unități de procesare, iar rolul sistemul distribuit este de a gestiona resursele asociate unităților de procesare. Un sistem distribuit are următoarele proprietăți:

- toleranța la defecțiuni este reprezentată de gradul în care sistemul distribuit îşi menține proprietățile în cazul în care apar defecțiuni hardware la entitățile ce îl compun;
- topologia de rețea reprezintă modalitatea de interconectare a calculatoarelor şi a perifericelor ce formează sistemul distribuit;
- gradul de independență este concretizat prin măsura în care calculatoarele ce alcătuiesc sistemul distribuit folosesc sau au cunoştință de celelalte calculatoare din cadrul sistemului distribuit.

Accesul la internet şi dezvoltarea rețelelor de calculatoare au determinat dezvoltarea de aplicații distribuite precum:

- plăți electronice ce se realizează către furnizori sau beneficiari, reducând formalitățile şi timpul necesar efectuării plății fizice;

- harți digitale ce permit stabilirea de trasee, calculul distanțelor şi vizualizarea de imagini din satelit (Cotfas, 2009a, pp. 466-471, 2009b, pp. 31-34);
- sortarea de imagini utilizând palete de culori pentru identificarea imaginilor ce conțin anumite nuanțe sau combinații de nuanțe;
- e-government ce permit o colaborare eficienta intre agențiile statului şi cetățeni prin implementarea de platforme online pentru plata impozitelor şi taxelor sau gestionarea problemelor şi responsabilităților statului şi cetățeanului;
- aplicații destinate gestionării activităților IMM-urilor prin oferirea de soluții integrate cu activitățile companiilor pentru buna desfăşurare a proceselor de aprovizionare (Catfas et al., 2010, pp. 1-13);
- analiza ortogonalității identificatorilor de organizație pentru a asigura înregistrarea organizațiilor cu denumiri semnificative în raport cu identificatorii de organizație înregistrați în baza de date.

Aplicațiile online orientate spre utilizator au următoarele avantaje conform (Ivan et al., 2009a, Ivan et al., 2009b, pp. 139-145):

- dau acces persoanelor la resursele dorite prin intermediul bazelor de date online ce stochează informații de interes pentru cetățeni;
- reduc duratele de aşteptare pentru îndeplinirea operațiunilor dorite de către utilizator sau rezolvarea problemelor;
- cresc eficiența operațiunilor efectuate prin procesarea rapidă a volumelor de operații necesare şi oferirea de rezultate într-un timp mult mai scurt;
- realizează legătura între clienți şi furnizori oferind un mediu colaborativ de lucru pentru rezolvarea problemelor, prestarea de servicii, achiziția de servicii, oferirea de bunuri şi achiziția lor;
- îmbunătățesc eficiența companiilor crescând vânzările şi oferind acces la o plajă mult mai mare de clienți pe plan local şi internațional;
- dau acces cetățeanului unei game de produse mult mai mare într-un spațiu online în care raportul calitate preț este ridicat;
- pun la dispoziția cetățenilor sisteme de gestiune financiară pentru înregistrarea veniturilor şi cheltuielilor individuale eliminând riscul de greşeli şi omisiuni în calculele realizate;
- cetățenii au acces la sisteme online bancare care permit verificarea contului, efectuarea de plăți online, gestiunea depozitelor şi gestiunea transferurilor bancare.

Aplicațiile online au un grad ridicat de diversitate oferind conținut variat şi posibilitatea efectuării de operații complexe conform (Vintilă, Pavel, 2010, pp. 64-72).

Caracteristicile aplicațiilor online în raport cu utilizatorul

La dezvoltarea aplicațiilor informatice se planifică nivelul calității. Calitatea reprezintă (DEX, 1998) totalitatea însuşirilor esențiale în virtutea cărora un lucru se deosebeşte de celelalte lucruri. Palaghita (2009, pp. 38-58) defineşte un sistem caracteristici de calitate asociate aplicațiilor informatice. Utilizatorii aplicațiilor online țin cont doar de anumite caracteristici de calitate ce îi vizează direct. Complexitatea este reprezentată de cantitatea de resurse necesare dezvoltării, testării, implementării, modificării, corectării şi utilizării aplicației informatice. Complexitatea McCabbe este definită prin:

$$C = m - n + 2$$

unde:

m - numărul arcelor din graf;

n - numărul nodurilor grafului.

Complexitatea McCabbe maximă presupune referirea oricărui nod de către altul diferit. În figura 1 se prezintă graful asociat complexității maxime pentru clasa de validare a denumirilor de organizație cu cinci noduri interconectate din produsul software AVIO.

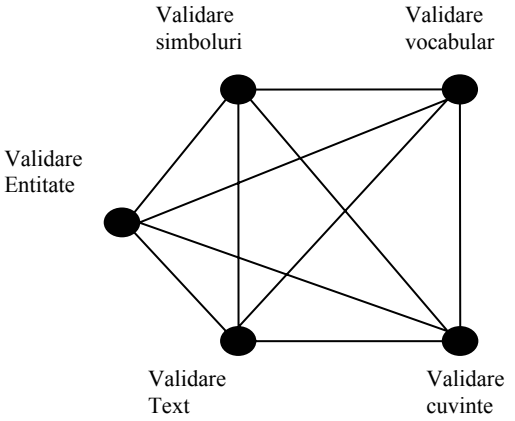

Figura 1. *Graf clasă validare denumiri AVIO*

Complexitatea McCabbe a clasei de validare a denumirilor de organizație este:

$$C_{den} = 11 - 5 + 2 = 8$$

Complexitatea maximă a unui modul nu trebuie să fie mai mare de 10 pentru a asigura desfăşurarea procesului de testare corespunzător, pentru a asigura fiabilitatea produsului informatic şi a păstra simplitatea proiectării software. Complexitatea minimă este atinsă în structurile liniare de aplicații. În figura 2 se prezintă structura liniară utilizată pentru clasa de gestiune a formatului RGB utilizat în compararea siglelor de organizație în aplicația AVIO.

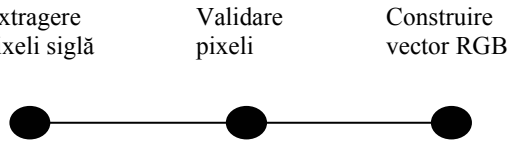

Figura 2. *Clasă gestiune RGB în aplicația AVIO*

Complexitatea clasei de gestiune RGB în aplicația AVIO este:
$C_{rgb} = 2\text{-}3\text{+}2 = 1$

Există şi structuri intermediare ce combină structura liniară cu cea de tip graf obținând structuri complexe software, dar cu un indice de complexitate potrivit pentru păstrarea fiabilității şi a testabilității la un nivel performant.

Corectitudinea conform Ivan şi Boja (2004) este gradul în care rezultatele obținute în urma utilizării aplicației sunt cât mai aproape de cele reale. Corectitudinea C este calculata utilizând următorul indicator:

$$C = \frac{N_c}{N_T}$$

unde:

N_e – numărul de rezultate corecte;
N_T – numărul total de rulări.

În aplicația AVIO, în urma rulării unui set de test ce conține 4.096 elemente de identificare grafică generate s-a determinat indicele de corectitudine cu $N_e = 3.072$ şi $N_T = 4.096$ indicele C având valoarea:

$$C = \frac{3072}{4096} = 0{,}75$$

Corectarea metodei de scalare a imaginilor şi a metodei de normalizare a imaginilor prin eliminarea reformatării implicite a identificatorilor grafici ce a cauzat valoarea indicelui C de 0,75 a adus indicele de corectitudine C la un nivel de 1, pentru setul de test executat.

Dacă o componentă a sistemului distribuit este construită din n sub-componente *{C1, C2, ..., Cn}* atunci nivelul corectitudinii este calculat utilizând indicatorul C_c:

$$C_C = \sum_{i=1}^{n} \frac{N_{ci}}{N_{Ti}} = \sum_{i=1}^{n} C_i$$

unde:

N_{ci} – numărul de rezultate corecte pentru componenta i*;*

N_{Ti} – numărul total de rezultate pentru componenta i*;*

C_i – gradul de corectitudine al componentei i.

După rularea setului de test s-au identificat valorile variabilelor asociate componentelor software ce alcătuiesc aplicația AVIO în vederea calculului indicatorul C_c conform datelor din Tabelul .

Tabelul 1

Indicatorul de corectitudine Cc

Componentă	N_{ci}	N_{Ti}	C_i
Imagini	4.096	4.096	1
Firma	4.096	4.096	1
DenumireArray<T>	4.096	4.096	1
ComplexArray	4.096	4.096	1
Complex	4.096	4.096	1
ImageMetrics	3.072	4.096	0,75
BitmapAlredyLoaded	4.096	4.096	1
Validator	4.096	4.096	1
ImageValidator	4.096	4.096	1
UnmanagedImage	4.096	4.096	1
RGBL	4.096	4.096	1
RGB	4.096	4.096	1
Histogram	4.096	4.096	1
ColorSetLocations	4.096	4.096	1
ColorLocationList	4.096	4.096	1
ColorLocation	4.096	4.096	1
BmpStatisticsHelper	4.096	4.096	1
BmpHelper	3.072	4.096	0,75
StatisticsHelper	4.096	4.096	1
LogHelper	4.096	4.096	1
perecheCulori	4.096	4.096	1
LogWriter	4.096	4.096	1
Cc			**0,97727273**

Setul de test arată o valoare a identificatorului C_c asociat aplicației AVIO înainte de rezolvarea defectelor identificate în procesul de testare de 0,977. Rezolvarea defectelor a condus la creşterea indicelui C_c la valoarea 1.

Continuitatea este caracteristica de calitate reprezentată de gradul în care se manifestă schimbările de interfață în versiunile produsului informatic. Se consideră un set de versiuni software SV = $\{V_1, V_2, \ldots, V_k\}$ ce are asociat un set de versiuni ale interfeței software SI = $\{I_1, I_2, \ldots, I_k\}$. O versiune de interfață software I_i asociată versiunii software V_i este definită de un set de componente vizibile utilizatorului $SCI_i=\{C_{i1}, C_{i2}, \ldots, C_{im}\}$. Un grad ridicat de continuitate pentru o aplicație informatică este definit de un nivel ridicat de asemănare între interfețele cu utilizatorul asociate fiecărei versiuni. Astfel este necesar un grad de asemănare ridicat între seturile de componente ce alcătuiesc interfețele. Modificările ce sunt aplicate componentelor de interfață sunt:

- interschimbare, ce este definită de schimbarea pozițiilor a două componente de interfață între ele;
- excludere, fiind reprezentată de ştergerea anumitor componente de interfață ce nu sunt reprezentative pentru versiunea curentă a interfeței software;
- adăugare, fiind operația prin care se creează o componentă de interfață nouă ce este inclusă în setul de componente asociat ultimei versiuni de interfață a produsului informatic;
- modificare, prin care se alterează forma, lungimea sau conținutul componentelor de interfață cu utilizatorul a aplicației software.

Continuitatea interfeței de utilizator I_i este definită prin indicatorul CT:

$$CT_i = \frac{\sum_{j=1}^{m} \frac{\min(TC_{ij}, CN_{ij})}{\max(TC_{ij}, CN_{ij})}}{m}$$

unde:

TC – total componente de interfață;

CN- număr componente nemodificate față de interfață I_{i-1}.

Indicatorul agregat de continuitate CT_i este uşor de determinat prin analiza dinamicii componentelor de interfață şi este o metrică folositoare în determinarea fluctuațiilor apărute în componența interfețelor software.

Securitatea este caracteristica de calitate a unui sistem distribuit ce se concretizează prin abilitatea de a proteja resursele logice şi fizice ale sistemului. Securitatea este[1] reprezentată de măsurile luate pentru a proteja un sistem.

Securitatea este considerată, de asemenea, ca o condiție a unui sistem care rezultă din instituirea şi menținerea unor măsuri pentru a proteja sistemul. Securitatea este o condiție a resurselor de sistem la care nu sunt permise accesul neautorizat şi schimbările neautorizate sau accidentale, distrugerea sau pierderea.

Securitatea unui sistem este influențată de protocoalele de comunicare în rețea utilizate, de topologia rețelei, de metodele de autentificare a utilizatorilor, de sistemele de criptare utilizate şi de factorul uman implicat în toate aspectele ciclului de viață al sistemului distribuit. Securitatea este reprezentată de controlul accesului la resurse software, hardware şi componente ale aplicației. Sistemele informatice implementează următoarele metode pentru a securiza accesul la resurse:

- autentificarea reprezintă procesul de confirmare a identității; înainte ca o aplicație să autorizeze accesul la resursele protejate este necesară executarea proceselor de autentificare pentru stabilirea identității utilizatorului şi verificarea dacă informațiile date de el în cadrul procesului de autentificare sunt sau nu sunt înregistrate în baza de date asociată grupului de utilizatori ai sistemului informatic distribuit;
- autorizarea reprezintă procesul de stabilire a permisiunii de acces a utilizatorului la resursele protejate din cadrul sistemului informatic distribuit; chiar dacă un utilizator a dovedit că este înregistrat în baza de date asociată grupului de utilizatori ai sistemului nu înseamnă că are şi acces la resurse;
- protecția datelor este procesul de asigurare a confidențialității şi a integrității datelor stocate în bazele de date ale sistemului distribuit; criptarea asigură confidențialitatea datelor; integritatea datelor este asigurată prin utilizarea semnăturii digitale, a algoritmilor hash şi a codurilor de autentificare mesaj.

Securitatea este un aspect importat pentru aplicațiile online (Doinea et al., 2010) fiind necesară păstrării integrității aplicațiilor şi a datelor, precum şi pentru impunerea nivelului de confidențialitate.

Restricții de acces al utilizatorilor în aplicația AVIO

Aplicația pentru analiza identificatorilor de organizație determină nivelul ortogonalității identificatorilor de organizație în vederea eliminării situațiilor în care există două companii cu denumiri şi sigle foarte apropiate.

În cadrul modulului de analiză a ortogonalității denumirilor de organizație se construieşte un vocabular VOCDEN = $\{D_1, D_2, \ldots, D_k\}$ ce conține toate

denumirile de organizație introduse în baza de date. Se consideră că entitatea are denumirea formată din mai multe cuvinte; astfel ortogonalitatea este stabilită prin analiza la nivel de vocabular şi la nivel de cuvânt.

Analiza la nivel de vocabular se realizează prima pentru a determina corespondenta între texte şi necesitățile de validare ale aplicației pentru calcul ortogonalității.

Pentru a analiza ortogonalitatea a două texte T_1 şi T_2 se construiesc două vocabulare V_1 şi V_2 ce sunt definite de sortarea alfabetică a cuvintelor care compun texte T_1, respectiv T_2. Vocabularele se definesc ca seturile de cuvinte sortate $V_1 = \{C_{11}, C_{12},..., C_{1n}\}$ şi $V_2 = \{C_{21}, C_{22}, ..., C_{2n}\}$ unde C_{1i} corespunde cuvântului de pe poziția i a vocabularului V_1, iar C_{2j} corespunde cuvântului de pe poziția j a vocabularului V_2. Ortogonalitatea denumirilor este reprezentată de formula

$$ORTOT(V_1,V_2) = 1 - \frac{NCC}{\max(NrCV_1, NrCV_2)}$$

unde:

NCC – număr cuvinte comune;
$NrCV_1$ – număr cuvinte cuprinse în vocabularul V_1;
$NrCV_2$ – număr cuvinte cuprinse în vocabularul V_2.

Analiza ortogonalității siglelor de organizație reprezintă determinarea prin analiza comparată a diferențelor existente între două sigle, rezultatul fiind un indice de ortogonalitate. O siglă reprezintă o formă grafică sau o emblemă unică utilizată de organizații, companii sau indivizi pentru a fi recunoscuți public. O siglă are următoarele caracteristici:

- unicitate, astfel încât fiecare siglă este asociată cu o singură entitate uşurând recunoaşterea identității posesorului;
- standardizare, ce se concretizează în formatarea siglei într-un fel anume ce garantează concordanța cu formatul celorlalte sigle existente; se urmăresc lățimea, înălțimea şi calitatea siglei;
- reprezentativitate, ce înseamnă gradul în care sigla definită este reprezentativă pentru domeniul de activitate al posesorului;
- simplitate, ce se caracterizează printr-o reprezentare ce este uşor de memorat având o complexitate a elementelor alfabetice şi grafice cât mai redusă;
- impactul este caracteristica ce determină succesul siglei considerând elementele de design ce influențează opinia publică asupra entității ce este reprezentată de siglă;

- culoare, existând sigle ce folosesc numai un set restrâns de culori ce sunt considerate de către designeri reprezentative pentru entitatea reprezentata sau sigle ce utilizează numai culorile alb şi negru;
- forma diferențiază siglele în funcție de elementele geometrice în care sunt reprezentate, existând sigle rotunde, sigle pătrate, sigle ovale, sigle dreptunghice, sigle hexagonale sau sigle ce sunt alcătuite din forme geometrice compuse; pe măsură ce o siglă conține mai multe forme geometrice complexitatea sa creşte; astfel măsura în care este uşor asociata cu entitate reprezentată scade.

Pentru ca două sigle să fie diferite trebuie:

- să existe elemente de culoare diferite între cele două sigle astfel încât să existe o diferență cromatică în analiza comparată;
- să existe elemente geometrice diferite în componenta siglelor, în aşa fel încât compararea lor vizuală să releve diferențe evidente.

Pentru determinarea ortogonalității siglelor S_{beta} şi S_{beta2} în aplicația AVIO de validare a identificatorilor de organizație se determina diferențele între cele două sigle urmând paşii:

- determinarea matricelor de pixeli asociate siglelor S_{beta} şi S_{beta2} scalate la dimensiunile:
  - 4x4 pixeli, creându-se matricea $MS_{beta4x4}$ asociată siglei S_{beta} şi matricea $MS_{beta24x4}$ asociată siglei S_{beta2}, fiecare matrice conține patru coloane şi patru linii de pixeli;
  - 8x8 pixeli, creându-se matricea $MS_{beta8x8}$ asociată siglei S_{beta} şi matricea $MS_{beta28x8}$ asociată siglei S_{beta2}, fiecare matrice conține opt coloane şi opt linii de pixeli;
  - 16x16 pixeli, creându-se matricea $MS_{beta16x16}$ asociată siglei S_{beta} şi matricea $MS_{beta216x16}$ asociată siglei S_{beta2} fiecare matrice conține 16 coloane şi 16 linii de pixeli;
- se creează două seturi de matrice ST_{beta}= {$MS_{beta4x4}$, $MS_{beta8x8}$, $MS_{beta16x16}$} şi ST_{beta2} = {$MS_{beta24x4}$, $MS_{beta28x8}$, $MS_{beta216x16}$};
- se realizează compararea seturilor de matrice utilizând formula ponderată:

$$\mathrm{ORTOST}(ST_{beta}, ST_{beta2}) = \frac{(ND4 \times 16 + ND8 \times 4 + ND16)}{256 \times 3}$$

unde:

ND4 – numărul de diferențe înregistrate între matricea $MS_{beta4x4}$ şi matricea $MS_{beta24x4}$, numărul maxim de diferențe este de $4 \times 4 = 16$;

ND8 – numărul de diferențe înregistrate între matricea $MS_{beta8x8}$ şi matricea $MS_{beta28x8}$, numărul maxim de diferențe este de $8 \times 8 = 64$;

ND16 – numărul de diferențe înregistrate între matricea $MS_{beta16x16}$ şi matricea $MS_{beta216x16}$, numărul maxim de diferențe este de $16 \times 16 = 256$;

$ORTOST(ST_{beta}, ST_{beta2}) \in [0,1]$ deoarece în cazul în care se înregistrează numărul maxim de diferențe între cele două seturi de matrice, adică ND4 = 16, ND8 = 64 şi ND16 = 256, atunci:

$$\text{ORTOST}(\text{ST}_{\text{beta}}, \text{ST}_{\text{beta 2}}) = \frac{16 \times 16 + 64 \times 4 + 256}{256 \times 3} = \frac{256 + 256 + 256}{256 \times 3} = 1$$

În contextul lucrului cu un volum mare de date conform (Doinea, Pavel, 2010, pp. 72-85) pentru aplicația AVIO se identifică următoarele tipuri de utilizatori:

- utilizatori ce au acces la funcționalitatea de afişare a organizațiilor cu identificatori ortogonali stocate în baza de date; acest tip de utilizatori nu necesită înregistrarea pe site pentru a accesa această funcționalitate;
- utilizatori ce au acces la funcționalitatea de validare identificatori de organizație prin introducerea de noi identificatori în vederea determinării ortogonalității; acest tip de utilizator necesită înregistrare pe site pentru a primi permisiunile necesare utilizării produsului AVIO;
- utilizatori ce au acces la funcționalitățile de administrare a produsului AVIO; acest tip de utilizator este unic, fiind reprezentat de administratorul aplicației informatice ce gestionează conținutul prezentat, cât şi buna funcționare a produsului software.

Pentru determinarea fluxurilor în aplicația AVIO este necesară determinarea modalităților de utilizare disponibile pentru tipurile de utilizatori descrişi. De asemenea, este importantă modalitatea de interacțiune cu aplicația informatică, dar şi interacțiunea între tipurile de utilizatori. Fluxurile în aplicația AVIO sunt determinate pornind de la cazul de utilizare descris în figura 3.

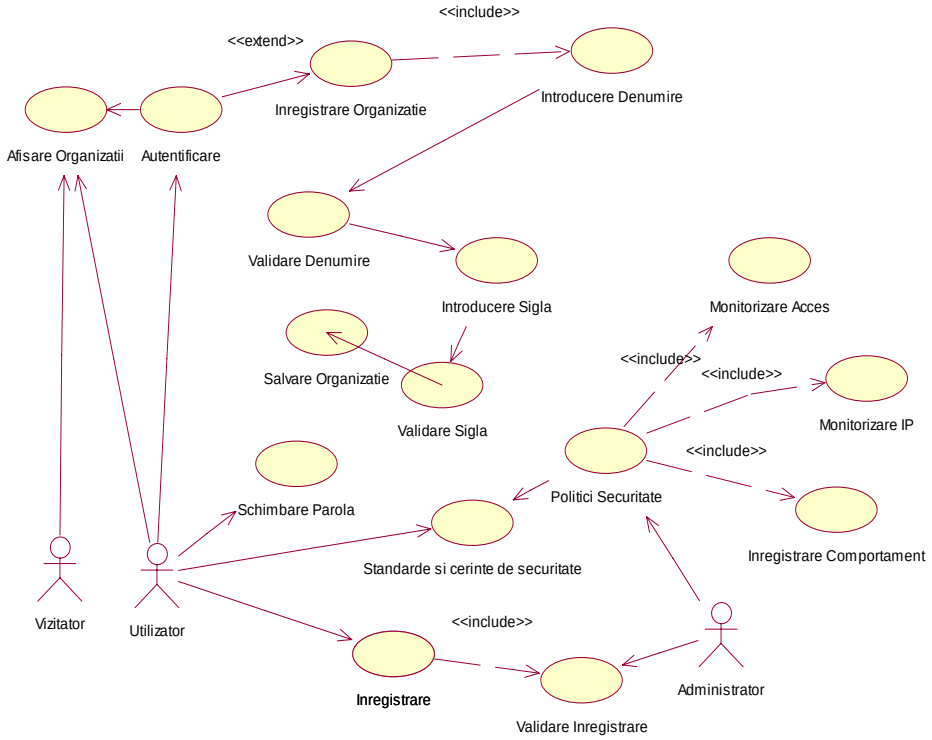

Figura 3. *Caz utilizare AVIO*

Din cazul de utilizare prezentat în figura 3 se determină matricea de acces la operații pentru aplicația AVIO în tabelul 2.

Tabelul 2

Matricea de acces la operațiuni AVIO

Permisie / Rol	Citire	Analizare ortogonalitate identificatori	Adăugare identificatori în baza de date	Validare utilizatori	Gestionare politici securitate	Gestiune utilizatori	Gestiune Evenimente
Vizitator	X						
Înregistrat	X	X	X				
Administrator	X			X	X	X	
Aplicație							X

Matricea de acces la tabelele ce compun baza de date utilizată de aplicația AVIO este prezentată în tabelul 3.

Tabelul 3

Matricea de acces la tabele în aplicația AVIO

Tabelă / Utilizator	App_FIRME	aspnet_Users	Log_EXCEPTII	Log_LIB	Log_Evenimente	Log_COMP	Log_ACTIUNI
Vizitator	X						
Înregistrat	X						
Administrator	X	X	X	X	X	X	X
Aplicație	X	X	X	X	X	X	X

Utilizatorul de tip Vizitator are privilegii de acces de Citire la identificatorii de organizație stocați în tabela App_FIRME fără a vedea ce utilizator i-a introdus.

În tabelul 4 se prezintă permisiile pentru câmpurile asociate tabelei App_FIRME pentru utilizatorul de tip Vizitator.

Tabelul 4

Permisiuni de acces la câmpurile tabelei App_FIRME pentru Vizitator

Câmp / Operație	Nume	Sigla	ID	UserID
Citire	X	X		

Utilizatorul de tip înregistrat are privilegii de citire, dar şi de introducere de noi identificatori de organizație dacă în urma analizei ortogonalității se dovedesc a fi ortogonali cu identificatorii deja stocați în baza de date. Utilizatorul de tip Înregistrat are permisii de ştergere restricționată doar pentru identificatorii introduşi de el, neavând permisie de ştergere şi pentru identificatorii introduşi de ceilalți utilizatori.

În tabelul 5 se prezintă permisiile pentru câmpurile asociate tabelei App_FIRME pentru utilizatorul de tip Înregistrat.

Tabelul 5

Permisiuni de acces la câmpurile tabelei App_FIRME pentru Înregistrat

Câmp / Operație	Nume	Sigla	ID	UserID
Citire	X	X		
Scriere	X	X		
Ştergere restricționată	X	X		

Administratorul are privilegii de acces extinse pentru tabela App_FIRME având permisii de înregistrare de noi identificatori de organizație ortogonali, citire, ştergere a unor identificatori existenți care sunt necorespunzători sau modificare a celor existenți. Modificare implică reluarea procesărilor pentru determinarea ortogonalității pentru modificarea realizată pe identificatori.

În tabelul 6 se prezintă permisiile pentru câmpurile asociate tabelei App_FIRME pentru utilizatorul de tip Administrator.

Tabelul 6

Permisiuni de acces la câmpurile tabelei App_FIRME pentru Administrator

Câmp / Operație	Nume	Sigla	ID	UserID
Citire	X	X	X	X
Scriere	X	X		X
Ştergere	X	X		X
Modificare	X	X		X

Tabelele aspnet_Users, Log_EXCEPTII, Log_LIB, Log_Evenimente, Log_COMP, Log_ACTIUNI prezintă drepturi de citire pentru Administrator şi drepturi de scriere pentru Aplicație. Tabela aspnet_Users este utilizată pentru gestionarea utilizatorilor, iar celelalte formează sistemul de monitorizare în aplicația AVIO având rol informativ pentru utilizatorul de tip Administrator.

Matricea de acces

Matricea de acces presupune existența structurii bazei de date deoarece accesul la câmpuri e realizat pornind de la arhitectura tabelelor ce stochează datele. Tipul de acces este impus prin includerea de informații de acces în tabele, precum şi crearea de tablele auxiliare pentru obținerea unui nivel de granularitate ridicat în definirea regulilor de acces. Pentru realizarea matricei de acces se porneşte de la date spre permisii prin determinarea nivelului de acces şi scopul câmpurilor din tabelele bazei de date. Se consideră o bază de date formată din setul de tabele $T=\{T_1, T_2, \ldots, T_n\}$. Fiecare tabelă T_i are asociat un set de înregistrări $I_i = \{I_{i1}, I_{i2}, \ldots, I_{ik}\}$. Înregistrarea I_{ij} este definită de setul de câmpuri $C_{ij} = \{C_{ij1}, C_{ij2}, \ldots, C_{ijm}\}$. Există restricții de acces la nivel de tabelă clasificate în funcție de rolul tabelei în ansamblul produsului software. Astfel există tablele ce sunt supuse operațiilor de citire, acestea permițând:

- acces nerestricționat pentru citire; acest tip de tabelă conține informații neconfidențiale având ca scop informarea utilizatorilor prin oferirea spre citire a datelor stocate; tabelele cu acces nerestricționat la date sunt utilizate în portaluri de informare, site-uri guvernamentale pentru informare sau alte tipuri de aplicații informatice ce au ca scop oferirea de informații de natură neconfidențială;
- acces parțial restricționat pentru citire; acest tip de tabelă conține informații de natură confidențială, dar şi informații publice astfel accesul este selecționat în funcție de nivelul de acces al utilizatorului;

dacă utilizatorul are drepturi de acces la datele confidențiale se prezintă tot tabelul, altfel se prezintă numai informațiile publice; aceste tabele sunt utilizate în cadrul aplicațiilor informatice ce implementează sisteme de securitate, gestiune de utilizatori şi roluri pentru acces diferențiat la informații şi resurse; tabelele ce au acces de citire parțial restricționat sunt folosite pentru înregistrarea detaliilor confidențiale, dar şi a elementelor de interes public ce sunt prezentate anonim în cazul lipsei drepturilor de acces;

- acces restricționat pentru citire; acest tip de tabelă prezintă numai informații confidențiale ce sunt prezentate utilizatorilor cu privilegii de acces; tabelele cu acces restricționat pentru citire sunt utilizate pentru înregistrarea informațiilor confidențiale, accesul este verificat, iar datele sunt criptate pentru a asigura un nivel ridicat de confidențialitate.

Există tabele pe care se realizează operații de scriere în funcție de scopul produsului informatic acestea permițând:

- acces de scriere nerestricționat; înregistrările sunt realizate automat de către aplicația informatică sau manual de către utilizator;
- acces de scriere parțial restricționat este cuantificat prin permiterea scrierii numai a unui set de câmpuri din tabelă, celelalte primind automat valori standard sau alocate de un algoritm de calcul; acest tip de tabelă este utilizat pentru vânzări unde valorile pentru valoarea vânzării, TVA şi valoare fără TVA sunt completate automat; astfel utilizatorul nu primeşte acces la scriere pentru întreaga tabelă;
- acces de scriere restricționat; astfel numai utilizatorii cu drepturi de scriere efectuează acest tip de operațiune;
- acces de scriere parțial restricționat sau restricționat cu validare; acest principiu este aplicat pentru drepturi de scriere parțial restricționat şi restricționat; utilizatorii ce efectuează inserări în acest tip de tabelă trebuie să aibă privilegii de acces speciale, iar cei ce efectuează validarea informațiilor de asemenea.

Există tabele pe care se realizează operații de modificare acestea permițând:

- acces nerestricționat de modificare în care modificările sunt realizate de către toți utilizatorii înregistrați ai bazei de date sau ai produsului informatic ce utilizează tabela;
- acces parțial restricționat de modificare prin nepermiterea modificării unor câmpuri decât cu privilegii de acces ridicate;
- accesul restricționat de modificare prin nepermiterea efectuării de modificări decât utilizatorilor cu un nivel ridicat de acces la tabelă;

- accesul parțial restricționat şi restricționat cu validare pentru modificare; acest tip de acces permite revenirea la forma nemodificată a înregistrării în cazul în care modificarea este eronată sau nu este acceptată de utilizatorul ce este responsabil să valideze operațiunea.

Operațiile de ştergere trebuie efectuate de către utilizatori cu drepturi ridicate de acces pentru a restricționa grupul de utilizatori ce au acces la această funcționalitate.

Există tabele ce trebuie să aibă permisii mixte pentru acces la citire, scriere, modificare sau ştergere astfel de acces este acces mixt, având combinații de tipuri de acces pentru fiecare operațiune prezentată. În tabelul 7 se prezintă matricea de acces la setul de tabele $T=\{T_1, T_2, \ldots, T_n\}$ pentru setul de utilizatori $U=\{U_1, U_2, \ldots, U_p, \ldots, U_t\}$.

Tabelul 7

Matrice de acces la tabele

Tabelă / Utilizator	T_1	T_2	…	T_{i-1}	T_i	T_{i+1}	…	T_{n-1}	T_n
U_1	X			X					X
U_2					X	X			
…									
U_{p-1}		X							
U_p		X			X			X	X
U_{p+1}	X	X		X	X	X		X	X
…									
U_{t-1}	X					X		X	
U_t		X			X				

Există mai multe tipuri de câmpuri:

- ce sunt utilizate pentru identificarea unui element dintr-o colectivitate după coordonate specifice cum sunt coduri unice de identificare, cod numeric personal, număr de înmatriculare sau alte elemente cu caracter unic;
- ce sunt folosite pentru descrierea entității ce conține câmpurile C_{ij}, astfel fiind necesare identificării caracteristicilor entității virtualizate de înregistrarea I_{ij} ce conține câmpurile de tip C_{ij}; câmpurile utilizate pentru descriere sunt necesare definirii caracteristicilor entității descrise pentru a stabili un grad de diferență în cadrul colectivității de entități stocate în tabela T_i;
- ce vizează starea şi dinamica elementului C_{ijl} aparținând colectivității de câmpuri C_{ij} asociat înregistrării I_{ij}; acest tip de câmp are o evoluție dinamică deoarece este supus modificărilor frecvente ce definesc dinamica entității; acest tip de câmp este utilizat pentru identificarea

evoluției unei perechi valutare pe piața valutară, gestionarea fisei de parcurs a unui automobil sau alte tipuri de activități ce necesită modificări frecvente;

- de legătură cu entități din alte tabele ce sunt destinate menținerii legăturilor logice între entități; aceste câmpuri sunt reprezentate de identificatori unici ce aparțin altor entități şi sunt folosiți pentru realizarea legăturii logice între cele două înregistrări;
- câmpuri pentru demarcarea cheltuielilor zilnice care sunt supuse modificării în funcție de numărul de articole achiziționate ca urmare a realizării operațiunilor de aprovizionare.

Pentru a aplica restricții de securitate pentru fiecare câmp este necesar să se stabilească condițiile de editare a câmpurilor. Astfel există câmpuri:

- cu permisii de citire nerestricționată ce sunt afişate tuturor utilizatorilor şi sunt de interes public în baza de date; accesul la aceste câmpuri se face cu minimul de privilegii;
- cu permisii de citire restricționată astfel fiind disponibile spre afişare numai utilizatorilor ce dispun de permisiile necesare pentru a căpăta acces la datele stocate în câmpurile respective; acest tip de câmp conține informații confidențiale sau cu un nivel de importanță crescut;
- cu permisii de scriere nerestricționată ce sunt scrise de către toți utilizatorii bazei de date; aceste câmpuri conțin elemente de interes general şi cu un nivel de importanță moderat;
- cu permisii de scriere restricționate ce sunt scrise doar de utilizatorii ce au permisii de modificare pe câmpul respectiv; acest tip de câmp prezintă importanță ridicată şi în unele cazuri conține şi informații confidențiale;
- cu permisii de modificare nerestricționate ce sunt modificabile de către toți utilizatorii bazei de date; aceste câmpuri sunt utilizate pentru stocarea datelor cu caracter dinamic care sunt modificate frecvent şi au un nivel de importanță moderat;
- cu permisii de modificare restricționate fiind modificabile numai de către anumiți utilizatori ai bazei de date ce au privilegii de acces la câmpul respectiv; aceste câmpuri sunt folosite pentru stocarea datelor cu caracter confidențial sau nivel de importanță crescut.

Pentru setul de câmpuri C_{ij} asociat tabelei T_i se consideră matricea de operații de bază permise pentru utilizatorul U_p prezentat în tabelul 8.

Tabelul 8

Operaţii de bază permise pentru utilizatorul U_p

Câmp / Operaţie	C_{ij1}	C_{ij2}	…	C_{ijo-1}	C_{ijo}	C_{ijo+1}	…	C_{ijm-1}	C_{ijm}
Citire	X	X		X				X	X
Citire Restricţionată					X	X			
Scriere		X							
Scriere Restricţionată	X								
Modificare		X			X			X	
Modificare Restricţionată	X			X		X			X
Simulare lucru		X		X				X	
Copiere date	X			X					X
Export date		X			X			X	

În figura 4 se prezintă matricea tridimensională ce asigură controlul accesului la câmpurile tabelului T_i.

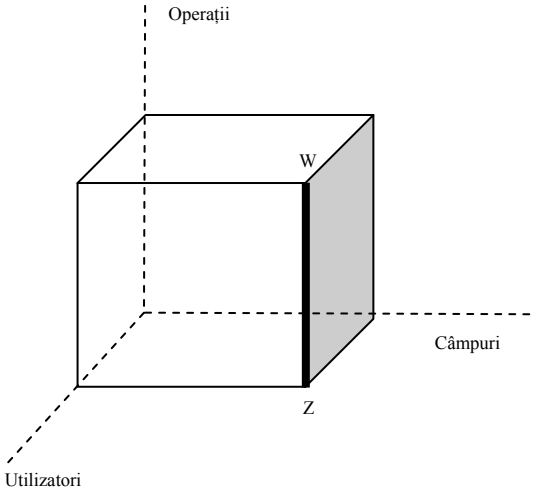

Figura 4. *Matrice tridimensională de acces la câmpuri*

Unde segmentul WZ este reprezentat de mulţimea operaţiilor ce se realizează de către toţi utilizatorii.

Figura 5 prezintă matricele tridimensionale de acces la câmpuri pentru colectivitatea de tabele $T=\{T_1, T_2, \ldots, T_n\}$. Pentru a optimiza accesul la câmpuri şi a impune restricţiile eficient se implementează roluri pentru utilizatori; astfel

se creează eficient restricțiile de operațiuni pentru utilizatori. Permisiile de acces la câmpuri sunt salvate în baza de date de către administrator şi asociate rolurilor utilizatorilor. Prin implementarea rolurilor pentru utilizatori se restrâng tabelele cu permisiuni astfel fiind nevoie de un număr de seturi de permisiuni egal cu numărul de roluri din baza de date.

Matricea tridimensională de acces bazată pe roluri este mai mică şi mai uşor de gestionat. Abordarea de control al accesului prin roluri este eficientă în momentul în care alocarea de permisiuni pentru fiecare utilizator este redundantă având mai mulți utilizatori cu aceleaşi seturi de operații permise.

Pentru buna gestiune a accesului la câmpuri este necesară folosirea de triggere pe tabele sau a gestiuni accesului la câmpuri din limbajul de programare ce implementează baza de date.

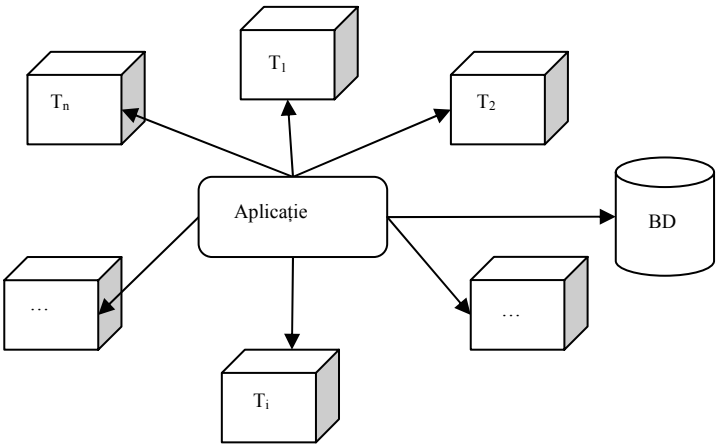

Figura 5. *Setul de permisii pentru colectivitatea de tabele T*

Setul de permisii pentru colectivitate de tabele T este reprezentativ pentru accesul la informațiile stocate în baza de date prin faptul că se implementează un nivel de acces la nivel de câmp ce permit controlul eficient al operațiilor asupra resurselor bazei de date.

Matricea de acces tridimensională oferă posibilitatea identificării tuturor acțiunilor utilizatorului şi controlarea lor dacă este cazul. Este importantă implementarea ei în contextul menținerii unui mod unitar de control al accesului la resurse.

Clasificarea utilizatorilor

Aplicațiile online prin complexitatea lor oferă o diversitate foarte mare de tipuri de interacțiuni cărora le corespund tipurile de utilizatori. Utilizatorii consultă aplicațiile online pentru a se informa. Există aplicații informatice online ce sunt utilizate pentru realizarea de operațiuni complexe şi cu caracter de confidențialitate precum:

- gestionarea de documente prin încărcarea şi stocarea documentelor pe un server al produsului informatic; acest tip de aplicație este util deoarece oferă disponibilitatea foarte mare a documentelor indiferent de terminalul utilizat; aplicațiile informatice care oferă acest serviciu au şi opțiunea de vizualizare a documentelor online, editarea lor, verificare gramaticală şi salvarea documentului modificat sau descărcarea lui pe terminalul de lucru; există restricții de securitate implementate pentru a păstra confidențialitatea documentelor stocate; sunt implementate şi funcționalități de schimbare a caracterului confidențial al documentelor intr-unul public;
- gestionarea online a bugetului lunar prin introducerea cheltuielilor şi veniturilor; acest tip de aplicație online este utilă pentru identificarea clară a cheltuielilor inutile şi eliminarea lor; datele personale privind veniturile şi cheltuielile trebuie să fie protejate de un sistem de securitate eficient deoarece pierderea confidențialității bazei de date conduce la dezvăluirea unui număr foarte mare de informații strict confidențiale;
- gestionarea conturilor bancare prin aplicații de e-banking; acest tip de aplicații pune la dispoziția utilizatorului un număr ridicat de operațiuni bancare precum gestiunea depozitelor, efectuarea de plăți către furnizori, efectuarea de viramente bancare sau vizualizarea extraselor de cont şi istoricul operațiunilor; pentru păstrarea confidențialității este necesară administrarea eficientă a sistemului de securitate şi utilizarea mecanis-melor de criptare a informațiilor, precum şi utilizarea unor mecanisme de autentificare eficiente care să țină cont de ultimele tipuri de amenințări;
- magazinele virtuale ce oferă funcționalități de vizualizare a produselor, de gestionare a coşului de cumpărături şi de plată online; acest tip de aplicații este util pentru efectuarea achizițiilor de produse diverse online, gestionarea comenzilor făcute şi vizualizarea istoricului de cumpărături.

Tipurile utilizatorilor în aplicațiile complexe ce au un nivel ridicat de confidențialitate este stabilit în funcție de gradul de acces de care au nevoie să îşi desfăşoare activitatea. Există utilizatori care:

- vizualizează informațiile prezentate de produsul informatic şi le utilizează în activitățile desfăşurate;

- adaugă informații în baza de date; aceşti utilizatori au nevoie de permisii diferențiate pentru a determina în ce tabele adaugă date, dar şi ce câmpuri sunt afectate de înregistrările adăugate;
- modifică informații în baza de date; aceste modificări survin diferențelor de stocuri sau schimbărilor efectuate în documente sau din cauza altor factori de influență; pentru a efectua modificări este nevoie de stabilirea limitelor impuse prin identificarea tabelelor şi câmpurilor modificabile de către utilizator; acest lucru se realizează prin stabilirea necesarului de permisii pentru ca utilizatorul să îşi desfăşoare activitățile propuse eficient; modificările efectuate sunt la nivel de câmp sau de tabelă şi implică modificări şi în unele cazuri în alte tabele sau câmpuri ca efecte secundare;
- şterg informații din baza de date ce nu mai sunt de folos sau au fost introduse eronat; acest tip de utilizator are nevoie de privilegii de acces ridicate şi bine delimitate pentru a selecționa tabelele şi câmpurile la care are acces; prin implementarea mecanismelor de ştergere logică se creează premisele unui management mai bun a bazei de date şi se micşorează riscurile de pierdere definitivă a informațiilor;
- validează modificările; acest tip de utilizator are un nivel de acces ridicat având sarcina de a valida modificările, adăugările sau operațiile de ştergere inițiate de ceilalți utilizatori; acest rol de utilizator este necesar în contextul în care produsul informatic lucrează cu informații valoroase cum sunt date bancare sau indicatori de bursă pentru a asigura integritatea bazei de date şi acuratețea ei; privilegiile sunt date în funcție de poziția şi gradul de competență al utilizatorului, având domenii de specialitate unde are experiența necesară pentru a valida modificările aduse tabelei sau câmpurilor alterate;
- administrează produsul informatic şi au cel mai înalt nivel de acces dintre toți utilizatorii; acest tip de utilizator are drepturi de gestiune asupra bazei de date aducând modificări structurale şi gestionând datele stocate în bază, are drepturi de gestiune a utilizatorilor a permisiilor atribuite lor şi a activării şi dezactivării conturilor de utilizator.

În figura 6 se prezintă modalitatea de gestionare a modificărilor în baza de date de către Administrator reprezentat de utilizatorul U_1, utilizatorii cu drepturi de validare U_2, respectiv U_3 şi utilizatorii ce efectuează modificările în baza de date U_4, U_5 şi U_6.

Figura 6 prezintă un scenariu limitat la şase utilizatori pentru diferențierea uşoară a nivelurilor de acces şi a rolurilor utilizatorilor. În produsele informatice aflate în uz există un număr foarte mare de utilizatori ce efectuează modificări.

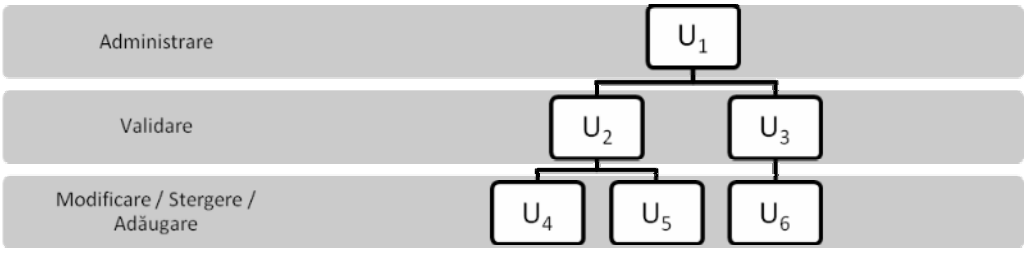

Figura 6. *Validarea operațiilor realizate de utilizatori*

Tipurile de utilizatori sunt ierarhizați în funcție de tipurile de privilegii pe care le primesc în cadrul aplicației distribuite. În figura 7 se realizează ierarhizarea utilizatorilor în funcție de grupul de permisii pe care le dețin în produsul informatic.

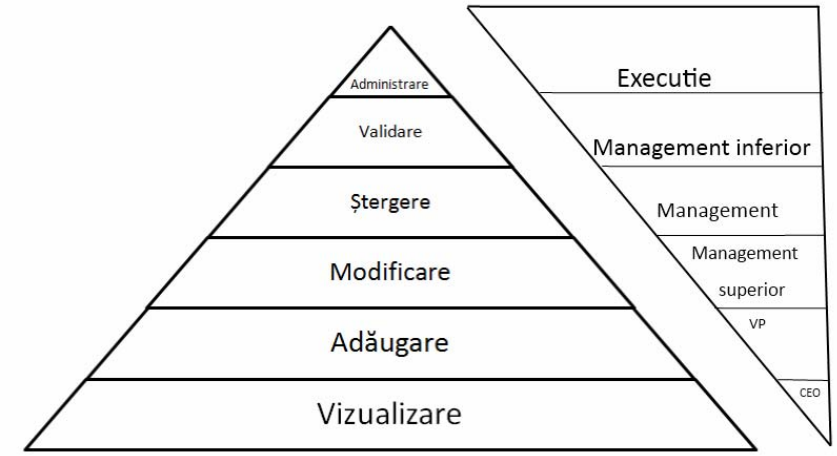

Figura 7. *Ierarhizarea tipurilor de utilizatori pe ierarhia din organizație*

Tipurile de utilizatori sunt determinate prin legătură directă cu atribuțiile utilizatorilor şi legătura lor cu entitățile din baza de date. Restricțiile de acces la tabele şi la câmpuri sunt gestionate în funcție de tipul utilizatorului. În cazul în care utilizatorul nu are privilegiile necesare pentru vizualizarea, modificarea sau ştergerea unui câmp sau a unei înregistrări dintr-o tabelă operațiunea este suspendată, iar acțiunea este înregistrată în tabela ce este destinată menținerii evidenței abaterilor de la regulile de acces impuse.

Concluzii

Aplicațiile online prezintă un interes crescut deoarece oferă servicii de o complexitate crescută într-un mediu distribuit. Aplicațiile online lucrează eficient cu baze de date ce fac uz de servicii şi au interfețe intuitive pentru utilizatori. Există aplicații online cu caracter informativ ce prezintă date de interes general, dar şi aplicații online ce realizează prelucrări de informații confidențiale ce necesită restricții de acces.

Problematica accesului la date este important să fie tratată pentru a delimita strict granițele între datele confidențiale şi cele neconfidențiale. Acest lucru este realizat prin analizarea fluxurilor de informații din cadrul aplicației informatice online. Este necesară stabilirea metodelor de acces la tablele din baza de date şi la câmpurile din tabele.

Prin utilizarea matricelor de acces la date se prezintă clar privilegiile de acces pentru tipurile de utilizatori din aplicația informatică online. Este necesară stabilirea pentru fiecare tip de utilizator a permisiilor de acces pentru a corela privilegiile de acces cu informațiile la care se oferă acces. Matricea de acces la date este un indicator stabil pentru gradul de acces al utilizatorilor, prezentând variații mici la un număr mic de operații disponibile unui număr mic de utilizatori, dar variații ridicate la un număr mare de operații disponibile pentru un număr ridicat de utilizatori.

Utilizarea matricei tridimensionale ca metodă de reprezentare a privilegiilor de acces este reprezentativă în contextul evaluării numărului de utilizatori şi a permisiilor pentru câmpurile din tabelele asociate operațiilor permise.

Aplicația informatică AVIO este realizată pentru a analiza ortogonalitatea identificatorilor de organizație. Procesele implementate pentru determinarea gradului de diferență sunt accesibile numai utilizatorilor înregistrați. Aplicația pune la dispoziție pentru vizualizarea identificatorii stocați în baza date. Procesul de configurare al accesului are la bază nivelul de confidențialitate al informațiilor. În acest scop numai administratorul are acces la informațiile de rulare şi baza de utilizatori a aplicației AVIO.

Costurile de realizare a matricei de acces la date sunt scăzute deoarece implică o analiză a modalităților de lucru din aplicația online prin identificare operațiilor în cazurile de utilizare. Valoarea costurilor de identificare a privilegiilor de acces potrivite tipurilor de utilizatori este mai scăzută utilizând matricea de acces în etapa de elaborare a specificațiilor decât determinarea lor în etapa de dezvoltare a sistemului de securitate.

Mulțumiri

Acest articol a fost elaborat ca parte a proiectului "Doctorat şi doctoranzi în triunghiul educație-cercetare-inovare (DOC-ECI)", proiect cofinanțat din Fondul Social European prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013 şi coordonat de Academia de Studii Economice din Bucureşti.

Notă

(1) Vezi http://www.ietf.org/rfc/rfc2828.txt

Bibliografie

Roşca, I.Gh., Ghilic-Micu, B., Stoica, M. (2006). *Informatica: societatea informațională: e-serviciile*, Editura Economică, Bucureşti, ISBN (10) 973-709-266-X

Cotfas, L., „A Genetic Algorithm and GIS based solution for public transport networks", *The Proceedings of the Ninth International Conference on Informatics in Economy*, 2009a, ISBN 978-606-505-178-2

Cotfas, L.A., „Advanced personalization of location based services", *4th International Conference on Knowledge Management: Projects, Systems and Technologies*, pp. 31-34, Bucharest: "Carol I" National Defence University, 2009b, ISBN 978-973-663-783-4

Vintilă, B., Pavel, S., „Assisted Design, Development And Evaluation Of Citizen Oriented Collaborative Applications", *Journal of Applied Collaborative Systems*, vol. 2, no. 3, 2010, ISSN 2066-7450

Dicționarul explicativ al limbii române (1998), Academia Română, Institutul de Lingvistică „Iorgu Iordan", Editura Univers Enciclopedic

Palaghita, D., „Quality characteristics of open source components", *Open Source Journal*, www.opensourcejournal.ro, 2009

Ivan, I., Boja, C. (2004). *Metode statistice în analiza software,* ISBN 973-594-498-7, Editura ASE, Bucureşti

Doinea, M., Ciurea, C., Dumitrache Marilena, „Collaborative Environmental Security Facing the Challenges of the Economic Process Development", *Proceedings of 17th International Economic Conference – IECS 2010*, „The Economic World Destiny: Crisis and Globalization?", May 13-14, 2010, Sibiu, Romania, Special Issue of Revista Economica, Lucian Blaga University of Sibiu

Doinea, M., Pavel, S., „Security Optimization for Distributed Applications Oriented On Very Large Data Sets", *Informatica Economica Journal*, Vol. 14, No. 2, 2010, ISSN 1453-1305

Cotfas, L.A., Diosteanu, Andreea, Smeureanu, I., „Knowledge Dynamics in Semantic Web Service Composition for Supply Chain Management", *Journal of Applied Quantitative Methods*, Vol. 5, No. 1, 2010, ISSN 1842-4562

Ivan, I., Vintila, B., Ciurea, C., Doinea, M., „The Modern Development Cycle of Citizen Oriented Applications", *Studies in Informatics and Control*, Vol. 18, No. 3, 2009, ISSN 1220-1766

Ivan, I., Vintila, B., Ciurea, C., Doinea, M., „Citizen Oriented Informatics Applications development Cycle", *Ekonomika, Statistika, Informatica, MESI*, No. 4, 2009b, ISSN 1994-7844