UNIVERSITATEA TEHNICĂ A MOLDOVEI

Cu titlu de manuscris
C.Z.U: 004.056(043)

DANILESCU MARCEL

CONTROLUL ACCESULUI ȘI ACȚIUNILOR ÎN SISTEMELE INFORMAȚIONALE

232.02 – TEHNOLOGII, PRODUSE ȘI SISTEME INFORMAȚIONALE

Teză de doctor în informatică

Conducător științific: **Beșliu Victor,**
dr., prof. univ.

Autor: **Danilescu Marcel**

CHIȘINĂU, 2021

CUPRINS

ADNOTARE

la teza „Controlul accesului și acțiunilor în sistemele informaționale” prezentată de către Danilescu Marcel pentru conferirea titlului științific de doctor în informatică, Chișinău, 2020

Structura tezei: introducerea, 4 capitole, concluzii generale și recomandări, bibliografia cu 78 titluri, 5 anexe, 128 pagini text de bază, inclusiv 21 de figuri și 17 tabele. Rezultatele sunt publicate în 11 lucrări.

Cuvinte cheie: Control acces, control acțiuni, obiecte, domenii, organizații, confidențialitate, integritate, tupluri, modelare XML.

Domeniul de studiu: Confidențialitatea și integritatea datelor și informațiilor.

Scopul tezei: Modelarea controlului accesului și a acțiunilor utilizatorilor asupra documentelor în format electronic, prin aplicarea politicilor bazate pe încredere.

Obiective: Utilizarea încrederii acordate membrilor organizațiilor, exemplificarea utilizării fluxurilor de lucru din organizații în scopul construirii politicilor bazate pe încredere, stabilirea condițiilor de interacțiune dintre obiect și subiect pe baza politicilor de încredere, definirea și crearea politicilor de control al accesului și acțiunilor, exemplificarea utilizării tehnologiei xml.

Noutatea și originalitatea științifică: S-a dezvoltat o nouă metodă, de asigurare a confidențialității și integrității datelor și informațiilor. Pentru prima dată au fost formalizate condițiile de încredere pe care trebuie să le îndeplinească un utilizator pentru a accesa un obiect și a interacționa cu acesta. Au fost create exemple de utilizarea documentelor în format xml.

Problema științifică soluționată: S-a creat o metodă de aplicare a încrederii acordate utilizatorilor pentru accesarea datelor și informațiilor din sistemele informatice ale organizației și modelarea proceselor informatice care acționează asupra acestora.

Semnificația teoretică: S-au creat noi paradigme (niveluri și valori de încredere) și s-au formalizat condițiile de aplicare a politicilor de încredere. S-au creat modele de aplicare a politicilor de control ale accesului și al interacțiunii dintre subiect (utilizator) și obiect, și s-au pus bazele unor cercetări ulterioare în domeniul controlului accesului, integrității și confidențialității datelor.

Valoarea aplicativă: În premieră au fost create modele noi, bazate pe încrederea în subiect, modele ce permit rafinarea și simplificarea controlului accesului, confidențialității și integrității datelor precum și a metodelor de proiectare și implementare ale acestora.

Implementarea: Rezultatele cercetării științifice au fost testate și implementate în cadrul proiectului PNCD-România, pentru Institutul de Cercetare Dezvoltare pentru Ecologie Acvatică, Pescuit și Acvacultură – Galați (I.C.D.E.A.P.A.).

ABSTRACT

to thesis „Control of access and actions in informational systems" presented by Danilescu Marcel for conferring the scientific title of PhD in Informatics
Chișinău, 2020

The thesis structure: introduction, 4 chapters, general conclusions and recommendations, bibliography with 78 titles, 5 annexes, 128 basic text pages, including 21 figures and 17 tables. The results are published in 11 papers.

Key words: Access control, action control, objects, domains, organizations, privacy, integrity, tuples, xml modeling.

The field of the investigation: Confidentiality and integrity of data and information.

The thesis aim: Modeling access control and user actions on documents in electronic format, by applying policies based on trust.

The objectives: Using trust in members of organizations, exemplifying the use of workflows in organizations to build trust-based policies, establishing conditions for interaction between object and subject based on trust policies, defining ,and creating access control policies and actions, exemplifying the use of xml technology.

Scientific novelty and originality of the results: A new method has been developed to ensure the confidentiality and integrity of data and information. For the first time, the conditions of trust that a user must meet in order to access an object and interact with it have been formalized. Examples of using xml documents have been created.

The scientific problem solved: A method of enforcing user trust has been created, to access data and information from the organization's IT systems and model the IT processes that act on them.

The theoretical importance: New paradigms (levels and values of trust) have been created, and the conditions for the implementation of trust policies have been formalized. Models have been created for the application of access control policies and the interaction between the subject (user) and the object, and the basis for further research in the field of access control, data integrity and confidentiality has been laid.

The applied value of the thesis: For the first time, new models have been generated based on trust in the subject, that allow refining and simplifying the control of access, confidentiality, and integrity of data as well as their design and implementation methods.

The implementation: The results of the scientific research were implemented within the PNCD-Romania project, for the Development Research Institute for Aquatic Ecology, Fisheries and Aquaculture - Galați (I.C.D.E.A.P.A.).

LISTA ABREVIERILOR

ABAC - Attribute Based Access Control (Controlul accesului bazat pe atribute)

EPAL - Enterprise Privacy Authorization Language (Limbaj de autorizare a confidențialității în întreprindere)

NIST - National Institute of Standards and Technology (Institutul național de standard și tehnologie)

MITRE - Corporație din SUA

RBAC - Role-Based Access Control (Control al accesului bazat pe roluri)

XACML - eXtensible Access Control Markup Language (Limbaj de marcare extensibil pentru controlul accesului)

DAI - Distributed Artificial Intelligence

LISTA TABELELOR

LISTA FIGURILOR

INTRODUCERE

Actualitatea temei și importanța problemei abordate: Pentru orice organizație, informația aflată în format electronic, fie că este vorba de baze de date, informații financiare, date contabile, profilurile angajaților și multe alte documente, publice sau cu diferite nivele de clasificare, reprezintă una dintre cele mai importante valori.

Necesitatea de informare, presupune și o protecție a informațiilor, pentru a nu permite devoalarea unor informații sensibile la niveluri de competență care nu au capacitatea de prelucrare și păstrare a confidențialității datelor. Prin urmare, este foarte importantă politica de asigurare a confidențialității și integrității datelor.

În privința controlului accesului la date și informații nu se poate face o abordare simplistă a drepturilor de acces de tipul permis/respins, sau altfel spus, de încredere și de neîncredere. De aceea, tema de cercetare, prin rafinarea și simplificarea controlului accesului, confidențialității și integrității datelor precum și a metodelor de proiectare și implementare ale acestora, prin introducerea politicilor bazate pe relații de încredere, aduce o îmbunătățire substanțială satisfacerii necesității de informare la toate nivelurile unei organizații.

Scopul lucrării

Ipoteza de lucru stabilită, este modelarea controlului accesului la documente în format electronic și a acțiunilor asupra acestora, prin aplicarea politicilor bazate pe încredere, scop atins prin realizarea următoarelor obiective:

- cuantificarea nivelurilor de încredere acordate membrilor organizațiilor;
- modelarea fluxurilor de lucru pentru câteva tipuri de organizații în scopul de a construi suportul pentru implementarea politicilor bazate pe încredere;
- stabilirea condițiilor pe care trebuie să le îndeplinească un utilizator pentru a avea acces și a interacționa cu un obiect pe baza politicilor de încredere;
- definirea politicilor de control al accesului, implementate pe durata fuxului de lucru modelat;
- crearea politicilor și modelarea controlului accesului și acțiunilor bazate pe încredere, utilizând tehnologii *xml*.

Metodologia cercetării științifice

Pornind de la ipoteza de lucru enunțată mai sus, teza reprezintă un progres față de stadiul actual al cercetărilor, o soluție atât teoretică cât și tehnică, aplicabilă pentru rezolvarea problemelor propuse spre a fi rezolvate.

Metodele de cercetare utilizate în teză sunt:

- **Abstractizarea** – au fost abstractizate: domeniile, obiectele care aparțin domeniilor, relațiile dintre utilizatori și obiecte pe baza nivelurilor de încredere ale obiectelor și valorilor de încredere atribuite utilizatorilor.
- **Formalizarea/matematizarea** – s-au formalizat condițiile pe care trebuie să le îndeplinească un utilizator pentru a accesa un obiect al unui domeniu, utilizându-se elemente din teoria mulțimilor.
- **Deducția** – au fost făcute raționamente, de la general la particular, și anume:
    - de la grupuri de obiecte la obiect;
    - de la domeniile grupurilor de obiecte la domeniu;
    - de la grupuri de utilizatori la utilizator;
    - de la nivelul de încredere al grupului la nivelul de încredere al utilizatorului;
    - de la contextul de lucru al grupului la contextul de lucru al utilizatorului.
- **Inducția** - au fost făcute raționamente, de la particular la general, și anume: prin generalizare se permite ca politica de încredere față de un obiect sau categorie de obiecte, aplicată unui utilizator, să fie aplicată tuturor membrilor din grupul lui, care au același nivel de încredere.
- **Clasificarea și tipologia** – prin operația logică de divizare a volumului noțiunii, au fost elaborate clasificări ale politicilor de încredere, după mai multe criterii: după modul de implementare (normale, stricte și hibride), după complexitate (simple și derivate).
- **Metoda axiomatică** – prin generarea de enunțuri afirmative care nu necesită demonstrare, așa cum sunt numeroasele definiții din teză: obiectul, grupul de obiecte, ciclul de viață al unui obiect, utilizatorul, grupul de utilizatori, domeniul de activitate, valoarea de încredere, nivelul de încredere, ierarhia parțial ordonată, relația, relația de încredere, procesul, contextul de încredere, restricțiile, delegarea, politicile normale, politicile stricte, politicile hibride, politica de control simplă, politica de control derivată, fluxul de lucru, contextul de lucru.

Prin aplicarea metodelor de cercetare mai sus menționate, a fost creată și demonstrată o nouă metodă de asigurarea confidențialității și securității sistemelor informatice.

Noutatea științifică constă în dezvoltarea unei noi metode de control al accesului și acțiunilor utilizatorilor, având ca bază încrederea pe care a căpătat-o un utilizator într-o organizație. Prin intermediul relațiilor de încredere, privind accesul la datele și procesele din cadrul sistemului informatic, se asigură confidențialitatea și integritatea datelor și informațiilor aplicându-se politicile de control al accesului și acțiunilor. Au fost create modele de documente în format *xml*,

în care sunt integrate elementele ce specifică domeniile de acțiuni, domeniul de procesare, contextul și tipul proceselor care pot fi aplicate obiectelor grupate pe domenii de activitate. Au fost generate modele de implementare a politicilor pentru informații clasificate pe domenii de activitate și grade de sensibilitate.

Problema științifică soluționată constă în găsirea metodelor de aplicare a încrederii acordate utilizatorilor pentru accesarea datelor și informațiilor din sistemele informatice ale organizației și crearea de procese informatice care acționează asupra acestora.

În ultimi 25 de ani s-au efectuat studii și cercetări privind încrederea în cadrul organizațiilor, calculându-se valorile încrederii acordate unor agenți, utilizatori, ținând cont de diverși parametri cum ar fi: reputația, disponibilitatea, benevolența, etc., cât și încrederea în agenții ce făceau recomandările.

Lucrarea de față și-a propus să ducă mai departe această problemă a încrederii obținute de un agent (utilizator), prin aplicarea valorilor de încredere obținute de acesta, în asigurarea controlului accesului și acțiunilor în cadrul organizației.

Lucrarea abordează condițiile ce trebuie îndeplinite de un utilizator pentru a avea acces la obiectele din cadrul organizației și procesele ce-i sunt permise a le aplica acestora.

Din studiile și cercetările efectuate, lucrarea de față, este printre primele lucrări, care abordează principiile de interacțiune dintre subiect și obiect în condițiile utilizării încrederii ca parametru.

Semnificația teoretică. Studiile și cercetările efectuate au condus la formularea unor noi paradigme (niveluri și valori de încredere) și s-au stabilit condițiile de aplicare a politicilor de încredere, care vor constitui puncte de pornire pentru cercetările viitoare.

Au fost create modele de aplicare a politicilor de control ale accesului și al interacțiunii dintre subiect (utilizator) și obiect.

S-au pus bazele unor cercetări ulterioare în domeniul controlului accesului, integrității și confidențialității datelor.

Valoarea aplicativă a lucrării. În premieră au fost generate modele care permit rafinarea și simplificarea controlului accesului, confidențialității și integrității datelor precum și a metodelor de proiectare și implementare a acestora, prin introducerea politicilor bazate pe relații de încredere.

Implementarea rezultatelor cercetării științifice a avut loc în cadrul parteneriatului dintre S.C. ASWIC s.r.l. și Institutul de Cercetare Dezvoltare pentru Ecologie Acvatică, Pescuit și Acvacultură – Galați (I.C.D.E.A.P.A.) România, prin proiectarea și implementarea soluțiilor de control al accesului și acțiunilor utilizatorilor bazate pe apartenența la domenii de activitate și pe ierarhii de acțiuni.

Rezultatele cercetărilor au fost transpuse în practică suplimentar prin realizarea unei aplicații, implementată la societatea ASWIC srl, pentru asistarea proiectanților de aplicații informatice bazate pe încredere. Aplicația denumită „Trust Analist" este prezentată în Anexa 1.

Rezultatele cercetărilor realizate au fost publicate în 11 lucrări științifice din diverse reviste și culegeri de specialitate.

Rezultatele științifice înaintate spre susținere:

1. Definițiile valorii de încredere, a contextului de încredere, a relației de încredere și a ierarhiilor și sub ierarhiilor parțial ordonate;
2. Modelul matematic al condițiilor de aplicare a politicilor de control al accesului și acțiunilor bazate pe încredere;
3. Demonstrarea asigurării confidențialității și integrității datelor prin modelarea politicilor de control al accesului în vederea respectării condițiilor Biba;
4. Metoda de aplicare a încrederii în construirea politicilor de control al accesului și acțiunilor bazate pe încredere;
5. Modele de aplicabilitate a politicilor de control al accesului și acțiunilor bazate pe încredere.

Aprobarea rezultatelor cercetărilor. Rezultatele tezei au fost validate în cadrul lucrărilor publicate în reviste internaționale și naționale:

1. Journal of Social Sciences Chișinău, Republica Moldova, Universitatea Tehnică a Moldovei, 2020
2. The Journal of Accounting and Management, 2(3), 2012, Galați, România, Universitatea Danubius
3. Acta Universitatis Danubius. Œconomica, 7(6), 2011, Galați, România, Universitatea Danubius
4. EuroEconomica 2, 2010, Galați, România, Universitatea Danubius

De asemenea, rezultatele tezei au fost prezentate la Conferințele Internaționale și publicate în lucrările Conferințelor:

1. Danubius International Conferences, 15th International Conference on European Integration - Realities and Perspectives, Vol 15, No1 (2020) Galați, România, Universitatea Danubius
2. International Conference on Information Technologies and Security 2012, Chișinău, Republica Moldova
3. Conferința Internațională „Educație și creativitate pentru o societate bazată pe cunoaștere" ediția a IV-a 2010, Universitatea „Titu Maiorescu", București, România.
4. IACSIT (Ed.), 2011 3rd International Conference on Computer technology and Development. Chengdu, 2011 China

5. Conferința Internațională „Educație și creativitate pentru o societate bazată pe cunoaștere” ediția a III-a 2009, Universitatea „Titu Maiorescu”, București, România.
6. The Tenth International Conference on Informatics in Economy IE 2010, Bucuresti, România.
7. International Conference on Computer and Software Modeling, ICCSM 2010, Manila, Philippine: Institute of Electrical and Electronics Engineers, Inc.

Structura și volumul lucrării. Teza este compusă din: introducere, patru capitole, concluzii generale și recomandări, bibliografie cu 78 titluri și 3 anexe. Conținutul de bază al tezei este expus pe 128 pagini text și inserează 21 de figuri și 17 tabele.

Cuvinte-cheie: Controlul accesului, controlul acțiunilor, politici, obiecte, domenii, organizații, încredere, confidențialitate, integritate, tupluri, modelare xml

Conținutul tezei. Primul capitol intitulat „ Principalele abordări anterioare în securitatea documentelor din sistemele informatice” face o trecere în revistă și o descriere condensată a modelelor politicilor de securitate: Bell-LaPadula, Biba, Clark-Wilson, RBAC și a limbajelor pentru definirea politicilor de confidențialitate: EPAL și XACML.

Se face o introducere în teoria încrederii (trust theory) prin analiza și sinteza unor cercetări care au stat la baza tezei, ca punct de pornire. Sunt definite și descrise conceptele de încredere și de reputație și este prezentată formalizarea încrederii în diferite abordări ale mai multor autori: Stephen Paul Marsh, Abdul-Rahman și Hailes, Lik Mui, George Pitsilis și Lindsay Marshal, Indrajit Ray și Sudip Chakraborty, Zuo și Panda.

În capitolul al doilea sunt prezentate: definiția organizațiilor, diverse clasificări ale acestora, și modul de organizare; încrederea în cadrul organizației, clasificarea încrederii și o etichetare a acesteia; exemple de implicare a încrederii în procesul formal-decizional al organizațiilor. Este arătat modul în care documentele formate în organizație sunt folosite în procesele decizionale prin intermediul acțiunilor utilizatorilor, trecând apoi la o conceptualizare a acestora prin abstractizarea lor și, prezentarea sub forma generică de obiecte care sunt supuse acțiunilor subiecților prin aplicarea încrederii. Este prezentat modul de clasificare a încrederii în cadrul unei organizații și relațiile între încrederea atribuită subiecților și obiectele din organizație.

În capitolul al treilea sunt definite elementele care concură la crearea politicilor bazate pe încredere și este prezentat un model de creare a acestora. Au fost definite elementele ce concură la crearea unei politici de control al accesului și acțiunilor bazată pe încredere. A fost prezentată condiția generală pentru ca un utilizator (subiect) să poată efectua o acțiune sau un set de acțiuni asupra unui obiect, prin intermediul politicilor. De asemenea, este subliniată importanța fluxului de lucru în proiectarea și aplicarea acestor politici.

Pe parcursul cercetării, în lucrările publicate, pentru proiectarea fluxului de lucru a fost utilizat standardul BPMN 2.0 [50; 51] și cele ale „Workflow patterns”[75; 76] ceea ce a asigurat o reprezentare eficientă a acestuia. În cadrul lucrării curente, a fost utilizat modelul de schemă inter funcțională, datorită simplității prezentării.

Au fost prezentate elementele care stau la baza modelării, proiectării și implementării politicilor de control al accesului și acțiunilor bazate pe încredere. S-au exemplificat cum se pot aplica politici de încredere care asigură confidențialitatea și integritatea datelor. S-a arătat cum se construiesc matricele de acces și de restricții și delegații.

În capitolul al patrulea, a fost abordat controlul accesului și al acțiunilor utilizatorilor unui sistem informatic bazat pe încredere. Au fost prezentate trei exemple de modelare a accesului și acțiunilor utilizatorilor asupra documentelor electronice, pentru diferite tipuri de organizații, și diferite arhitecturi ale sistemului informațional. Au fost prezentate trei exemple teoretice, de implementare a politicilor de control al accesului și acțiunilor utilizatorilor, de la o aplicare simplă în care politicile sunt aplicate la nivel de grupuri de lucru, până la o aplicare complexă în cadrul organizațiilor cu informații clasificate. S-a demonstrat flexibilitatea politicilor de control al accesului și acțiunilor bazate pe încredere, în implementarea și utilizarea lor.

1. PRINCIPALELE ABORDĂRI ANTERIOARE ÎN SECURITATEA DOCUMENTELOR DIN SISTEMELE INFORMATICE

Una din modalitățile de asigurare a securității documentelor este controlul accesului.

Prezentul capitol prezintă termenii utilizați în lucrare și face o trecere în revistă a principalelor cercetări din domeniul securității documentelor în format electronic.

În acest capitol, sunt prezentate lucrări ce au stat de-a lungul timpului la baza standardelor de proiectare a aplicațiilor și a sistemelor de securitate. De la modelul Bell-LaPadula, până la prezentarea modelului ABAC, sunt evocate, lucrări importante din cercetarea domeniului securității și controlului accesului și acțiunilor utilizatorilor. În continuare o parte dintre aceste lucrări, sunt prezentate pe scurt, întrucât au influențat cercetarea de față.

1.1. Controlul accesului -Termeni, definiții, istoric și cercetări anterioare

Controlul acțiunilor reprezintă exercitarea controlului asupra celor care pot interacționa cu o resursă. De multe ori, dar nu întotdeauna, acest lucru implică o autoritate, care exercită acest control pe baza unui set de reguli stabilit aprioric.

Confidențialitatea datelor este limitarea accesului la informație și nedivulgarea utilizatorilor autorizați cât și prevenirea accesului sau divulgarea acestora către persoanele neautorizate. Cu alte cuvinte, informația este disponibilă doar persoanelor autorizate.

Integritatea datelor se referă la încrederea în resursele informaționale. Încrederea include conceptul de „integritate a datelor" - și anume, faptul că datele nu au fost modificate în mod necorespunzător, fie prin accident sau o printr-o activitate răuvoitoare deliberată și include, de asemenea, stabilirea „originii" sau „integritatea sursei" -, faptul că datele au venit de la persoana sau entitatea despre care se crede că le-a generat, mai degrabă decât de la un impostor (autenticitatea sursei).

Integritatea poate include chiar și ideea că persoana sau entitatea în cauză a introdus informații corecte sau că informațiile reflectă circumstanțele reale (în statistică, există conceptul de „valabilitate") și că, în aceleași circumstanțe, ar genera date identice (ceea ce statisticienii numesc „fiabilitate").

Dintr-un punct de vedere mai restrictiv, integritatea unui sistem de informare include doar conservarea datelor fără a fi corupte, a tot ce a fost transmis sau a intrat în sistem, indiferent dacă este corect sau greșit.

Disponibilitatea datelor se referă la disponibilitatea resurselor de informare. Disponibilitatea, ca și alte aspecte de securitate, poate fi afectată de probleme pur tehnice (de

exemplu, o parte disfuncțională a unui computer sau dispozitiv de comunicare), fenomene naturale (de exemplu, vântul sau apa), sau de cauze umane (accidental sau intenționat).

În data de 1 martie 1973 Bell D. Elliott și LaPadula J. Leonard au publicat lucrarea „Secure Computer Systems: Mathematical Foundations", în MITRE Technical Report 2547, Volume I [8]. Acesta a fost un moment definitoriu pentru cercetarea în domeniul securității datelor din sistemele de calcul, prin crearea unei metode matematice de exprimare a unui model de securitate.

Au reluat prezentarea conceptelor de securitate expuse, în lucrarea „Secure Computer System: Unified exposition and multics interpretation" [7].

În 1975, Keneth J. Biba, a abordat problema integrității datelor și informațiilor în lucrarea „Integrity Considerations for Secure Computer Systems", având ca punct de plecare lucrările lui Bell D. Elliott și ale lui LaPadula J. Leonard.

Ulterior Dorothy E. Denning în 1976, a publicat articolul „A lattice model of secure information flow" în Communication of ACM numărul din luna mai, articol în care prezintă o vedere ce unifică diversele sisteme de restricționare a fluxului de informații, creând posibilitatea clasificării acestora conform cu obiectivele de securitate și sugerând abordări noi [29].

Modelul bazat pe „lattice" a fost dezvoltat de Sadhu, Ravi S. în noiembrie 1993 în lucrarea „Lattice-based access control models" publicată în IEEE Computer [64].

Acest model bazat pe „lattice" (numit și LBAC - Lattice based access control) este cunoscut ca și controlul accesului bazat pe etichete.

În 1994 Stephen Paul Marsh, în lucrarea „Formalising Trust as a Computational Concept" a pus bazele conceptelor de încredere aplicate agenților inteligenți [45].

În 1996 a fost prezentat modelul bazat pe roluri de către Ravi S. Sadhu și alții, model adoptat de NIST și refăcută prezentarea acestuia în lucrarea „The NIST Model for Role-Based ACCESS Control: Towards a Unified Standard" [65, 66].

În 2003, Compania I.B.M. a prezentat modelul EPAL (Enterprise Privacy Authorization Language) pentru asigurarea confidențialității, consorțiului W3C pentru standardizare [4].

În 2005 organizația OASIS a publicat XACML (eXtensible Access Control Markup Language) care a devenit un model de facto pentru modelarea securității datelor [49].

Pitsilis Giorgios și Marshall Lindsay cu lucrarea „Trust as a Key to Improving Recommendation Systems" [57] abordează problema sistemelor de recomandare din rețelele centralizate, comparându-le eficiența și performanța, căutând să ofere o soluție de îmbunătățire a calculabilității încrederii a recomandorului în recomandat.

În 2009 Danilescu Laura și Danilescu Marcel au prezentat „Tehnici bazate pe XML pentru confidențialitatea datelor în e-business la Conferința Internațională „Educație și creativitate pentru o societate bazată pe cunoaștere” Universitatea Titu Maiorescu – [20].

În 2010 Danilescu Laura și Danilescu Marcel au prezentat în cadrul conferinței ICCSM 2010 – Manila, Philipine „Controlul accesului la informații aplicând politici bazate pe ierarhii de încredere [23].

În 2011 Adomnicăi Cosmin și Danilescu Marcel au prezentat lucrarea „Asigurarea unui model de comportament în rețelele sociale bazate pe încredere” ICCTD 2011 Chengdu, China [1].

În 2014, Smari W. Waleed, Clemente Patrice și Lalande Jean-Francois în lucrarea „An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system” [69] prezintă un model extins de control al accesului bazat pe atribute asociate cu obiecte și subiecți. Incorporează probleme de încredere și confidențialitate pentru a face ca deciziile de control al accesului să fie sensibile la contextul de colaborare între organizații, printr-un studiu de caz care arată politici ABAC în domeniul sistemelor distribuite de gestionare a crizelor cu organizații multiple, incorporând un motor de decizie ce evaluează dinamic a încrederea și confidențialitea.

”Dynamic Trust Based Access Control Framework for Securing Multi-Cloud Environment” [6] este lucrarea din 2014, în care R. K. Banyal, V. Jain, P. Jain propun un cadru de control al accesului ce abordează problemele de securitate și confidențialitate în cloud. Acest cadru se bazează pe încrederea dinamică a utilizatorului folosind mai multe straturi, politici și mecanisme de control al accesului. Controlul accesului se bazează pe încrederea utilizatorului pentru a reduce posibilitatea de a efectua activități neautorizate și asigură accesul doar la resursele cloud ale utilizatorului autorizat.

În 2014 Feraiolo David și alții în cadrul NIST au publicat „Guide to Attribute Based Access Control (ABAC) Definition and Considerations”, lucrare ce vine să completeze contribuția NIST la cercetarea și standardizarea metodelor de proiectare în vederea asigurării securității datelor și informațiilor din sistemele informaționale[40].

”MT-ABAC: A Multi-Tenant Attribute-Based Access Control Model with Tenant Trust” este lucrarea în care Pustchi Navid și Sandhu Ravi în 2015 [59] prezintă un nou model de control al accesului bazat pe atribute (ABAC) pentru a permite colaborarea între clienții dintr-un cloud IaaS. Abordarea lor permite repartizarea atributelor între clienți pentru a oferi acces la resursele partajate între aceștia. Modelul de control al accesului bazat pe atribute multi-chiriași a fost denumit ca MT-ABAC.

Rajpoot Qasim Mahmood, Damsgaard Jensen Christian și Hhishnan Ram au abordat problema integrării atributelor în RBAC [60].

În lucrarea, „AR-ABAC: A New Attribute Based Access Control Model Supporting Attribute-Rules for Cloud Computing," din 2015 [62], Khaled Riad, ZhuYan, Hongxin Hu și Gail-Joon Ahn au creat un model ce asociază utilizatorii cu obiectele, și propun accesarea obiectelor pe baza nivelurilor lor de sensibilitate. Ei au stabilit un acord care determină ce fel de atribute ar trebui utilizate și apoi numărul de atribute luate în considerare pentru luarea deciziilor de acces, în vederea asigurării partajării în siguranță a resurselor între potențialii chiriași de încredere ai serviciilor de cloud. De asemenea se acceptă diferite permisiuni de acces pentru același utilizator în aceeași sesiune.

Chiregi Matin și Navimipour Nima Jafari au publicat lucrarea „A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities" în 2016 [14]. În lucrare au propus o metodă de evaluare a încrederii în cloud computing folosind lideri de opinie și, entități troll ce permit construirea unui grad de încredere, în funcție de disponibilitate, fiabilitate, integritate a datelor, identitate și capacitate. Pentru aceasta se utilizează trei măsuri topologice: măsuri de intrare, de ieșire și măsuri de încredere pentru identificarea liderilor de opinie. Aceasta permite actualizarea valorilor de încredere și reputație prin eliminarea efectului entităților troll și folosirea sfaturilor liderilor de opinie.

Conectarea la dispozitivele IoT în mod dinamic presupune cerințe de securitate ridicată. Utilizând ABAC pentru asigura securitatea într-un sistem distribuit, și bazându-se pe evaluarea încrederii, Junshe Wang, Han Wang, Hongbin Zhang și Ning Cao în 2017, în lucrarea „Trust and Attribute-Based Dynamic Access Control Model for Internet of Things" [73] propun un model de control al accesului bazat pe atribute de încredere.

În 2017 Khaled Riad și Zhu Yan în lucrarea „Multi-Factor Synthesis Decision-Making for Trust-Based Access Control on Cloud"[63] prezintă o metodă nouă bazată pe încredere ca baza pentru acordarea accesului, ce are o dinamică a permisiunilor atribuite utilizatorului pe baza nivelului său de încredere.

Cu lucrarea „Trust based access control model for securing electronic healthcare system" [67] din 2018 autorii Ashish Singh și Kakali Chatterjee propun un cadru de securitate bazat pe încredere pentru sistemul de sănătate (TBACMHS), compus din mecanismul de încredere, modelul de încredere și politicile de control al accesului care sporesc acuratețea și eficiența sistemului. Acest cadru de control al accesului are rolul de a asigura că doar utilizatorul de încredere autorizat, poate accesa datele și resursele.

În 2019 în lucrarea „TACRM: trust access control and resource management mechanism in fog computing” a autorilor Wided Ben Daoud, Mohammad S. Obaidat, Amel Meddeb-Makhlouf, Faouzi Zarai și Kuei-Fang Hsiao [24], propun un model de securitate care se bazează pe cooperarea dintre IoT și fog computing. Scopul modelului este un control eficient al accesului asociat cu un sistem de monitorizare pentru a asigura o cooperare sigură între diverse resurse și diferite părți operaționale și care, este bazat pe un control al accesului distribuit, în condiții de ultra-încredere și constrângeri cu latență redusă.

Lucrarea „Trust-Based Access Control in Cloud Computing Using Machine Learning” a autorilor Pabitr Mohan Khilar,Vijay Chaudhari și Rakesh Ranjan Swain [38] tratează securitatea datelor clienților într-un cloud, și a luat în considerare abordarea bazată pe încredere care oferă acces utilizatorului în cloud prin valoarea de încredere calculată pe baza acceselor și comportamentului trecut. Considerând diverși parametrii, cum ar fi comportamentul utilizatorului, falsa cerere de servicii, solicitarea neautorizată, cererea interzisă și specificarea intervalului, aceștia au propus o strategie de evaluare a încrederii bazată pe abordarea învățării automate care prezice valorile de încredere ale utilizatorului și resurselor. pentru a evalua sistemul de management al încrederii.

În lucrarea din 2019, „A Role and Trust Access Control Model for Preserving Privacy and Image Anonymization in Social Networks” autorii Nadav Voloch, Priel Nissim, Mor Elmakies și Ehud Gudes [71], au abordat confidențialitatea rețelelor sociale online. (OSN) iar dintre aspecte au abordat încrederea și credibilitatea care implică datele utilizatorului OSN transmise de diferite relații din rețea, date care sunt expuse într-un mod considerat a fi relativ privat, sau chiar parțial public, unor entități necunoscute și posibil nedorite, cum ar fi adversarii utilizatorului, roboții sociali, utilizatorii falși, spammerii sau culegătoriilor de date. În această lucrare este prezentat un nou model de control al accesului bazat pe rol și încredere, notat ca RTBAC, în care rolurile, care manifestă permisiuni diferite, sunt atribuite utilizatorilor conectați iar fiecărui utilizator îi este evaluată încrederea în funcție de mai multe criterii, cum ar fi numărul total de prieteni, vârsta contului de utilizator și durata prieteniei. Modelul creat se presupune că oferă decizii mai precise și viabile de partajare a informațiilor permițând un control mai bun al confidențialității în rețeaua socială.

Securitatea și confidențialitatea datelor din sistemele electronice de sănătate (EHS) este tratată de Ashish Singh și Kakali Chaterji în lucrarea „An adaptive mutual trust based access control model for electronic healthcare system” din anul 2020 [68]. Pornind de la necesitatea unui mecanism de control al accesului fără informații prealabile despre utilizatorii asistenței medicale cât și controlul volumului de date care va fi partajat de către serviciile medicale și de către medic,

scopul principal al lucrării este de a controla vizualizarea accesului, astfel încât numai utilizatorul autorizat să poată accesa informațiile într-un mod controlat. De aceea ei au propus un model de control al accesului, care se bazează pe gradul de încredere al utilizatorului și al serviciului medical, numit încredere reciprocă.

Panjun Sun în „Research on cloud computing service based on trust access control" [56], a propus un model de control al accesului pentru serviciile de cloud, bazat pe evaluarea încrederii directe, a riscului încrederii și feedbackul la aceasta, penalizare și recompense.

1.2. Modelul Bell-LaPadula

Acest model este cel mai cunoscut model al politicilor de securitate, fiind propus de David Bell și Len LaPadula [7; 8]. Modelul este cunoscut ca un model de securitate multi nivel. Sistemele ce le adoptă sunt numite MLS (Multi-Level Secure). Proprietatea de bază a acestor sisteme este aceea că informația poate circula în jos.

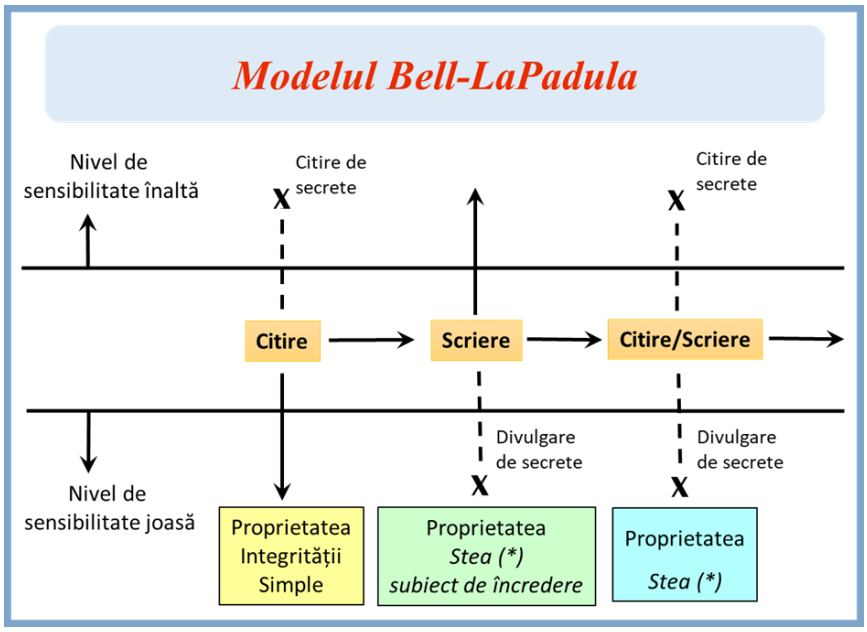


Figura 1.1. Modelul Bell-LaPadula cu cele trei principii
[Sursa: https://www.ktunotes.in/wp-content/uploads/2019/05/PIS-M2-Ktunotes.in_.pdf]

Formal, modelul Bell-LaPadula a introdus trei principii:

- ***principiul securității simple***, prin care nu-i este permis nici unui proces să citească date aflate pe un nivel superior lui. Este cunoscut ca No Read Up (NRU);
- ***principiul * (stea),*** *nici un proces nu poate scrie date pe un nivel aflat sub el. Este cunoscut și ca No Write Down (NWD);*
- ***principiul securității discreționare*** *introduce o matrice de acces pentru a specifica controlul accesului discreționar. Este cunoscut și ca Trusted Subject (subiect de încredere)*

*Prin acest principiu, subiectul de încredere violează principiul * dar nu se abate de la scopul său.*

În cele ce urmează vom face o scurtă prezentare a modelului Bell-LaPadula (D. Elliott Bell and Leonard J. LaPadula, 1973) [7; 8].

Modelul prezintă implementarea confidențialității bazată pe relațiile dintre subiecte, obiecte, pe baza clasificărilor acestora, precum și un model de mașină de stare utilizat pentru aplicarea controlului accesului în aplicațiile guvernamentale și militare.

Modelul Bell-LaPadula se axează pe confidențialitatea datelor și controlul accesului la informații clasificate. Entitățile dintr-un sistem informațional sunt împărțite în subiecte și obiecte. Este definită noțiunea de „stare sigură" și este dovedit că fiecare tranziție de stare păstrează securitatea trecând de la o stare sigură la alta, astfel că sistemul îndeplinește obiectivele de securitate ale modelului. Tranziția de la o stare la alta este definită prin funcțiile de tranziție.

O stare a sistemului este definită a fi „sigură" dacă singurele moduri de acces permise ale subiecților la obiecte sunt în conformitate cu o politică de securitate. Pentru a determina dacă un mod de acces specific este permis, permisiunea unui subiect este comparată cu clasificarea obiectului pentru a determina dacă subiectul este autorizat pentru modul de acces specific. Schema de degajare / clasificare este exprimată în termeni de grilă. Modelul definește o regulă de control de acces discreționar (DAC) și două reguli de control de acces obligatorii (MAC) cu trei proprietăți de securitate[7; 8]: de securitate simplă, stea și discreționară.

Transferul informațiilor de la un document cu sensibilitate înaltă la un document cu sensibilitate mai mică în modelul Bell – LaPadula, se poate face prin conceptul de subiecți de încredere. Subiecții de încredere nu sunt restricționați de proprietatea Stea. Aceștia trebuie să fie dovediți a fi de încredere în ceea ce privește politica de securitate.

Modelul de securitate Bell-LaPadula este îndreptat către controlul accesului.

Cu Bell-LaPadula [7; 8], utilizatorii pot crea conținut doar la propriul nivel sau mai sus de propriul nivel de securitate (adică utilizatorii ce au nivel de securitate „secret" pot crea fișiere „secret" sau „top-secret", dar nu pot să creeze fișiere publice; nu ca să fie înregistrate). În schimb, utilizatorii pot vizualiza conținut doar la nivelul lor sau sub nivelul lor de securitate (adică utilizatorii cu un nivel de securitate „secret" pot vizualiza fișiere publice sau secrete, dar este posibil să nu vizualizeze fișiere „top-secret"; nici măcar să le citească).

Stările sistemului

Au fost definite stările sistemului [8], astfel încât să reprezinte toate informațiile ce pot fi considerate necesare din punct de vedere al securității.

Tabelul 1.1. Elementele modelului Bell-LaPadula [8]

Mulțimi	Elemente	Semantică
S	$\{S_1,S_2,\bullet\ \bullet\ \bullet,S_n\}$	*subiecte*; procese, programe în execuție, utilizatori
O	$\{O_1,O_2,\bullet\bullet\bullet,O_m\}$	*obiecte;* date, fișiere, programe, subiecte
C	$\{C_1,C_2,\bullet\bullet\bullet,C_q\}$ $\{C_1 > C_2 > \bullet\bullet\bullet > C_q\}$	*clasificări*; nivelul de autorizare al unui subiect, clasificarea unui obiect
K	$\{K_1,K_2,\bullet\bullet\bullet, K_r\}$	*Categoria needs-to-know;* numărul proiectului, privilegiile de acces
A	$\{A_1,A_2,\bullet\bullet\bullet,A_p\}$	*atributele accesului*; citire, scriere, copiere, adăugare, proprietar, control
R	$\{R_1,R_2,\bullet\bullet\bullet,R_u\}$	*cerințe*; intrări, comenzi, cereri pentru acces la obiecte de către subiecte
D	$\{D_1,D_2,\bullet\bullet\bullet,D_v\}$	*decizii*; ieșiri, răspunsuri, „yes", „no", „error"
T	$\{1,2,\bullet\bullet\bullet,t,\bullet\bullet\bullet\}$	*indici*; elemente ale setului timp; identificarea momentelor discrete; un element t este un index la o secvență de cereri și decizii
$P\alpha$	Toate submulțimile ale α	*set de puteri al* α
α^{β}	toate funcțiile de la mulțimile *b* la mulțimile *a*	----------
$\alpha\times\beta$	$\{(a, b): a \in \alpha, b \in \beta\}$	*Produsul cartezian t al setului* α, *și* β
F	$C^S\times C^O\times(PK)^S\times(PK)^O$ un element arbitrar al lui F este scris sub forma $f = (f_1,f_2,f_3,f_4)$	*Clasificarea / vectorilor need-to-know*; f_1: funcția subiectul-clasificării f_2: funcția obiectul-clasificării f_3: funcția subiect-need-to-know f_4: funcția obiect-need-to-know
X	R^T un element arbitrar al lui X este scris x	*Secvențe de cereri*
Y	D^T un element arbitrar al lui Y este scris y	*Secvențe de decizii*
M	$\{M_1,M_2,\bullet\bullet\bullet, M_c\}$, $c = nm2^p$; un element M_k al lui M este o matrice $n \times m$ cu intrări de la PA; intrarea (i, j) a lui M_k arată atributele accesurilor $S_i's$ relative la O_j	*Matrici de acces*
V	$P(S\times O)\times M\times F$	*Stări*
Z	V^T un element al lui Z este scris z; $z_t \in z$ este starea cu numărul t în secvența de stări z	*Secvențe de stări*

O stare v este un tuplu de 3 elemente (b, M, F) unde

$B \in P(S\times O)$ indicând ce subiect are acces la care obiect în starea v; [8]

$M\in$ indicând intrările în matricea de acces în starea v;[8]

$f \in$ indicând nivelul de autorizare al tuturor obiectelor, nivelul de clasificare (grupare) al tuturor obiectelor, și „need-to-know” asociat cu toate subiectele și obiectele în starea ***v***.[8]

Relația stării de tranziție

Fie $W \subseteq R \times D \times V \times V$ Sistemul $\sum(R,D,W,z_0) \subseteq X \times Y \times Z$ este definit de $(x, y, z) \in \sum(R,D,W,z_0)$ dacă și numai dacă $(x_t, y_t, z_t, z_{t'-1}) \in W$ pentru oricare $t \in T$, unde z_0 este starea inițială normală a formatului (ϕ, M, fi) și ϕ reprezintă o mulțime vidă [8].

W a fost definită ca o relație dar poate fi gândită și ca o funcție. Atunci când se analizează probleme de proiectare, *W* va fi considerată o funcție, precizând următoarea stare și următoarea ieșire. *W* ar trebui să fie considerat în mod intuitiv ca întrunind normele de funcționare ale sistemului, cele care determină decizia sa pentru o cerere dată și trecerea în starea următoare.

Bell-LaPadula modelează starea sistemului ca fiind o stare exprimată printr-un cvadruplu de forma *(b, m, f, h)*, unde $b \subseteq B$ și, conține accesul curent permis utilizatorilor, $m \subseteq M$ este matricea actuală de control al accesului discreționar, $f = (f_s, f_o, f_c) \in F$ este funcția de nivel de securitate triplă, iar *h* este ierarhia obiectelor.

Modelul Bell-LaPadula susține că, dacă un sistem îndeplinește următoarele trei proprietăți, sistemul este sigur.

Proprietatea de simplă securitate $(s, o, p) \in S \times O \times P$ este satisfăcută [8] dacă și numai dacă se aplică una dintre următoarele două reguli:

- $p = e$ sau $p = a$
- $p = r$ sau $p = w$ și $f_o(o) \leq_d f_c(s)$

unde p e, r, a, w reprezintă:

- *p reprezintă tipul de acces;*
- tipul de acces *e* (nici observație, nici modificare- echivalent execuție);
- tipul de acces *r* (observarea fără modificări – echivalent citire);
- tipul de acces *a* (modificare fără observație – echivalent adăugare);
- tipul de acces *w* (atât observare, cât și modificare – echivalent scriere).

Simbolurile e, r, a și w sunt derivate din modurile de acces generalizate executare, citire, atașare și scriere și, de fapt, cuvintele subliniate sunt utilizate interschimbabil cu simbolurile cu litere mai scurte.

Proprietatea ***** - $\forall(s, o, p) \in S \times O \times P$ satisface proprietatea ***** dacă și numai dacă se respectă una dintre următoarele reguli:

$p = e$

$p = a$ și $f_c(s) \leq_d f_o(o)$

$p = w$ și $f_c(s) = f_o(o)$

$p = r$ și $f_o(o) \leq_d f_c(s)$

Proprietatea de securitate discreționară. O stare de sistem *(b, m, f, h)* satisface proprietatea de securitate discreționară dacă și numai dacă, $\forall (s, o, p) \in b, (s, o, p) \in m$. [8]

Concluzii despre modelul Bell-LaPadula

Controlul accesului formează fundamentul pentru o politică de securitate într-o organizație. Modelul Bell-LaPadula [7; 8] a fost unul dintre primele modele dezvoltate pentru a controla accesul la date într-un sistem informatic, prin garantarea confidențialității datelor. Există unele deficiențe la acest model: în cazul în care o organizație utilizează controlul accesului în mod exclusiv pentru a pune în aplicare normele de afaceri, nu va lua în considerare aspecte cum ar fi integritatea sau disponibilitatea. Următorul model, modelul Biba a fost creat pentru a trata deficitul din controlul integrității.

1.3. Modelul Biba

Întrucât modelul Bell LaPadula se axează pe controlul confidențialității în sistem, modelul Biba [9] a fost creat pentru a asigura integritatea și a fost unul dintre primele modele care au abordat, punerea în aplicare a integrității. Modelul Biba este format dintr-o familie de politici diferite, care pot fi folosite pentru a impune integritatea. Politicile care alcătuiesc gama de modele Biba sunt foarte restrictive

Modelul Bell-LaPadula [7; 8] este un model clasic care se bazează pe un sistem de clasificare în stil militar (Military Access Control - MAC) care are ca singur scop prevenirea scurgerii de informații, și de a nu permite celor ce nu sunt privilegiați de a accesa informațiile. Din punct de vedere al integrității datelor, el nu este perfect. Se poate ca un subiect clasificat la un nivel inferior de acces să scrie într-un obiect clasificat superior.

Însă modelul Biba la rândul său, se bazează puternic pe modelul Bell-LaPadula [9].

Modelul Biba folosește în locul termenului de clase de securitate pe cel de clase de integritate. Se bazează pe faptul că în multe cazuri confidențialitatea și integritatea sunt concepte duale: în timp ce prin confidențialitate se impun restricții celor ce pot citi un mesaj, prin integritate sunt controlați cei ce pot să scrie sau să modifice un mesaj.

Integritatea vizează trei scopuri principale:

- protejarea datelor împotriva modificărilor efectuate de utilizatorii neautorizați;
- protejarea datelor împotriva modificărilor neautorizate efectuate de utilizatori autorizați;

- asigurarea consistenței interne și externe a datelor.

La fel ca modelul Bell-LaPadula care operează cu niveluri diferite de sensibilitate, modelul Biba clasifică obiectele în diferite niveluri de integritate. Modelul enunță trei axiome ale integrității:

1. axioma integrității simple. Ea stabilește că unui subiect aflat pe un anumit nivel de integritate nu-i este permis să observe (citească) un obiect de o integritate mai joasă (No Read Down, Nu citi dedesubt).

2. axioma integrității * (stea) stabilește că unui obiect situat pe un anumit nivel de integritate nu-i este permis să modifice (scrie) alt obiect situat pe un nivel mai înalt de integritate (No Write Up, Nu scrie deasupra);

3. un subiect de pe un anumit nivel de integritate nu poate solicita un subiect situat pe un nivel de integritate superior.

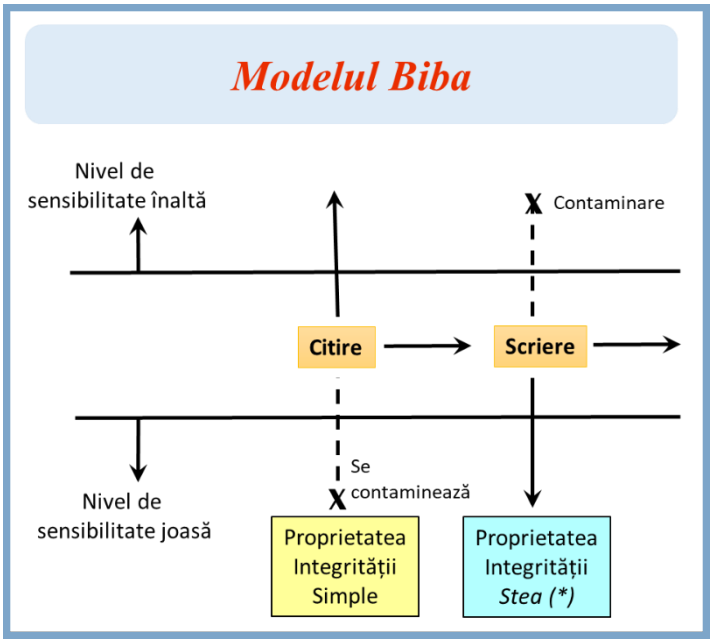


Figura 1.2. Modelul Biba cu cele trei principii

[Sursa: https://www.ktunotes.in/wp-content/ uploads/2019/05/PIS-M2-Ktunotes.in_.pdf]

1.3.1. Etichetele

În modelul Biba [9] fiecare subiect și obiect trebuie să posede o etichetă de integritate. Subiecții sunt componentele active în sistem, ca de exemplu procesele create de utilizatori, iar obiectele - entitățile protejate, de exemplu sistemul de fișiere. Etichetele nu oferă protecția datelor, ci sunt completate de un mecanism de securitate, în scopul de a oferi o protecție [61]. În mod obișnuit, la nivelul unei etichete, securitatea rămâne constantă, dar există și excepții de la această regulă. Unele dintre politicile modelului Biba susțin etichetele dinamice, ce permit niveluri de integritate variate, astfel că în modelul Biba se pot utiliza ambele etichete, statice și dinamice.

O etichetă de integritate are două părți: clasificarea și un set de categorii. Clasificarea de integritate constituie o mulțime organizată ierarhic. Un exemplu de clasificare ar putea fi „foarte importantă”, „importantă”, și „nesemnificativă”. „Foarte importantă” ar avea cel mai înalt nivel de clasificare și „nesemnificativă” ar avea cel mai scăzut nivel de clasificare. Numele pentru nivelul de clasificare poate fi corespunzător cerințelor de organizare a ierarhiei clasificărilor.

A doua parte a etichetei va consta dintr-un set de categorii, de asemenea, cunoscut ca un compartiment. Setul de categorii cuprinse în etichetă vor fi un subset al tuturor seturilor din sistem. Clasificarea setului de categorii este non-ierarhică.

Prezentăm un astfel de exemplu de categorii. Fie două categorii, X și Y care sunt formate după cum urmează:

categoria $X = \{Craiova, București, Cluj\}$;

categoria $Y = \{Craiova, Cluj\}$.

În acest caz, $X \geq Y$ *(X domină Y)*, pentru că *Y* este un subset al *X*.

În cazul în care există un compartiment care conține a treia categorie, $Z = \{Craiova, București, Brașov\}$, compartimentele *Z* și *X*, sunt non-comparabile, deoarece cel de-al treilea element din seturi diferă.

Fiecare nivel de integritate va fi reprezentat ca $L = (C, S)$, unde *L* este nivelul de integritate, *C* este clasificarea și *S* este un set al categoriei. Nivelurile de integritate formează apoi o relație de dominare. De exemplu, nivelul de integritate $L_1 = (C_1, S_1)$ domină ($\geq$) nivelul de integritate L_2, $L_2 = (C_2, S_2)$ dacă și numai dacă pentru această relație sunt satisfăcute condițiile:

1. $C_1 \geq C_2$
2. $S_1 \supseteq S_2$.

Etichetele de integritate se referă la gradul de încredere care poate fi avut față de datele utilizate [61]. Încrederea în datele introduse inițial nu creste, dar este posibil ca nivelul de integritate al unui obiect să scadă, dacă un set de date cu un nivel de integritate ridicat este transmis într-o rețea care are un nivel de integritate scăzut. În acest caz, încrederea în date nu va fi la fel ca înainte ca acestea să fi fost transmise în întreaga rețea. Nivelul de integritate al datelor ar putea fi redus ca urmare a acestui fapt. Datele din acest exemplu ar fi atunci reetichetate la un nivel inferior de clasificare. Modelul Biba are un număr redus de politici de marcare care pun în aplicare această etichetare dinamică.

În cazul unui sistem informatic în rețea, fiecare sistem din rețea trebuie să permită utilizarea de etichete de integritate. Dacă anumite sisteme din rețea nu acceptă etichetele de integritate, acolo are loc o pierdere a încrederii în integritatea datelor. Modurile de acces din modelul Biba sunt

formate din moduri de acces de grup și sunt similare cu cele utilizate în alte modele, deși poate folosi termeni diferiți pentru a le defini. Modurile de acces care aparțin modelului Biba sunt:

1. *Modificare*: permite unui subiect de a scrie într-un obiect. Acest mod este similar cu modul de scriere în alte modele.

2. *Observare:* permite unui subiect să citească un obiect. Este sinonim cu comanda de citire din alte modele.

3. *Invocare*: permite unui subiect de a comunica cu un alt subiect.

4. *Executare*: permite unui subiect să execute un obiect. Comanda în esență, permite unui subiect să execute un program care este obiectul.

Modelul Biba are două tipuri de politici:

1. obligatorii;
2. discreționare.

În cadrul acestor două tipuri de divizare, există o serie de politici care pot fi selectate în funcție de nevoile de securitate.

Politici obligatorii:

- Politica de strictă de integritate;
- Politica de limită inferioară pentru subiecți;
- Politica de limită inferioară pentru obiecte;
- Politica de audit al integrității de limită inferioară;
- Politica de inel.

Politici discreționare:

- Listele de control acces;
- Ierarhia obiectului;
- Inelul.

1.3.2. Politicile obligatorii Biba

Politica de integritate strictă este prima parte a modelului Biba [9]. Aceasta prevede:

Starea de integritate simplă: $s \in S$ poate observa $o \in O$, dacă și numai dacă $i(s) \leq i(o)$.[9]

Proprietatea de integritate stea *[9]:

$s \in S$ poate modifica $o \in O$, dacă și numai dacă $i(o) \leq i(s)$.

Invocarea proprietății:

$s_1 \in S$ poate invoca $\boldsymbol{s_2 \in S}$ dacă și numai dacă $i(s_2) \leq i(s_1)$.

Politica de integritate strictă este politica cea mai populară în modelul Biba. Prima parte a politicii este cunoscută sub numele de proprietatea integrității simple.

Proprietatea prevede faptul că un subiect poate observa un obiect doar dacă nivelul de integritate al subiectului este mai mic decât nivelul de integritate al obiectului.

A doua regulă este proprietatea integrității stea. Această proprietate prevede că un subiect poate scrie într-un obiect doar dacă nivelul de integritate al obiectului este mai mic sau a egal cu nivelul subiectului. Această regulă împiedică un subiect de a scrie într-un obiect ce are un nivel de încredere mai mare.

Ultima regulă este invocarea proprietății. *s* = proprietatea invocării și prevede faptul că un subiect s_1 invocă doar un alt subiect s_2, dacă s_2 are nivelul de integritate mai mic sau egal cu s_1.

Politica privind integritatea strictă impune:

„no write-up" („nu scrie sus"); - limitează daunele pe care pot face obiectele periculoase în sistem;

„no read down" („nu citi jos") - nu se pot introduce datele pentru un nivel de clasificare mai scăzut într-un de nivel de clasificare mai mare și, astfel să se propage informații nesigure sau inexacte.

Politica de integritate strictă este cea mai restrictivă dintre politicile care alcătuiesc modelului Biba, ea limitează citirea obiectelor de nivel inferior și poate fi prea restrictivă, în unele cazuri. Pentru a combate aceasta problemă, Biba a conceput o serie a politici de integritate dinamice, care ar permite subiecților de încredere accesul la obiectele sau subiectele de ne - încredere. Biba a implementat acestea într-un număr de politici diferite „low watermark"(limită inferioară).

Politica de „low-watermark" [9] pentru subiecți, este a doua parte a modelului Biba. Politica prevede:

1. proprietatea integritate stea;
2. $s \in S$ poate modifica $o \in O$, dacă și numai dacă $i(o) \leq i(s)$;
3. Dacă $s \in S$ examinează $o \in O$, $i''(s) = min\ (i(s), i(o))$, unde $\boldsymbol{i''(s)}$ este nivelul de integritate al subiecților după citire;
4. Proprietatea invocare: $s_1 \in S$ poate invoca $s_2 \in S$ dacă și numai dacă $i(s_2) \leq i(s_1)$.

Politica de „low-watermark" pentru subiecți reduce nivelul de integritate al subiectului la cel mai scăzut nivel de integritate al subiectului și al obiectului implicat. Prima regula a acestei politici este proprietatea de integritate stea care impune „nu scrie". Acest lucru previne modificarea obiectelor mai de încredere. A doua regulă a politicii afirmă că, dacă acțiunea unui subiect este

citirea unui obiect de mai mică încredere, nivelul său de integritate, al subiectului, va scădea cu cel al obiectului. Acest lucru previne ca un obiect să contamineze un subiect, deoarece nivelul integritate al subiectului sau al subiecților va fi redus la cel al obiectului.

Politica de „low-watermark" pentru subiecți este o politică dinamică, deoarece aceasta scade nivelul de integritate al unui subiect pe baza observațiilor obiectelor. Această politică face ca în cazul în care un subiect observă un obiect de integritate mai mică, va scădea nivelul integrității subiectului. Apoi, în cazul în care subiectul trebuie să observe în mod legitim un alt obiect ce nu are nivelul de integritate scăzut nu poate fi în măsură să facă acest lucru, deoarece nivelul de integritate al subiectului a fost redus ceea ce va putea duce la o negare a serviciului (Denial of service).

Politica de „low-watermark" (limită inferioară) pentru obiecte este a treia parte a modelului Biba. Această politică este similară cu politica de „low-watermark" pentru subiecți.

Aceasta prevede:

1. $s \in S$ poate modifica orice $o \in O$, indiferent de nivelul de integritate;
2. Dacă $s \in S$ observă $o \in O$ $i''(o) = min\ (i(), i''(o))$, *unde* $i''(o)$ este nivelul integrității obiectelor după ce acesta este modificat.

Această politică permite oricărui subiect să modifice orice obiect. Nivelul de integritate al obiectelor este coborât în cazul în care nivelul integrității subiectului este mai mic decât nivelul obiectelor. Politica este, de asemenea dinamică, deoarece nivelurile integrității obiectelor din sistem sunt modificate pe baza a ceea ce modifică subiecții. Ea nu protejează obiectul de subiect, astfel ca un subiect de neîncredere să modifice un obiect de încredere, nu oferă nici o protecție reală într-un sistem, și scade încrederea acordată obiectelor. Prin urmare se poate ca în scurt timp sistemul să fie populat de obiecte de neîncredere.

Politica de audit al integrității „low-watermark" este a patra politică obligatorie în conformitate cu modelul Biba.

Această politică prevede:

1. $s \in S$ poate modifica orice $o \in O$, indiferent de nivelurile de integritate;
2. Dacă un subiect modifică un obiect de nivel mai mare tranzacția este înregistrată într-un jurnal de audit.

În concluzie, această politică este similară cu politica de „low-watermark" pentru obiecte, în sensul că nu face nimic pentru a preveni modificarea necorespunzătoare a unui obiect. Ea înregistrează pur și simplu faptul că o modificare necorespunzătoare a avut loc. Înregistrările din jurnalul de audit trebuie să fie apoi examinate pentru a determina cauza modificării necorespunzătoare.

Politica „ring” („inel”) este ultima politică obligatorie în modelul Biba.

Această politică nu este dinamică, așa cum sunt primele trei politici. Etichetele de integritate folosite pentru politica inel sunt fixate, similar cu cele din politica privind integritatea strictă. Politica ring prevede:

1. Orice subiect poate observa orice obiect, indiferent de nivelurile integrității;
2. Proprietatea integritate stea $s \in S$ poate modifica $o \in O$, dacă și numai dacă $i(o) \leq i(s)$;
3. Proprietatea invocare $s_1 \in S$ poate invoca $s_2 \in S$ dacă și numai dacă $i(s_2) \leq i(s_1)$.

Politica inel permite oricărui subiect de a observa orice obiect.

Politica se referă numai la modificarea directă. Un subiect poate scrie într-un obiect numai în cazul în care nivelul integrității obiectului este mai mic sau egal cu nivelul integrității subiectului, ceea ce este proprietatea integrității stea.

Ultima parte a politicii „inel” este proprietatea invocării.

Politica „inel” nu este perfectă, ea permite modificări improprii. Un subiect poate citi un obiect de nivel scăzut, și apoi modifica datele observate la nivelul integrității sale [9]. Un exemplu în acest sens ar fi, un utilizator citind un obiect de mai mică de încredere, își amintește apoi datele pe care le citește și apoi, mai târziu, scrie datele într-un obiect de la nivelul lui de integritate. Politica inel permite o modificare indirectă a datelor de încredere.

1.3.3. Politici discreționare Biba

Modelul Biba [9] are un și un număr de politici discreționare. Un prim exemplu de politică discreționară este o listă de control al accesului, care determină ce subiecți pe care obiecte le pot accesa. Lista de control de acces poate fi modificată de subiecții cu privilegii corecte. În al doilea rând, integritatea poate fi executată prin utilizarea ierarhiei unui obiect. În această metodă, există o rădăcină și obiecte care sunt urmași ai rădăcinii. Pentru a accesa un anumit obiect, subiectul trebuie să observe privilegiile pentru acele obiecte și toate celelalte obiecte de pe toată calea până la rădăcină. O altă politică discreționară este politica inel, care are niște numere de inele, iar în sistem, numărul cel mai mic fiind cel mai mare privilegiu. Modurile de acces ale subiectului trebuie să se încadreze într-un anumit interval de valori pentru a permite să acceseze un obiect.

1.4. Modelul Clark-Wilson

Wilson și Clark [74] au fost printre cei care au constatat că cercetările privind modelele de control al accesului au accentuat mai mult confidențialitatea datelor, decât integritatea acestora (adică, accesarea-vizualizarea neautorizată decât modificarea neautorizată). În consecință, au

propus un model care să redreseze ceea ce vedeau ca fiind dintr-o perspectivă militară care se deosebea semnificativ de cea comercială.

Modelul Clark-Wilson este format dintr-un triplet subiect, obiect și reguli despre date [74].

Toate modelele formale de control de acces care preced modelul Clark-Wilson tratează o pereche subiect / obiect ordonată - adică un utilizator și un articol sau o colecție de date, cu privire la o relație fixă (de exemplu, citire sau scriere) între cei doi. În modelul Clark- Wilson s-a arătat că relația poate fi pusă în aplicare printr-un program arbitrar. În consecință, ei tratează un subiect/program/obiect ordonat. Se folosește termenul „procedură de transformare" pentru program pentru a confirma că programul are relevanță pentru integritate, deoarece modifică sau transformă datele în conformitate cu o regulă sau o procedură. Datele pe care procedurile de transformare le modifică se numesc elemente de date restricționate, deoarece numai procedurile de transformare le pot modifica și procedurile de verificare a integrității exercită constrângeri asupra acestora pentru a se asigura că au anumite proprietăți, dintre care consistența și conformitatea cu lumea reală sunt două dintre cele mai semnificative. Elementele de date nerestricționate sunt toate celelalte date, în principal, cheia de intrare a procedurilor de transformare.

Un subiect a fost constrâns astfel încât poate avea acces la obiecte numai prin procedurile de transformare specificate, iar procedurile de transformare au orice logică necesară pentru limitarea privilegiului și separarea îndatoririlor. Procedurile de transformare (programele) pot controla accesul subiecților la obiecte la un nivel de granularitate mult mai fin decât cel disponibil în sistem. De exemplu, ei pot exercita controale mai fine (rezonabilitate și verificări de consecvență asupra articolelor de date nerestricționate) pentru scopuri precum evidența contabilă cu dublă intrare, asigurându-se astfel că orice este scăzut dintr-un cont este adăugat la altul, astfel încât activele să fie conservate în tranzacții.

1.5. Modelul RBAC

În 1992, David Feraiollo și Richard Kuhn au prezentat în cadrul „15th National Computer Security Conference" un concept nou de control al accesului și acțiunilor utilizatorilor, RBAC (Role-Based Access Control) [31; 32].

Acest concept pleacă de la premisa că utilizatorii nu sunt „proprietarii" informațiilor, pentru care au un permis de acces. Organizațiile sunt proprietarii reali ai obiectelor din sistem și a programelor care le procesează. Controlul accesului se bazează adesea pe funcțiile angajaților care joacă diferite roluri în organizație, mai degrabă decât pe proprietatea datelor. Prin urmare, controlul accesului este determinat adesea de rolul utilizatorilor individuali luați ca parte a

organizației. Aceasta include specificarea atribuțiilor, responsabilităților, precum și calificările necesare pentru rolul respectiv. În literatura de specialitate, frecvent este prezentat exemplul rolurilor din cadrul unui spital. Aceasta poate presupune că rolul de medic, asistent medical, farmacist, etc. Sau, într-o bancă, rolurile pot fi de: casier, analist de credite, analist financiar, ofițer front office, contabil, etc. Rolurile se pot, de asemenea, aplica sistemelor militare.

O politică de control al accesului bazată pe roluri (RBAC) își bazează deciziile de control al accesului pe funcțiile unui utilizator și pe ceea ce îi este a permis să efectueze în cadrul unei organizații. Utilizatorii nu pot transmite permisiunile de acces pentru alți utilizatori, la alegerea lor, pentru că nu ei sunt responsabili de administrarea politicilor. Pentru administrarea lor, este necesar un administrator de securitate care este responsabil pentru aplicarea politicii și reprezintă organizația. Acesta nu poate lua decizii discreționare, ci în conformitate cu cerințele de securitate specifice ale organizației. Aceste cerințe sunt transformate în politici ce trebuie să răspundă legislației existente, eticii, regulamentelor interne, sau practicilor general acceptate. Aceste politici sunt aplicate în mod inevitabil asupra tuturor utilizatorilor, deci sunt non-discreționare. De exemplu, într-un spital, un medic are dreptul de a prescrie tratamente, dar nu are autoritatea de a transmite această operațiune unei asistente medicale, care nu poate stabili un diagnostic.

RBAC reprezintă un mijloc de a restricționa accesul la obiecte, obiecte ce au informații sensibile (sensibilitatea lor este reprezentată de o etichetă) și de autorizare a subiecților pentru a accesa informațiile ce au o asemenea sensibilitate [32].

Un rol poate fi considerat ca un set de tranzacții pe care un utilizator sau un grup de utilizatori le poate efectua în cadrul unei organizații. Rolurile sunt orientate pe grup. Pentru fiecare grup, este alocat și menținut un set de tranzacții. O tranzacție poate fi gândită ca o procedură de prelucrare (un program sau o parte a unui program, a unui set de date). În plus, fiecare rol are un set asociat de membri individuali (Figura 1.3). Ca urmare, RBAC oferă un mijloc de a numi și a descrie relații „mulți-la-mulți” între persoane fizice și drepturile lor. În Figura 1.3 sunt descrise relațiile dintre utilizatorii individuali, grupuri/roluri, procedurile de transformare și obiectele din sistem.

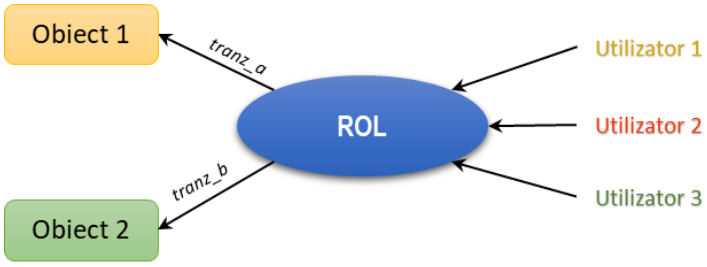


Figura 1.3. Relațiile din cadrul RBAC –[31]

1.5.1. Descrierea formală a RBAC

Descrierea simplă formală, în termeni de seturi de relații și de control al accesului de bază este prezentată în cele ce urmează.

Pentru fiecare subiect **s**, rolul activ este cel pe care subiectul îl folosește în prezent:

AR (s: subiect) = {rolul activ pentru subiectul s}.

Fiecare subiect poate fi autorizat să efectueze unul sau mai multe roluri:

RA (s: subiect) = {roluri autorizate pentru subiectul s}.

Fiecare rol poate fi autorizat să efectueze una sau mai multe tranzacții:

TA (r: rol) = {tranzacțiile autorizate pentru rolul r}.

Subiectele pot efectua tranzacții. Predicatul *exec (s, t)* este adevărat dacă subiectul poate executa tranzacția *t* la momentul curent, altfel este fals:

exec (s: subiect, t: tran) = true dacă și numai dacă obiectul **s** poate executa tranzacția *t*.

Trei reguli de bază sunt necesare:

1. Atribuirea de rol. Un subiect poate executa o tranzacție doar în cazul în care subiectul a ales sau i-a fost atribuit un rol.

$\forall s: subiect, t: tran, (exec (s, t) \Rightarrow AR (s) \neq \varnothing$

Identificarea și procesul de autentificare (de exemplu conectarea), nu sunt considerate tranzacții. Toate celelalte activități ale utilizatorului în sistem sunt efectuate prin intermediul tranzacțiilor. Astfel, toți utilizatorii activi sunt obligați să aibă un rol activ.

2. Autorizația de rol. Rolul unui subiect activ trebuie să fie autorizat pentru subiect.

$\forall s: subiect, (AR (e) \subseteq RA (s)).$

Împreună cu regula 1, această regulă se asigură că utilizatorii pot avea numai roluri pentru care au autorizație.

3. Autorizarea tranzacției. Un subiect poate executa o tranzacție doar în cazul în care tranzacția este autorizată pentru rolul subiectului activ.

$\forall s: subiect, t: tran, (exec (s, t) \Rightarrow t \in TA (AR (s))).$

Regulile (1) și (2) ne asigură că utilizatorii pot executa doar operațiunile pentru care au autorizație. Reținem că, deoarece este condiționată „numai dacă”, această regulă permite posibilitatea de a introduce restricții suplimentare în executarea tranzacției. Aceasta înseamnă că regula nu garantează ca o tranzacție să fie executabilă doar pentru că este în *TA (AR (s))*, adică setul de tranzacții potențial executabile de rolul subiectului activ. De exemplu, unui stagiar pentru

rolul de supraveghere îi poate fi atribuit rolul de „Supervizor”, dar s-au aplicat restricții la rolul de utilizator al lui, care limitează tranzacțiile accesibile la un subset față de cei care în mod normal au rolul de Supervisor

Mai sus, o tranzacție a fost definită ca o procedura de transformare, plus un set de elemente ale datelor accesate prin procedura de transformare. Controlul accesului, în regulile de mai sus, nu are nevoie de verificări privind dreptul utilizatorului de a accesa un obiect de date, sau cu privire la procedura de transformare; este dreptul de a accesa un element de date, deoarece căile de acces ale datelor sunt construite în tranzacție.

O altă utilizare a RBAC este sprijinirea integrității. Integritatea a fost definită într-o varietate de moduri, dar un aspect al integrității este o cerință în care datele și procesele pot fi modificate numai în moduri „autorizație” de către utilizatorii autorizați. Acest lucru pare a fi un obiectiv rezonabil al securității pentru multe sisteme reale, și RBAC ar trebui să fie aplicabil în astfel de sisteme.

În general, problema de a stabili dacă datele au fost modificate numai în moduri „autorizație” poate fi la fel de complexă ca și tranzacția care a făcut modificarea. Din acest motiv, abordarea practică este ca tranzacțiile să fie certificate și de încredere. În cazul în care tranzacțiile trebuie să fie de încredere, controlul accesului poate fi încorporat direct în fiecare tranzacție. Cerința sistemului de a controla accesul programelor de tranzacție la obiecte prin intermediul funcției de acces, utilizând regulile necesare, ar putea fi o formă utilă de redundanță, dar s-ar putea implica depășiri semnificative pentru un beneficiu limitat în aplicarea cerințelor de integritate. Prin urmare, includerea unei tranzacții ca funcție de control al accesului la obiect în RBAC, ar fi utilă în unele aplicații, dar nu în toate.

1.5.2. Administrarea centralizată a securității prin intermediul RBAC

RBAC este flexibil, prin faptul că acesta poate avea caracteristicile organizaționale în termeni de politici și de structură. Una dintre cele mai mari virtuți ale RBAC este capacitatea administrativă pe care acesta o acceptă.

Odată ce tranzacțiile unui rol sunt stabilite în cadrul unui sistem, aceste operațiuni tind să rămână relativ constante sau se schimbă încet de-a lungul timpului. Sarcina administrativă constă în acordarea și retragerea apartenenței la un set de roluri specifice, numite în cadrul sistemului. Atunci când o persoană nouă intră în organizație, administratorul îi acordă pur și simplu o calitate de membru la un rol existent. Schimbările funcției unei persoane în cadrul organizației presupun schimbarea calității de membru a utilizatorului și a rolurilor sale existente, care pot fi cu ușurință șterse și acordate altele noi. În cele din urmă, atunci când o persoană părăsește organizația, toate

apartenențele la toate rolurile se elimină. Pentru o organizație care prezintă o cifră mare de personal, o politică a securității bazată pe roluri, este singura alegere logică.

În plus, rolurile pot fi compuse din alte roluri. De exemplu, un terapeut într-un spital poate fi compus din roluri terapeut, stagiar, și medic. Figura 1.4 prezintă de exemplu o astfel de relație.

Prin acordarea apartenenței la rolul de medic se presupune accesul la toate operațiunile definite de terapeut și stagiar, precum și cele de medic. Pe de altă parte, prin acordarea apartenenței la rolul de stagiar, acest lucru implică tranzacții de stagiar și terapeut, nu de medic. Cu toate acestea, prin acordarea apartenenței la rolul terapeut, aceasta permite numai accesul la aceste resurse permise în conformitate cu rolul de terapeut.

Principiul privilegiului minim

Principiul de cel mai mic privilegiu a fost descris ca fiind important pentru îndeplinirea obiectivelor integrității Principiul de cel mai mic privilegiu impune ca unui utilizator să i se acorde privilegiul care este minimum necesar pentru a efectua un job.

Asigurând cel mai mic privilegiul pe locuri de muncă ce necesită identificarea utilizatorului reprezintă determinarea setului minim de privilegii necesare pentru a efectua acest job, precum și limitarea utilizatorului la un domeniu cu aceste privilegii și nimic mai mult. Prin refuzul de a permite subiecților accesul la tranzacțiile care nu sunt necesare pentru îndeplinirea sarcinilor lor, refuzarea acestor privilegii nu poate fi folosită la eludarea politicii de securitate organizaționale. Prin utilizarea RBAC, impunerea privilegiilor minime poate fi ușor de realizat pentru utilizatorii de sisteme generale.

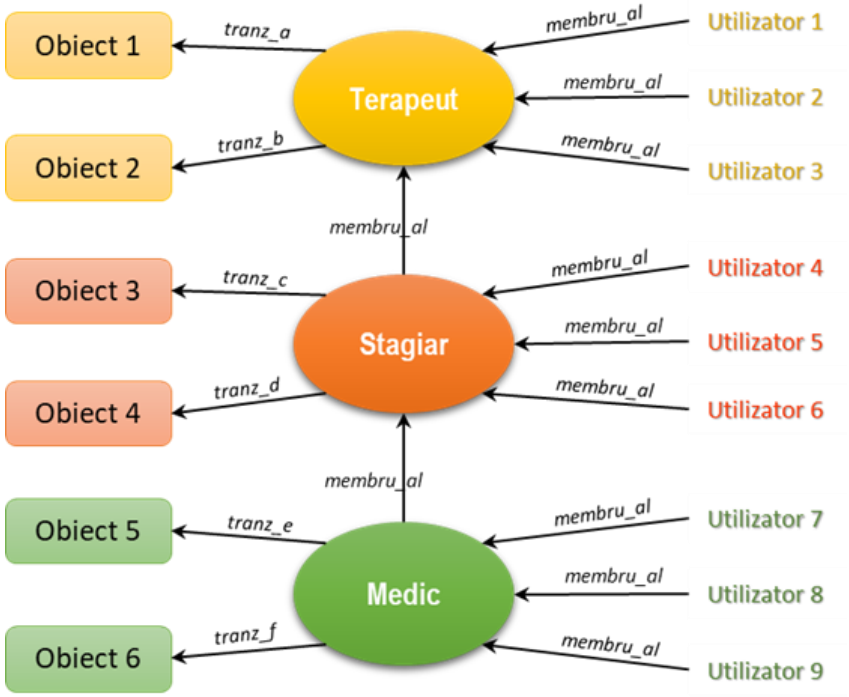


Figura 1.4. Relațiile dintre roluri în RBAC- [31]

Separarea sarcinilor

Mecanismele RBAC pot fi utilizate de către un administrator de sistem în aplicarea unei politici de separare a sarcinilor. Separarea sarcinilor este considerată valoroasă în descurajarea fraudei, deoarece frauda poate apărea în cazul în care există o oportunitate de colaborare între facilitățile oferite de diferite joburi. Separarea de sarcini prevede că, pentru seturi de tranzacții, nici unui individ unic să nu i se permită să execute toate tranzacțiile în cadrul setului. Exemplele cele mai frecvent utilizate sunt tranzacțiile separate necesare pentru a iniția o plată și autorizarea ei. Nici un singur individ n-ar trebui să fie în măsură să execute ambele tranzacții. Separarea de sarcini este un element important în sistemele reale. Seturile în cauză vor varia în funcție de aplicație. În situații reale, doar anumite tranzacții trebuie să fie restricționate în conformitate cu separarea cerințelor de serviciu. De exemplu, ne-am aștepta ca o tranzacție pentru „autorizarea plății" să fie limitată, dar o tranzacție „transmite sugestia către administrator" să nu fie.

Separarea a sarcinilor poate fi statică sau dinamică. Conformitatea cu cerințele de separare statice pot fi determinată pur și simplu de repartizarea de roluri persoanelor fizice și alocarea de roluri tranzacțiilor. Cazul cel mai dificil este separarea dinamică a sarcinilor în cazul în care respectarea cerințelor poate fi determinată numai în timpul funcționării sistemului. Obiectivul din spatele separării dinamice a sarcinii este de a permite o mai mare flexibilitate în operațiuni. Luăm în considerare cazul de inițiere și de autorizare a plăților. O politică statică ar putea cere ca nici un individ, care poate servi în calitate de inițiator al plății nu ar putea servi, de asemenea, ca și ordonator al plății. Acest lucru ar putea fi pus în aplicare asigurându-ne că nici unul care poate efectua rolul de inițiator nu ar putea efectua, de asemenea, rolul de ordonator. O astfel de politică poate fi prea rigidă pentru uz comercial, făcând costul de securitate mai mare decât pierderea care ar fi rezultat, fără securitate. Mai multă flexibilitate ar putea să fie permisă printr-o politică dinamică, care permite aceluiași individ să aibă ambele roluri - inițiator și ordonator-, cu excepția faptului că nimeni nu ar putea autoriza plățile pe care el sau ea le-a inițiat. Politica statică ar putea fi pusă în aplicare prin controlul rolurilor, doar de utilizatori, pentru cazul dinamic, sistemul trebuind să folosească atât rolul cât și ID-ul de utilizator în verificarea accesului la tranzacții.

1.6. Controlul accesului bazat pe atribute - ABAC

În 2014, NIST, a publicat „Guide to Attribute Based Access Control (ABAC) Definition and Considerations" [40]. Noul standard [33; 40] înlocuiește RBAC, și presupune o creștere a controlului accesului în sistemele informatice**:** o metodă de control de acces în care subiectul solicită să efectueze operațiuni pe obiecte este acordat sau refuzat pe baza atributelor atribuite ale

subiectului, atribute atribuite obiectului, condiții de mediu și un set de politici specificate în termenii acelor atribute și condiții

Controlul accesului bazat pe atribute - ABAC [17; 33; 40] este o metodă de control de acces în care subiectul solicită să efectueze operațiuni pe obiecte este acordat sau refuzat pe baza atributelor atribuite ale subiectului, atribute atribuite obiectului, condiții de mediu și un set de politici specificate în termenii acelor atribute și condiții

ABAC are câteva componente principale care sunt descrise mai jos.

Atributul – care reprezintă o caracteristică a oricărui element din rețea, și poate defini:

- O caracteristică a utilizatorului - poziția acestuia, locul de muncă, adresa IP, sarcinile, etc.;
- O caracteristică a obiectului - tip, sensibilitatea, nivelul necesar de pregătire etc.;
- Un tip de acțiune - citire, scriere, editare, copiere, etc.;
- O caracteristică a mediului - ora, ziua săptămânii, locația etc.

Subiectul - orice utilizator sau resursă care poate efectua acțiuni în rețea; unui subiect i se atribuie atribute pentru a-i defini nivelul de acțiune

Obiectul - orice tip de dată stocată în rețea; obiectelor li se atribuie atribute pentru a le descrie și identifica

Operația - orice acțiune întreprinsă de orice subiect din rețea

Politica - un set de reguli care permit sau restricționează orice acțiune. de prelucrare a datelor; regulile sunt declarații „IF / THEN” bazate pe atribute ale oricărui element (utilizator, resursă, mediu)

Spre deosebire de RBAC, în ABAC se pot folosi chiar și atribute care nu sunt încă înregistrate în sistem, dar care vor apărea în timpul procesului de lucru.

Implementarea ABAC are patru componente importante [33; 40]:

- Punctul de aplicare a politicii (Policy Enforcement Point-PEP), responsabil pentru protejarea aplicației;
- Punct de decizie politică (Policy Decision Point - PDP),responsabil cu procesarea cererii primite și evaluarea în conformitate cu politicile de autorizare cu care a fost configurat;
- Punctul de informare a politicii (Policy Information Point -PIP), este driverul care conectează PDP la sursele subiacente de atribute;

- Punctul de administrare a politicilor (Policy Administration Point -PAP) și este instrumentul prin care administratorii creează, gestionează și editează politicile de autorizare.

ABAC standardizează modul de interogare a autorizației. ABAC [17] se reduce la un răspuns simplu „Da” sau „Nu”. Acest lucru se aplică oricât de complicată este întrebarea. Simplitatea procesului de cerere / răspuns facilitează integrarea cu diferite aplicații și cadre.

ABAC permite, de asemenea, să fie și fluxuri de răspuns mai bogate[17]. Deși răspunsul este întotdeauna în termeni de răspuns la o întrebare prin Da / Nu, decizia poate fi mărită cu declarații suplimentare, cum ar fi:

- Da, permiteți + înregistrați faptul că utilizatorul a primit acces;
  sau
- Nu, refuză + redirecționează utilizatorul la o pagină de autentificare cu doi factori.

Politicile de tip ABAC se pot aplica împreună cu politicile RBAC, crescând gradul de control al accesului al utilizatorilor.

1.7. Limbajul EPAL pentru definirea politicilor de confidențialitate

Limbajul de autorizare a confidențialității întreprinderii (EPAL) [4], dezvoltat de IBM [4], permite unei întreprinderi să formalizeze politica de confidențialitate care trebuie aplicată în cadrul întreprinderii. Aceasta formalizează promisiunile de confidențialitate în politici și asociază o politică consimțită fiecărei date colectate. Această politică consimțită poate fi apoi utilizată în deciziile de control al accesului pentru a pune în aplicare promisiunile de confidențialitate făcute. Limbajul de politici EPAL clasifică datele pe care le deține o întreprindere și regulile care guvernează utilizarea datelor din fiecare categorie. O politică EPAL este în esență un set de reguli de confidențialitate. O regulă este o declarație care include un utilizator de date, o acțiune, o categorie de date și un scop. O regulă poate conține, de asemenea, condiții și obligații.

Obiectivele limbajului EPAL sunt următoarele:

- Să aibă capacitatea de a codifica politicile și procedeele de prelucrare a datelor, legate de confidențialitate;
- Să fie un limbaj care să poată fi importat și impus de sistemele de impunere a confidențialității.

EPAL își propune să formalizeze politicile de confidențialitate interne ale întreprinderii. Acest lucru necesită un vocabular care să formalizeze aspectele relevante pentru confidențialitate ale unei întreprinderi. De asemenea, include o ierarhie a scopurilor pentru care întreprinderea

colectează date. EPAL, este conceput special pentru a exprima o politică internă de confidențialitate care poate fi aplicată de un sistem de gestionare a confidențialității întreprinderii.

O politică EPAL clasifică datele deținute de o organizație și regulile care administrează utilizarea fiecărei categorii de date. Datorită faptului că EPAL este creat pentru a captura politicile de confidențialitate în mai multe arii de responsabilitate, limbajul nu poate predefini elementele politicii de confidențialitate. Așadar, EPAL pune la dispoziție un mecanism pentru definirea elementelor care sunt utilizate pentru construirea politicii. O politică EPAL este, în primul rând, un set de reguli de confidențialitate.

O regulă este un enunț care conține o decizie, un utilizator de date, o acțiune, o categorie de date și un scop.

O regulă poate de asemenea conține condiții și obligații.

Obiectivele EPAL (și non-obiectivele) sunt următoarele:

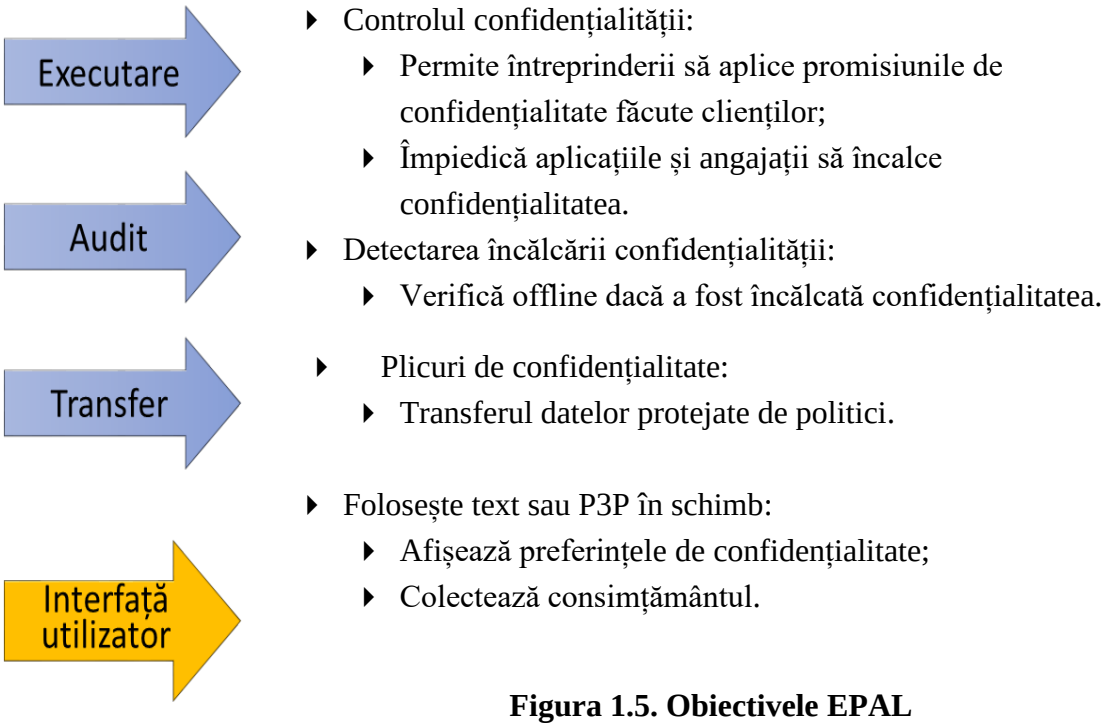


Figura 1.5. Obiectivele EPAL
[Sursa:https://yuwang.gitbooks.io/data-protection/content/privacy-aware_access_control_part_1.html]

Regulile dintr-o politică sunt ordonate după prioritate. Regulile care au întâietate în mod necondiționat sunt luate în considerare înaintea celor cu o prioritate mai scăzută. De exemplu, o organizație ar putea avea următoarea regulă în politica sa de confidențialitate:

Regulile sunt utilizate pentru a determina dacă o cerere este permisă sau refuzată. O cerere conține un utilizator de date, o acțiune, o categorie de date și un scop. Continuând cu aceeași organizație de mai sus, se consideră următoarea cerere:

Tabelul 1.2. Regulile dintr-o politică de confidențialitate-[20]

politica de confidențialitate (informal)	Permite unui agent de vânzări sau unui supervizor de vânzări să colecteze datele utilizatorului pentru înregistrarea comenzii dacă cumpărătorul a depășit vârsta de 13 ani și a fost notificat în legătură cu politica de confidențialitate. Șterge datele după 3 ani.
decizie	permite
utilizator de date	departamentul de vânzări
acțiune	depozitare
categorie de date	evidența cumpărătorilor
scop	procesarea comenzilor
condiție	cumpărătorul a depășit vârsta de 13 ani
obligație	șterge datele după 3 ani

Regula de mai sus acceptă cererea, deci agentului de vânzări îi este permis să depoziteze informațiile de contact ale utilizatorului. Reguli adiționale pot stabili apoi modul în care pot fi folosite datele depozitate.

Tabelul 1.3. Exemplu de regulă dintr-o politică de confidențialitate - [20]

cerere (informal)	O persoană comportându-se ca un agent de vânzări și un angajat cer sa colecteze email-ul unui cumpărător pentru înregistrarea comenzii.
utilizator de date	departamentul de vânzări
acțiune	depozitare
categorie de date	evidența cumpărătorilor
scop	procesarea comenzilor

Specificația politicii de confidențialitate EPAL

Politicile de confidențialitate specifică:

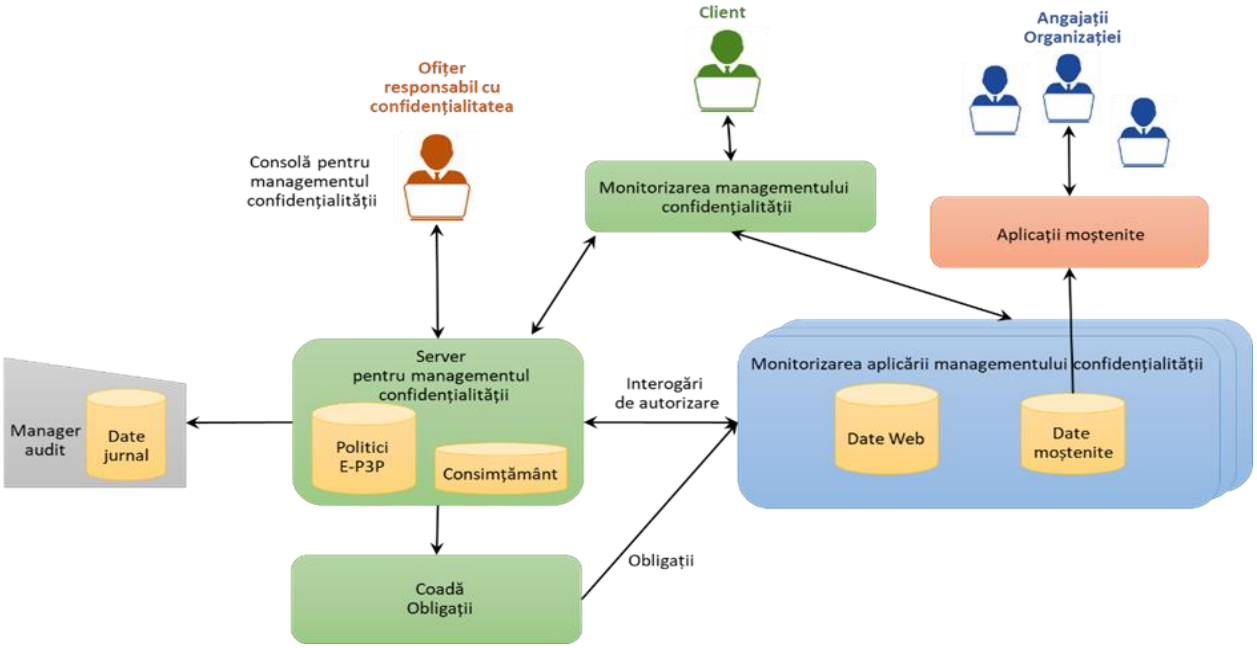


Figura 1.6. Arhitectura unei politici EPAL
[Sursa: https://yuwang.gitbooks.io/data-protection/content/privacy-aware_access_control_part_1.html]

- Cine: identități sau roluri ale utilizatorilor;
- Ce: resurse sau date;
- Cum: acțiuni;
- De ce: motivul pentru care sunt prelucrate datele;
- Condiții: în care se acordă / refuză accesul;
- Datele sunt transmise împreună cu politica care reglementează accesul la acestea;
- EPAL definește terminologia politicii și regulile de autorizare;
- Regulile permit / refuză acțiunile relevante privind confidențialitatea, în funcție de scop;
- Obligații: cerințe obligatorii care trebuie îndeplinite.

1.8. Limbajul XACML (eXtensible Access Control Markup Language)

Limbajul extensibil de marcare XML este standardul pentru descrierea informației structurate și a conținutului pe Internet. Este bine cunoscut care sunt beneficiile utilizării XML ca și container de informație: simplitatea lui, bogăția structurii de informații și o excelentă manipulare a caracterelor internaționale.

Când XML devine un format codificat larg răspândit pentru aplicațiile Web, informațiile trebuie să fie protejate de amenințările posibile atâta timp cât există informații confidențiale sau sunt cerute actualizări pentru probe de nerepudiere.

Asemănător cu limbajele de politică existente, XACML [49] este folosit pentru a specifica o politică orientată obiect-subiect-acțiune-condiție în contextul unui document particular XML. Noțiunea de subiect cuprinde identitate, grup, și rol. Granularitatea unui obiect este la fel de fină precum fiecare element în parte din cadrul fișierului de date. În mod curent, există patru acțiuni posibile: citire, scriere, creare și ștergere.

XACML se sprijină pe un model de autorizare provizoriu, unde poate fi specificată o acțiune provizorie asociată cu o acțiune primitivă (citire, scriere, creare, sau ștergere).

Aproape toate studiile în sistemele de autorizare și control al accesului au presupus următorul model:" Un utilizator face o cerere pentru a accesa un sistem într-un context, și sistemul ori autorizează cererea de acces ori o respinge." În modelul de autorizare provizorie, răspunsul de la sistem nu este pur și simplu „permis" sau „respins" El spune utilizatorului că cererea sa va fi autorizată și sistemul necesită câteva acțiuni sau că cererea sa este respinsă dar sistemul totuși trebuie să execute câteva acțiuni. Astfel de acțiuni se numesc acțiuni provizorii. Exemple de acțiunii provizorii includ: controlul, verificarea de semnătură digitală, codificarea și transformările XSL precum și acțiunile de scriere, creare și ștergere. Aceste acțiuni provizorii ne permit să specificăm politici cum ar fi:

1. Un utilizator este autorizat să acceseze o informație confidențială, dar accesul trebuie să fie jurnalizat;

2. Un utilizator este autorizat să citească o informație sensibilă, dar mai întâi trebuie îndeplinite niște termene și condiții;

3. Dacă este detectat un acces neautorizat, trebuie să se expedieze un mesaj de alarmă la un administrator.

În mecanismele existente de control al accesului, toate acțiunile provizorii sunt codificate în aplicații, dar în sistemul de autorizare provizoriu, ele pot să fie prelucrate de către modulul de impunere a politici, dar nu de aplicații.

Modelele anterioare de autorizare au presupus că sistemul ori autorizează cererea de acces, ori o respinge.

Cercetări recente au ca scop furnizarea unui cadru general care este capabil să susțină politici de control de acces multiplu și flexibil, ca de exemplu o politică de suprascriere sub-subiect și o politică de suprascriere de cale.

Toate aceste modele, presupun fie că sistemul autorizează cererea fie că o respinge. Modelul de autorizare provizorie permite sistemului de autorizare să întoarcă mai multe decizii de acces mult mai flexibile, prin includerea ideii de acțiune provizorie în semantica de autorizare tradițională. XACL este primul limbaj pentru controlul accesului bazat pe XML, pentru modelul de autorizare provizoriu.

Figura 1.7 arată arhitectura sistemului de autorizare provizorie. Avem două module principale:

- un modul de evaluare a accesului;
- un modul de executare a cererilor.

Fie o cerere de acces dată care să execute o acțiune pentru un document țintat XML; politica asociată (scrisă în XACL) este impusă după cum urmează:

Pasul 1: Un inițiator trimite o cerere de acces incluzând un element țintă (un element în documentul țintă XML), un subiect (identitatea inițiatorului și rolurile lui), și o acțiune. Când inițiatorul dorește să joace un rol, rolul va fi desemnat de niște mecanisme de atribuire a rolurilor. Nu prezintă interes cum se desemnează un rol și cum se autentifică identitatea inițiatorului.

Pasul 2. Cererea de acces este evaluată conform cu politica (scrisă în XACML) și stările asociate cu documentul de țintă XML. Dacă este necesar, modulului de evaluare a accesului îi este permis să acceseze nu numai politica ci și întregul document țintă XML. De asemenea, el verifică și calitatea de membru al grupului pentru inițiator, dacă este necesar. Decizia de acces indică nu numai răspunsul „ permis" sau" respins", ci și niște acțiuni provizorii.

Pasul 3. Cererea este executată în modulul de executare a cererii, unde sunt executate ambele acțiuni: cele solicitate și cele provizorii specificate în decizia de acces. Documentul țintă XML este actualizat când acțiunea cerută este" scriere"," creare", sau" ștergere". Stările asociate pot fi actualizate.

Pasul 4. Este creată o vedere a inițiatorului când acțiunea cerută este" citire."

Aici sunt două rezultate importante de luat în considerare:

1. Cum se leagă o politică la un document XML?

Una este la nivelul DTD și alta este la nivelul fiecărui document specific. XACML poate fi aplicat în ambele cazuri. În accesul anterior, o singură politică este limitată la toate documente valabile conform cu DTD. În consecință, este nevoie să se mențină legătura intre un DTD particular și politica asociată cu el. În abordarea la nivelul fișierului de date, fiecărui document specific îi este asociată o politică, folosind una din cele două metode:

- Politică asociată, care este notată ca elementul <policy>, element conținut în documentul țintă XML;
- Maparea trebuie să se mențină între fiecare document specific și politica asociată.

2. Cui îi este permis să acceseze politica pentru a o defini sau modifica?

O politică scrisă în XACL este un document XML sau un element al unui document XML. În consecință, XACML poate fi utilizat pentru a specifica o politică de controlul al accesului la politică.

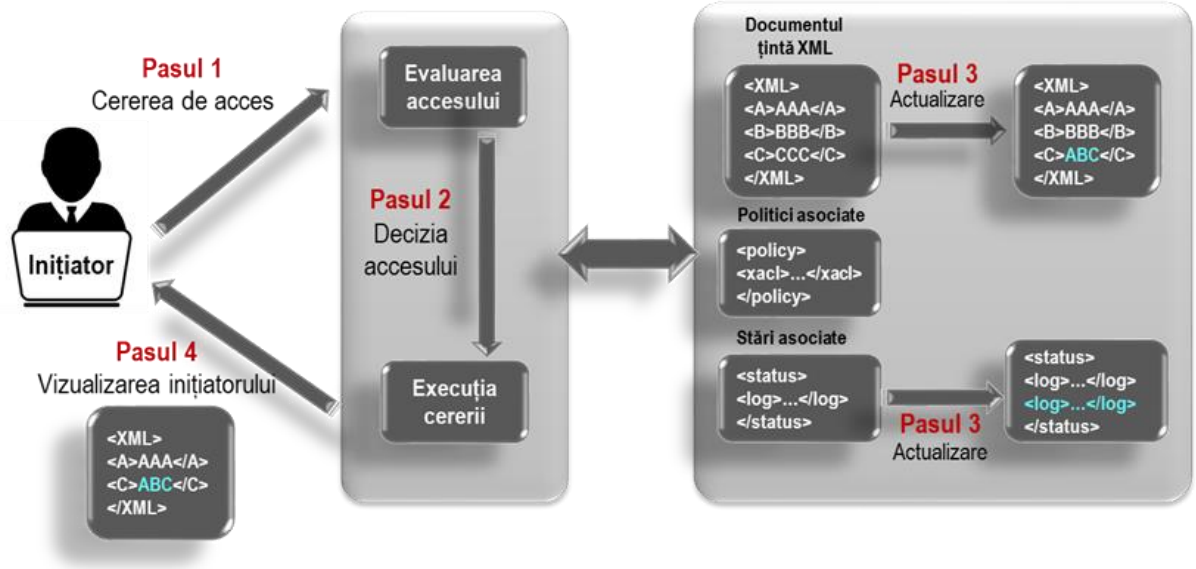


Figura 1.7. Arhitectura de autorizare provizorie XACML - [20]

1.9. Concluzii la capitolul 1

În baza analizei literaturii din domeniul securității documentelor din sistemele informatice, putem deduce că securitatea datelor din sistemele informatice constituie o preocupare constantă, atât pentru specialiștii din domeniu cât și pentru organizații și organisme de stat, astfel că modelarea politicilor de securitate este o temă de mare actualitate.

Principalele cercetări și dezvoltări din domeniul controlului accesului, confidențialității și integrității datelor precum și a metodelor de proiectare și implementare ale acestora, au condus la dezvoltarea unor modele cu aplicabilitate în diverse domenii. Modelele mai importante care au fost prezentate în acest capitol, sunt: Biba, Bell-La Padula, Clark-Wilson, RBAC, ABAC, EPAL, XACML.

Stadiul actual al cercetărilor în domeniul controlului accesului și acțiunilor bazate pe încredere nu permite mai mult decât calculul valorii de încredere acordate unui agent/utilizator și, prin urmare, acest domeniu necesită un studiu mai aprofundat.

În baza acestor concluzii, s-au formulat scopul și obiectivele lucrării.

Scopul: modelarea controlului accesului la documente și a acțiunilor asupra documentelor, prin aplicarea politicilor bazate pe încredere.

Obiectivele de bază:

1. Clasificarea organizațiilor și cuantificarea nivelurilor de încredere acordate membrilor acestora după criterii rezultate în urma studiilor efectuate;
2. Modelarea fluxurilor de lucru pentru câteva tipuri de organizații în scopul de a construi suportul pentru implementarea politicilor bazate pe încredere;
3. Stabilirea condițiilor pe care trebuie să le îndeplinească un utilizator pentru a avea acces și a interacționa cu un obiect pe baza politicilor de încredere;
4. Definirea politicilor de control al accesului, implementate pe durata fuxului de lucru modelat;
5. Crearea politicilor de control al accesului și acțiunilor bazate pe încredere;
6. Modelarea controlului accesului și acțiunilor bazate pe încredere, utilizând tehnologii xml.

2. CONCEPTUL DE „ÎNCREDERE” ÎN CONTEXTUL ORGANIZAȚIONAL

Încrederea este un sentiment, o stare și un concept universal ce este parte a vieții de zi cu zi, și pe baza ei ne definim relațiile sociale. Una din definițiile utilizate, în contribuții științifice, este cea dată de Mayer, Davis și Schoorman [44;45]: „*Consimțământul unei părți de a fi vulnerabilă la acțiunile unei alt e părți, pornind de la premisa că cealaltă parte va întreprinde o anumită acțiune semnificativă pentru cel care oferă încrederea, indiferent de abilitatea de a monitoriza sau controla cealaltă parte”*.

Încrederea este baza interacțiunii umane, în familie, afaceri și societate, sentimentele de încredere sau neîncredere ne definesc modul de acțiune și interacțiune.

De-a lungul timpului au existat numeroase cercetări în domeniul psihologiei, sociologiei, managementului organizațional, tehnologiei informației etc., ce analizează importanța încrederii, și modul în care aceasta afectează interacțiunea umană. Marsh, în 1994 în lucrarea „Formalizing trust as computational concept”, a pus bazele calculării valorii de încredere.

În acest capitol, vom prezenta încrederea și modul în care aceasta intervine în cadrul organizațiilor, de la organizații virtuale până la organizații largi, formale, în crearea de politici de control al accesului, al asigurării confidențialității și integrității datelor.

2.1. Încredere și reputație

“Încrederea implică un anumit grad de incertitudine cu privire la rezultat. Încrederea implică speranță sau optimism în ceea ce privește rezultatul” [39; 45].

Ca aspect social, încrederea este un fapt al vieții de zi cu zi [5;14;24;43;45;78]. Într-adevăr, fără încredere, așa cum sugerează citatul de deschidere al acestui capitol, societățile ar înceta să mai existe [45].

Încrederea se manifestă față de persoane, grupuri de persoane și evenimente.

Interacțiunea cu alte persoane sau grupuri de persoane în vederea atingerii unui scop este ceea ce caracterizează o organizație.

Ca elemente de interacțiune în cadrul unui grup avem:

- Cooperarea;
- Coordonarea;
- Colaborarea;
- Comunicarea;
- Benevolența.

Luhmann, în lucrările ale sale, spune că „Teza principală este că încrederea este un mijloc de reducere a complexității societății” [43;45].

Pentru a putea interacționa cu alți membri ai organizației, un membru al unei organizații, sau o persoană exterioară acesteia, folosește încrederea față de aceștia sau față de grupurile din care face parte.

Exemplu: O persoană se prezintă la o clinică pentru un consult de specialitate, întrucât are încredere în personalul clinicii sau într-un anumit medic. Încrederea este aplicată profesionalismului personalului sau medicului, compasiunii, empatiei de care dă dovadă, etc.; prin urmare, încrederea de sine stătătoare nu este folositoare, ci ea este aplicată unor atribute pe care trebuie să le aibă persoana căreia i se aplică aceasta.

Definiție. Avem încredere sau nu într-o persoană sau grup de persoane, în funcție de manifestarea unor anumite atribute comportamentale, sau aplicarea anumitor cunoștințe profesionale supuse aprecierii.

În funcție de modul de manifestare a atributelor comportamentale sau a cunoștințelor, încrederea față de o persoană sau grup de persoane poate oscila de la neîncredere totală până la încrederea deplină.

Deutsch [27], afirmă că:

a. individul se confruntă cu o cale ambiguă, o cale care poate duce la un eveniment perceput ca benefic (Va^{+}) sau la un eveniment perceput ca dăunător (Va^{-});

b. el percepe că apariția Va^{+} sau Va^{-} este dependentă de comportamentul altei persoane;

c. percepe puterea lui Va^{-} ca fiind mai mare decât puterea lui Va^{+}.

Dacă o persoană alege o cale ambiguă cu astfel de proprietăți, se poate spune că face o alegere bazată pe încredere; dacă nu alege calea, face o alegere bazată pe neîncredere.

A „percepe”, implică faptul că încrederea este o noțiune subiectivă, una în care alegerile care se fac se bazează pe opinii subiective ale lumii, în condițiile în care există multe puncte de vedere ale încrederii, ceea ce duce la premisa că în orice situație, diferite persoane vor putea vedea situația în mod diferit [45].

Faptul că diverse persoane au percepții diferite asupra valorii proprietăților unei situații, sau a unei căi de urmat, duce la concluzia că încrederea este subiectivă, deci și valorile percepute sunt diferite, creând premise diferite pentru fiecare persoană; prin urmare, valoarea percepției încrederii depinde și de situația, momentul în care ea este acordată. În concluzie, încrederea depinde, pe lângă percepția persoanei, și de contextul în care este evaluată.

2.2. Formalizarea încrederii

Încrederea, după cum a demonstrat Deutsch [28], poate fi cuantificată obținându-se atât valori pozitive cât și valori negative, în funcție de percepția pe care o are persoana ce face observațiile față de comportamentul și modul de interacțiune cu persoana față de care trebuie să-și manifeste încrederea.

Pentru o mai bună prezentare a celor ce urmează, pentru persoana sau agentul care execută acțiunea de manifestare a încrederii și a celei căreia i se aplică încrederea, vom folosi termenii de *recomandant* și *recomandat* pe care îi vom defini astfel:

- *recomandant*, este persoana sau agentul care manifestă sau cuantifică încrederea față de altă persoană sau agent;
- *recomandat*, este persoana sau agentul față de care se manifestă sau se cuantifică încrederea.

În general, abordarea încrederii a fost făcută din perspectiva utilizării inteligenței artificiale, în rețele de calculatoare.

2.2.1. Abordarea încrederii de către Stephen Paul Marsh

Una din primele lucrări privind formalizarea încrederii este „Formalising Trust as a Computational Concept" de Stepen Paul Marsh [45], care a tratat problema formalizării, pentru DAI (Distributed Artificial Intelligence).

În cadrul lucrării el face o departajare a tipurilor de încredere, definind următoarele tipuri:

a) Încredere de bază (Basic trust);
b) Încredere generală (General trust);
c) Încredere situațională (Situational trust).

Acestea sunt definite după cum urmează:

a). Pentru încrederea de bază, agenții sunt considerați a fi entități de încredere ce au o „încredere de bază", derivată din experiența anterioară. Aceasta este reprezentată ca T_x adică încrederea în agentul „*x*", unde $-1 \leq T_x \leq +1$;

b). Încrederea generală sau încrederea în agenți,

Fiind dați doi agenți, *x și y* ce aparțin lui *A*, unde *A* este mulțimea agenților, pentru a nota "*x* are încredere în *y*", folosim: $T_x(y)$, iar aceasta are și un interval de valori în $[-1, +1) \Rightarrow -1 \leq T_x(y) < +1$. Valoarea reprezintă mărimea încrederii pe care *x* o are în *y*., și reprezintă pur și simplu încrederea generală a unui agent *x* într-un alt agent *y*. O valoare de *0* înseamnă *x* nu are încredere în *y* (este posibil să nu-l știe deloc pe *y*, deși existența unei reprezentări pentru $T_x(y)$ pare să implice această cunoaștere.), iar o valoare de *-1* ar reprezenta o încredere negativă - neîncredere completă [10; 45; 70].

c). Încrederea situațională. Fiind dați doi agenți *x* și *y*, *x* are încredere în *y* în situația α dar nu are dacă *y* ar fi în situația β. Încrederea a lui *x* în *y* la momentul α o notăm cu $Tx(y,\alpha)$

Alte elemente care sunt prezentate sunt:

- utilitatea unei determinări a încrederii;
- importanța determinării încrederii.

Acestea sunt notate asemănător cu cele de mai sus [45]:

- $U_x(\alpha)$ pentru determinarea utilității determinării încrederii de către utilizatorul x în situația α;
- $I_x(\alpha)$ pentru determinarea importanței determinării încrederii de către utilizatorul *x* în situația α.

Valorile pe care le pot lua elementele cuantificabile sunt în domeniul [-1,+1] pentru utilitate și [0,+1] pentru importanță.

Pentru o trecere în revistă a notațiilor de bază se creează tabelul 2.1 prezentat mai jos [45].

Tabelul 2.1. Rezumat al notațiilor privind încrederea de bază- [45]

Descriere	Reprezentare	Domeniul de valori
Situații	$\alpha,\beta...$	
Agenți	*a, b, c,...*	
Mulțimea de agenți	*A*	
Societăți de agenți (grupuri)	$S_1, S_2... S_n \in A$	
Cunoașterea (*x* cunoaște pe *y*)	$K_x(y)$	True/False
Importanța (situației α pt. *x*)	$I_x(\alpha)$	[0, +1]
Utilitatea (situației α pt. *x*)	$U_x(\alpha)$	[−1, +1]
Încrederea de bază (*a* lui *x*)	T_x	[−1, +1)
Încrederea generală (*a* lui *x* în *y*)	$T_x(y)$	[−1, +1)
Încrederea situațională (*a* lui *x* în *y* pt. α)	$T_x(y, \alpha)$	[−1, +1)

Faptul că încrederea este variabilă în timp, în funcție de contactele dintre *x* și *y* sau de modificarea percepției lui *x* față de *y* [12], a condus la introducerea de către Marsh [45] a unui index temporal. Aceasta face ca elementele din tabelul 2.1 să fie notate ca în tabelul 2.2.

Pentru calculul încrederii situaționale, Marsh [45] utilizează următoarea formulă:

$T_x(y,\alpha) = U_x(\alpha) \times I_x(\alpha) \times T_x(y)$

Tabelul 2.2. Rezumat al notațiilor indexate în timp - [45]

Descriere	Reprezentare	Domeniul de valori
Situații	$\alpha,\beta...$	
Agenți	*a, b, c,...*	
Mulțimea de agenți	A	
Societăți de agenți (grupuri)	$S_1, S_2... S_n \in A$	
Cunoașterea (*x* cunoaște pe *y*)	$K_x(y)^t$	True/False
Importanța (situației α pt. *x*)	$I_x(\alpha)^t$	[0, +1]
Utilitatea (situației α pt. *x*)	$U_x(\alpha)^t$	[−1, +1]
Încrederea de bază (*a* lui *x*)	T_x^t	[−1, +1)
Încrederea generală (*a* lui *x* în *y*)	$T_x(y)^t$	[−1, +1)
Încrederea situațională (*a* lui *x* în *y* pt. α)	$T_x(y,\alpha)^t$	[−1, +1)

Această formulă poate fi interpretată ca „*încrederea unui agent x în altul y într-o situație dată ca fiind probabilitatea ponderată dată de U și I în care x se așteaptă de a obține un rezultat ca și cum ar avea încredere în y"* [70;45].

Marsh introduce de asemenea formule de calcul ale:

- "pragului de cooperare" pe care îl determină ca fiind de forma:

  $Pragul\_de\_cooperare_x(\alpha) = \frac{Risc\_perceput_x(\alpha)}{Competența\_percepută_x(\alpha)} \times I_x(\alpha)$

- "competenței percepute" ca fiind de forma:

  $Competența\_percepută_x = T_x I_x(\alpha)$

De asemenea prezintă și importanța memorării experiențelor avute de un agent x cu un alt agent y de-a lungul timpului și modul cum aceste experiențe influențează încrederea actuală a lui x în y.

Pentru cuantificarea încrederii, Marsh [45] propune următorul tabel de valori (tabelul 2.3). În analiza făcută valorilor extreme, se arată că dacă o valoare a încrederii de *-1* (adică, complete distrust= neîncredere deplină) este posibilă, valoarea de *+1* (blind trust= încredere oarbă) nu este posibil de atins.

Tabelul 2.3. Valorile de încredere ale lui Marsh- [45]

Domeniul de valori	Eticheta
+1	Blind Trust
> 0.9	Very high trust
0.75 to 0.9	High trust
0.5 to 0.75	High medium trust
0.25 to 0.5	Low medium trust
0 to 0.25	Low trust
−0.25 to 0	Low distrust
−0.5 to −0.25	Low medium distrust
−0.75 to −0.5	High medium distrust
−0.9 to −0.75	High distrust
< −0.9	Very high distrust
−1	Complete distrust

2.2.2. Abordarea încrederii de către Abdul-Rahman și Hailes

Mai mulți cercetători au abordat încrederea în cadrul rețelelor de calculatoare și a organizațiilor virtuale. Dintre multiplele abordări vom prezenta abordarea Abdul-Rahman și Hailes pentru sistemele distribuite.

Alfarez Abdul-Rahman și Stephen Hailes au propus un model distribuit în „Un model de încredere distribuit" [2], un model de calcul al încrederii bazat pe încrederea directă și încrederea în agentul care face recomandarea. Încrederea directă a lui *A* în *B* este diferită de încrederea lui *A* în recomandarea lui *C* de către *B*, întrucât valoarea de recomandare a lui *B* pentru *C* este subiectivă, iar *B* poate fi afectat de subiectivitatea relației cu *C*. În lucrare, se propune și un protocol de recomandare.

Formula de calcul a valorii de încredere propusă de ei este prezentată mai jos.

$tv(T) = tv(Rl)/4 \times tv(R2)/4 \times .... \times tv(Rn)/4 \times rtv(T)$,

unde:

tv(Ri) = Valoarea de încredere a *recomandanților* pe calea de întoarcere, inclusiv primul *recomandant* (care a primit *RRQ* original) și ultimul *recomandant* (care a creat *recomandarea*);

rtv(T) = valoarea de încredere recomandată a țintei *T* dată în recomandare;

tvp(T) = valoarea de încredere a țintei T derivată din recomandarea primită pe calea de întoarcere p.

Un solicitant poate avea mai multe recomandări pentru o singură țintă și, prin urmare, recomandările trebuie combinate pentru a obține o singură valoare.

tv(T) = Average(tv,(T),.., tvpT))

Valorile pentru încrederea directă și încrederea recomandatului sunt diferite de cele din lucrarea lui Marsh [45] și sunt prezentate mai jos.

Tabelul 2.4. Semnificația valorilor de încredere directă- [45]

Valoare	Semnificație	Descriere
-1	Neîncredere	Neîncredere completă.
0	Ignorare	Nu se pot face judecăți despre valoarea de încredere a entității.
1	Minimă	Cel mai mic nivel de încredere
2	Mediu	Încredere medie. Corespunde încrederii majorității entităților.
3	Bună	Încredere mai mare decât a majorității entităților.
4	Completă	Încredere completă în entitate.

Tabelul 2.5. Semnificația valorilor de încredere ale recomandatorului - [45]

Valoare	Semnificație	Descriere
-1	Neîncredere	Neîncredere completă.
0	Ignorare	Nu se pot face judecăți despre valoarea de încredere judecată de agent.
1	„Grad de apropiere“ a judecății *Recomandatorului* de judecata proprie despre încredere	
2		
3		
4		

În lucrarea lor, Alfarez Abdul-Rahman și Stephen Hailes [2; 3], analizează încrederea pe baza reputației, în cadrul unei rețele descentralizate, unde eventualele legături pot fi ad-hoc. În protocolul propus de ei, fiecare agent poate fi un recomandant sau un solicitant al unei recomandări. Orice entitate poate fi o țintă pentru o recomandare.

O **recomandare** [2;3] este o informație de încredere comunicată, care conține informații despre reputație. Aceasta are forma:

Reputație = (nume, categorie de încredere, valoare de încredere)

Un **solicitant** emite un mesaj de cerere de recomandare sau un *RRQ* și primește înapoi un mesaj de recomandare. Recomandările pot fi reîmprospătate sau revocate folosind mesajul de actualizare.

Aceste mesaje au următoarea structură (prezentată în format *BNF*):

RRQ::= Requestor_ID, Request_ID, Target_ID, Categories, RequestorPKC, GetPKC, Expire

Categories::= SET OF (Category_Name)

Recomandarea va fi de forma:

Recommendation::= Requestor_ID, Request_ID, Rec_Path, [SEQUENCE OF (Recommendation_Set, TargetPKC) | NULL]

Rec.-Path::= SEQUENCE OF {Recommender-ID)

Recommendation-Set::= SET OF Recomendation-Slip

RecommendationS1ip::= SET OF SEQUENCE(Target-ID, Category_Name, Trust-Value, Expiry)

Mesajul *Refresh* va fi:

Refresh::= Rec_path, Recommendation_Set, Requestor_ID, Request_ID, Target_ID, Recommender_ID

Categories este o mulțime de denumiri de categorii despre care se interesează solicitantul.

RequestorPKC este cheia publică al solicitantului, care poate fi utilizată pentru criptarea *Recomandation_Set*. *GetPKC* este un flag boolean care, atunci când este setat pe true, indică faptul că solicitantul ar dori, de asemenea, o copie a cheii publice a țintei pentru mai multe comunicări. Dacă este disponibil, un certificat cu cheie publică, acesta este returnat în *Recomandation*, în câmpul *TargetPKC*.

Câmpul *Rec_path* conține o secvență ordonată de ID-uri de recomandare. Aceasta arată calea prin care recomandarea s-a propagat de la recomandator la solicitant.

Setul de recomandări conține mai multe instanțe ale *Recomandation-Slip*, care conține informațiile de încredere reale de care este interesat solicitantul. Pentru fiecare categorie, există o secvență care conține *Category_Name*, valoarea de încredere a țintei în raport cu acest nume de categorie, și *Expiry*.

Câmpul *Expiry* conține data de expirare pentru *RRQ* sau *Recommandation*. În cazul *RRQ*, acesta este folosit pentru a elimina orice *RRQ* vechi care ar mai putea exista. În cazul fiecărei recomandări, aceasta este folosită pentru a indica perioada de valabilitate a recomandării, după care nu ar trebui să se mai bazeze pe recomandare.

Dacă *RRQ* ajunge la un punct mort în calea sa și nu reușește să ajungă la un recomandant care este capabil să furnizeze o recomandare, câmpurile *Recommendation_Set* și *TargetPKC* vor fi înlocuite cu valori *NULL*.

2.2.3. Alte abordări ale calculului nivelului încrederii

Lik Mui și alți colaboratorii [47;48], în lucrările „ Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks”, și „A computational model of trust and reputation”, prezintă diferențele dintre reputație și încredere și propun modele de calcul al reputației bazate pe metode statistice și mecanisme de propagare a reputației.

George Pitsilis și Lindsay Marshal în lucrarea „Trust as a key to improving Recommendation Systems” [57], propune o tehnică de modelare a relațiilor de încredere între entități, bazate pe experiențele trecute și un model care să ofere o metodă de estimare încrederii pe care ar trebui să o aibă două entități între ele, ținând cont de asemănările dintre ele. În acest model, entitățile sunt considerate mai asemănătoare, dacă pot prezice cu mai multă exactitate evaluările celorlalte. De asemenea, propune și o metodă de calul al factorului de acoperire normalizat, ce reprezintă o combinare a erorii de recomandare și a calculabilității.

Mai jos sunt prezentate în ordine cele două formule:

$p_{a,i}=\overline{r_a} + \sum_{u=1}^{n} w_{a,u}(r_{u,i} - \overline{r_u})$,

unde

$\overline{r_a}$ = este rating-ul mediu al interogării utilizatorului;

$w_{a,u}$ = coeficientul de corelare a similarității (asemănării) utilizatorului α cu utilizatorul *u* (care apare ca pondere în abatere);

$\overline{r_u}$ = este rating-ul (evaluarea) mediu pentru fiecare dintre cele *n* entități care oferă recomandări;

$r_{u,i}$ = este rating-ul fiecăruia din cei *n*;

$p_{a,i}$ = este rating-ul presupus

$F = (1- \bar{E}) \cdot C$,

unde:

F = factorul de acoperire normalizat ce reprezintă combinarea dintre eroarea medie de recomandare a unui utilizator cu calculabilitatea valorii pentru acel utilizator;

E = eroarea medie de recomandare pentru un anumit utilizator;

C = calculabilitatea valorii unui utilizator.

Scopul lucrării a fost de determinare a unei metode de calcul a încrederii, utilizând parametrii cantitativi și calitativi, bazându-se pe alegeri comune, în vederea eficientizării sistemului de recomandare.

„A Vector Model of Trust for Developing Trustworthy Systems” este lucrarea în care Indrajit Ray și Sudip Chakraborty [34], propun un model vectorial de evaluare a încrederii ținând cont de context, timp, experiență, cunoștințe, recomandări și experiența anterioară. Scopul este de a calcula încrederea între doi agenți, de a explora dinamica încrederii și influența relației anterioare de încredere.

În lucrarea „Component based trust management in the context of a virtual organization” [77] este propus un model de administrare a încrederii pentru menținerea nivelurilor de încredere

în cadrul unui VO. Acestea pot fi actualizate dinamic, iar modelul acceptă integrarea valorilor de încredere parțiale pentru a evalua încrederea compusă a unei entități compuse.

2.4. Clasificarea organizațiilor și modul de organizare

Pentru început vom căuta să definim ce este o organizație.

ORGANIZAȚIE: Asociație, instituție socială care reunește oameni cu preocupări și, uneori, cu concepții comune, constituită pe baza unui regulament, a unui statut, etc., în vederea depunerii unei activități organizate și realizării unor scopuri comune [52].

Dicționarul Cambridge o definește ca fiind: un grup de oameni care lucrează împreună într-un mod organizat pentru un scop comun [53].

În Dicționar Oxford: un grup organizat de oameni cu un scop anume, cum ar fi o afacere sau departament guvernamental [54].

Din cele trei definiții de mai sus, rezultă că o organizație este o grupare ce are un anumit scop.

Având în vedere scopul, beneficiul activității sau natura comportamentului membrilor organizațiilor, se identifică cinci tipuri diferite de organizații caracteristice societății contemporane și se încearcă diferențierea pe baza scopului general al fiecăruia [30]:

- asociațiile voluntare, de tipul celor religioase, științifice, etc;
- organizații militare;
- organizații filantropice (de binefacere), spirituale, asociații de asistență socială;
- organizații de tip corporații (organizații industriale, financiare etc.);
- organizații de afaceri familiale, micile afaceri.

O altă clasificare, bazată pe principiul categoriilor de beneficiari, este cea de mai jos, formată din următoarele patru tipuri:

- organizații de beneficiu reciproc, al căror prim beneficiar sunt membrii și cei înscriși care dețin un rang (partidele politice, sindicatele, cluburile etc);
- organizațiile de afaceri, care au ca prim beneficiar proprietarii și managerii (firmele industriale, băncile, companiile de asigurări, magazinele de vânzări cu ridicata și cu amănuntul);
- organizații care realizează servicii și au ca prim beneficiar clienții; în această categorie autorii exemplifică agențiile de plasare a forței de muncă; spitalele, școlile, societățile de ajutor, clinicile de sănătate mintală;

- organizațiile publice de care beneficiază marele public, aici fiind incluse, spre exemplificare, statistica la nivel statal, serviciile militare, departamentele poliției și pompierilor, poliția locală.

În general, atât organizațiile publice cât și cele care realizează servicii, au structuri de tip ierarhic, stabilite prin lege.

Organizațiile de afaceri pot avea una din următoarele structuri [55]:

1. pre-birocratice;
2. birocratice;
3. post-birocratice;
4. funcționale;
5. divizionale;
6. matriciale;
7. cerc organizaționale;
8. echipe;
9. rețele;
10. virtuale.

În cele ce urmează vom prezenta pe larg structurile de mai sus [55].

Structurile pre-birocratice (antreprenoriale) nu au sarcinile standardizate. Sunt cel mai frecvent întâlnite în organizațiile mai mici, caracterizate de rezolvarea de sarcini simple, cum ar fi vânzările. Structura este total centralizată. Liderul ia toate deciziile cheie, iar cea mai mare parte a comunicării se face pe baza conversației. Este deosebit de utilă pentru afacerile noi (antreprenoriale), deoarece permite fondatorului să controleze creșterea și dezvoltarea. Acestea se bazează de obicei pe dominația tradițională sau dominația carismatică.

Structurile birocratice au un anumit grad de standardizare. Sunt mai potrivite pentru organizații mai complexe sau mari, adoptând de obicei o structură complexă. Caracteristicile birocrației sunt:

- Roluri clare și responsabilități definite;
- O structură ierarhică;
- Respect pentru merit.

Acestea au mai multe niveluri de management, de la directori executivi seniori și manageri regionali, până la manageri de magazine, iar autoritatea decizională trebuie să treacă prin mai multe niveluri decât în organizațiile antreprenoriale. Au proceduri, politici și constrângeri rigide și stricte. Acest tip de structuri este reticent la adaptarea la condițiile pieței sau la modificarea a ceea ce făceau de la începutul companiei. Există organigrame pentru fiecare departament, se știe

cine este responsabil și care sunt responsabilitățile în fiecare situație. Deciziile se iau printr-o structură piramidală, autoritatea se află în vârful piramidei și deciziile circulă de sus în jos, ceea ce determină mai multe reguli și standarde pentru companie, iar procesul operațional este urmărit cu o supraveghere atentă. Dintre avantajele managerilor de nivel superior este faptul că au un control deosebit, ceea ce este bine pentru cei care au un stil autoritar de management. Luarea deciziilor strategice este, de asemenea, mai rapidă, deoarece există puține persoane de la care să trebuiască să se ia aprobare.

În cadrul *structurilor post-birocratice*, deciziile se bazează pe dialog și consens, mai degrabă decât pe autoritate și comandă. Organizația este mai mult o rețea decât o ierarhie, și se pune accentul pe meta-reguli de luare a deciziilor și nu pe regulile de luare a deciziilor. Acest tip de luare a deciziilor orizontale pe modelul consensului este adesea utilizat în organizațiile non-profit sau organizațiile comunitare. Este utilizat pentru a încuraja participarea în grupuri de lucru.

În organizațiile bazate pe *structurile funcționale*, activitățile principale constau în coordonarea, supravegherea și alocarea sarcinilor. Structura organizațională determină modul în care organizația realizează sau funcționează, prin modul în care persoanele din organizație sunt grupate. În general, oamenii se organizează după funcții, de exemplu producția, marketingul, resursele umane și contabilitatea. Această organizare a specializării duce la eficiență operațională, iar angajații devin specialiști în propriul domeniu de expertiză.

Structurile divizionale sunt formate din diviziuni de sine stătătoare, diviziuni care produc un produs și, pot opera ca un business separat sau ca un centru de profit. Diviziunile pot avea, de asemenea, departamente proprii precum: marketing, vânzări și inginerie. În structura divizională se folosește autoritatea delegată, astfel încât performanța poate fi măsurată direct cu fiecare grup, iar acest lucru conduce la performanțe mai bune și un moral mai ridicat al angajaților.

Structurile matriciale grupează angajații atât pe funcție cât și pe produs, simultan. O organizație matricială folosește frecvent echipe de angajați pentru a realiza munca, pentru a profita de punctele tari, precum și pentru a compensa punctele slabe ale formelor funcționale și descentralizate. Un exemplu ar fi o companie care produce două produse, „produsul a” și „produsul b”. Folosind structura matricială, această companie va organiza funcții în cadrul companiei după cum urmează: departamentul de vânzări „produs a", departamentul de servicii pentru clienți „produs a", departamentul contabilitate „produsul a", departamentul de vânzări „produsul b", departamentul serviciul de clienți „produsul b", departamentul de contabilitate „produsul b”.

Structurile plane (sau cerc) sunt de obicei forma de organizare a companiilor mici (start-up-uri, spin-off-uri universitare). Pe măsură ce companiile cresc, acestea tind să devină mai complexe și ierarhice, ceea ce duce la o structură extinsă, cu mai multe niveluri și departamente.

Unele din companiile mari, precum Valve Corporation, Google, au păstrat această structură deși au devenit companii mari. În general, companiile de IT sau cele de avocatură păstrează această formă.

Structurile de echipă, sunt structuri nou apărute, echipele fiind constituite atât pe nivel orizontal cât și pe nivel vertical. Toți cei dintr-o locație de profit constituie o echipă, dar și șefii echipelor constituie o echipă la rândul lor. Se pot plia perfect pe organizații birocratice.

Structurile de rețea sunt apărute mai recent, și sunt de asemenea structuri moderne, bazate pe comunicații și managementul relațiilor externe. Pot folosi diverși furnizori, ceea ce permite reducerea prețurilor produselor.

Structurile virtuale permit o legătură strânsă cu furnizorii și clienții, gestionând ușor procesele de afaceri din întreaga organizație. Se bazează pe software-ul existent, ea creând o rețea de alianțe, folosind Internet-ul. Aceasta presupune că nucleul organizației poate fi mic, dar totuși compania poate opera la nivel mondial pentru a fi lider de piață în nișa sa. Amazon este un exemplu de organizație virtuală.

2.5. Organizație și încredere

Integrarea unui nou membru într-o organizație nu aduce automat și o încredere în capabilitățile acestuia, indiferent de reputația care l-a precedat pe acesta.

S-a discutat la începutul capitolului despre încredere și diferite moduri de determinare a acesteia pentru organizații virtuale. În cele ce urmează se va încerca să arătăm cum aceste metode pot fi aplicate și în alte tipuri de organizații, în care încrederea nu este calculată ci este bazată pe o lungă colaborare și are la bază competența, loialitatea, bunăvoința, perseverența personalului și acestea sunt determinate pe baza unui complex de factori, dar cel mai important este aprecierea și considerația membrilor organizației.

Procesul informațional-decizional se manifestă prin crearea de documente ce conțin date și informații care sunt procesate de persoane (numite în continuare subiecți) ce fac parte din organizație.

În structura relațiilor din cadrul organizației precum și a relațiilor dintre organizații, unde îndeplinirea sarcinilor are loc prin utilizarea de sisteme de informare și comunicare și unde comportamentul actorilor este influențat de îngrădirea socială și de formalități, trebuie acordată atenție diferitelor tipuri de încredere:

- încrederea personală. Actorul are, pe baza experienței și a aprecierii, intenția de a se baza cu un sentiment puternic de siguranță, pe dependența unei alte persoane sau a unui grup de

persoane, fiind conștient de eventualele consecințe negative. Pentru această intenție se evaluează din timp nivelul de încredere al unei persoane;

- încrederea impersonală. Aceasta este așteptarea ca un sistem sau o instituție să permită o dezvoltare viitoare pozitivă. Sistemul este evaluat înainte de a i se acorda încredere.

„Încrederea este intenția de a acționa ca și cum persoanele sau sistemele impersonale se comportă în modul așteptat și prevăzut. Aceste așteptări se bazează pe experiențele avute, iar actorul este conștient de riscul în care este implicat”.

Încrederea se manifestă prin permiterea accesului la diferite date și informații, funcție de poziția subiectului față de acele informații. Informațiile vehiculate, indiferent de cine le-a produs, sunt considerate proprietatea organizației. *Subiecții* pot astfel să ia la cunoștință sau nu despre acestea, să modifice informațiile, să le citeze, modifice, etc.

Subiecții fac parte din diverse grupuri de lucru, formale și informale. Grupurile formale sunt cele care formează organizația (departamente, servicii, secții, birouri, compartimente, ateliere, etc.), iar grupurile informale sau grupurile ad-hoc sunt grupuri create cu scop lucrativ și care își încetează activitatea în urma atingerii scopului.

Pe durata activității acestor grupuri (formale și informale), accesul la obiectele sau categoriile de obiecte stocate, create sau utilizate, se bazează pe încrederea (trust) acordată de organizație fiecărui subiect care face parte dintr-un grup.

Acordarea încrederii se face diferențiat, în funcție de poziția, activitatea și importanța subiectului în cadrul grupului (formal sau informal) și a organizației.

Nu se poate face o abordare simplistă a acestor nivele de încredere (trust) de tipul da/nu, adică de încredere și de neîncredere (trust/distrust). Specialiștii din domeniul sociologiei [45], au stabilit că nivelul de încredere adoptă valori fuzzy, adică valori cuprinse între 0.00 și 1.00, valori cărora, în mod grosier le-au fost atribuite nivele corespondente de încredere. Nivelurile, pot corespunde unor intervale de valori ca cele prezentate în tabelul 2.6.

Abordarea acestui mod de clasificare, bazat pe etichetarea încrederii, nu corespunde în totalitate realității, dar permite o clasificare mai rapidă a nivelurilor de încredere prin acordarea unui nivel grupului din care face parte un subiect și moștenirea acestuia de către toți subiecții ce aparțin grupului de lucru.

Pentru a rafina nivelul de încredere al personalului se poate atribui un coeficient de corecție ce permite creșterea nivelului de încredere până la nivelul maxim, dar acest coeficient nu se aplică tuturor membrilor grupului, ci pe cazuri individuale.

Tabelul 2.6. Intervalele de valori ale încrederii - [45]

Gamă de valori	Etichetare
+1	Blind trust
> 0,9	Very high trust
0,75 până la 0,9	High trust
0,5 până la 0,75	High medium trust
0,25 până la 0,5	Low medium trust
0 până la 0,25	Low trust

Coeficientul de încredere nu poate fi negativ, pentru că în acest caz, nivelul de încredere manifestat față de un membru al grupului poate fi mai mic decât cel al grupului, fapt ce duce la excluderea persoanei din grupul de lucru, deci pierderea calității de membru. Totuși sunt și situații în care nivelul de încredere pentru accesarea unui obiect poate fi scăzut ca urmarea a unei decizii a conducerii organizației.

În general, nivelul de top al unei organizații beneficiază de cel mai înalt nivel de încredere iar nivelul de execuție de un nivel de încredere mai scăzut, direct proporțional cu importanța activității depuse în cadrul organizației. Astfel, liderul organizației are cel mai înalt nivel de încredere în cadrul ei. Însă cum el nu se poate ocupa de toate problemele din cadrul acesteia, face delegare de responsabilități și atribuții. În imaginea de mai jos, prezentăm o posibilă schemă de organizare la nivelul unei organizații de cercetare-dezvoltare.

Ca exemplu, un general manager din cadrul unei organizații va numi un director științific pe probleme de cercetare care se va ocupa și de contractare, un director economic care se va ocupa de probleme financiar-contabile, un șef de serviciu administrativ, care se va ocupa de problemele administrative, iar aceștia fiecare mai departe vor trebui să delege din responsabilități și atribuții, funcție de complexitatea organizației și a activității desfășurate, pe secții, birouri, compartimente, subiecți din compartimente.

Astfel se creează o ierarhie de delegări de responsabilități și competențe ce poate fi reprezentată ca în schema de mai jos din figura 2.1.

În acest mod se ajunge la faptul ca subiectul X din compartimentul ZZ să aibă un nivel de încredere (trust) ridicat pe problemele pe care trebuie să la rezolve zilnic („High Trust”) iar pentru problemele din compartimentul WW ce sunt rezolvate de subiectul Y, să aibă nivelul de încredere „Low Trust” sau „No Trust”.

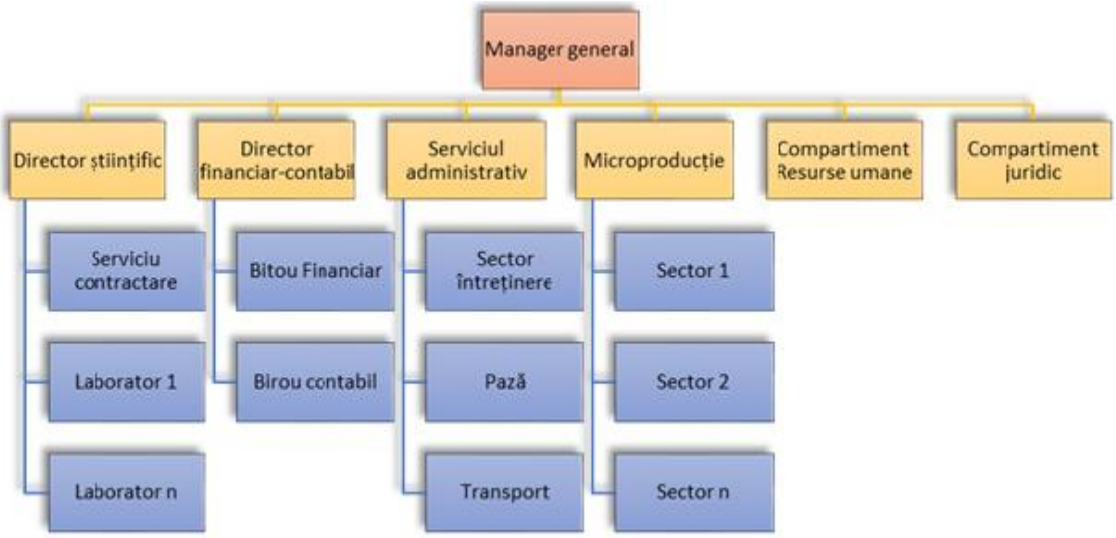


Figura 2.1. Structura organizatorică ipotetică a unei organizații de cercetare

O altă concluzie, ce rezultă de aici, este că circuitul documentelor din cadrul ierarhiei prezentate mai sus se bazează pe cel mai mare nivel de încredere, ce poate fi menținut pe o anumită categorie de date, informații și documente. Astfel, nivelul de încredere, pe care îl poate avea o persoană față de o anumită categorie de date și informații, poate fi unul ridicat, iar față de alte categorii de date și informații din alte sectoare de activitate poate fi unul scăzut.

De asemenea, o importanță deosebită o are și delegarea de competențe pe diferite ramuri ale structurii ierarhice din cadrul organizației, prin stabilirea unui anumit circuit informațional și niveluri de încredere diferite pe diversele categorii de date și informații pentru subiecții organizației. Astfel, deciziile privind activitatea sunt transmise de sus în jos, iar rezultatele activității se centralizează de jos în sus, creând o contrabalansare a acestora, deciziile influențând rezultatele și invers (figura 2.2).

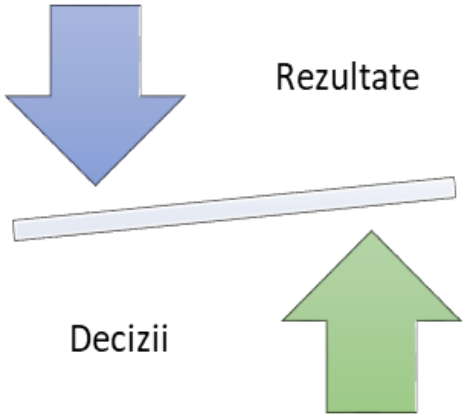


Figura 2.2. Fluxul de decizii și răspunsul la acestea

De aici mai rezultă o altă concluzie și anume că, manipularea datelor și a informațiilor de bază ale organizației este efectuată de subiectul cu cea mai mică responsabilitate privind actul de decizie de pe o anumită ramură a arborelui de delegare a responsabilităților și competențelor, comentarea și modificarea acestora efectuându-se de cei de pe același nivel sau un nivel intermediar, iar aprobarea efectuându-se de cei de pe nivelele de top (de conducere).

2.5.1. Un exemplu de utilizare a încrederii

Considerăm o organizație de afaceri care prestează activități de cercetare-dezvoltare și, are contracte cu alte organizații publice care lucrează cu informații clasificate. Pentru accesarea informațiilor clasificate, pentru personalul care este implicat în activitate, este nevoie de o autorizare pentru nivelul corespunzător de clasificare a informației. De asemenea, pentru o perioadă determinată, este nevoie de personal extern pentru a putea finaliza angajamentele luate.

Personalul implicat va fi de două categorii:

- Personal care are autorizare privind informațiile clasificate;
- Personal intern și extern care nu are autorizare de accesare a informațiilor clasificate.

De asemenea, personalul poate fi angajat la sediul companiei, și/sau să facă parte dintr-o rețea virtuală, creată pentru acest scop.

Personalul din a doua categorie, deși, nu are autorizare privind informațiile clasificate, datorită competențelor pe care le deține, este necesar în dezvoltarea produselor ce vor fi implementate.

În această situație, pentru aplicațiile ce vor fi folosite, trebuie luate măsuri, pentru un control riguros al accesului, asigurarea confidențialității și integrității datelor.

Ca și în exemplele privind organizațiile virtuale, și în această situație, încrederea este un factor major în selecția personalului. Doar că, de această dată, selecția nu va fi impersonală, pe baza unui sistem IA, ci hibridă, printr-o selecție de personal bazată pe cunoaștere directă, cât și printr-un mecanism de recomandare impersonal, bazat pe calculul reputației (metodele descrise la începutul capitolului) pentru rețeaua virtuală. Astfel, în cadrul organizației prezentate mai sunt două grupări care conlucrează la realizarea contractelor:

- Grupul virtual;
- Grupul formal din cadrul organizației, ce este la rândul lui format din două categorii de personal:
  - Personal permanent;
  - Personal temporar angajat pe durata contractului.

Presupunem că structura organizatorică a personalului implicat în proiect va avea următoarea formă (figura 2.3).

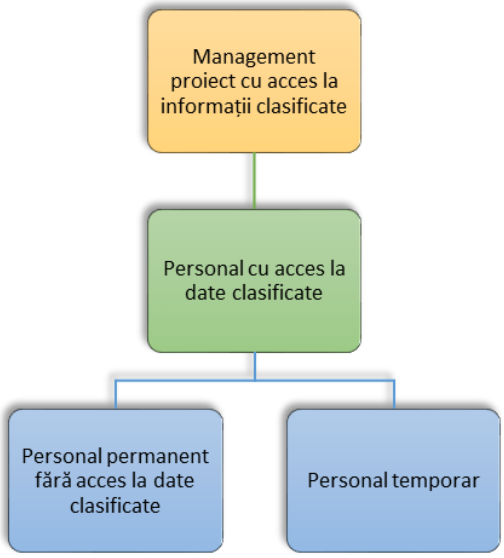


Figura 2.3. Structura organizatorică a grupului de lucru

În această situație, se creează un flux și o ierarhie de execuție și un flux și o ierarhie de decizie, ca în figura 2.4.

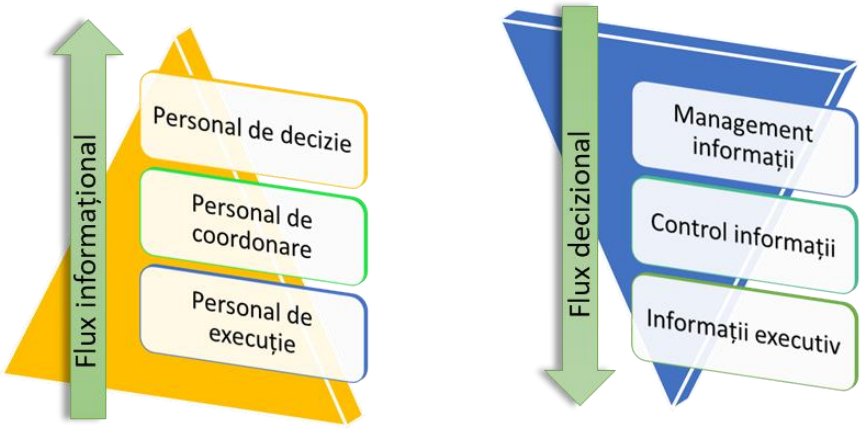


Figura 2.4. Fluxul informațional și decizional

Nivelul de încredere în informație crește, pe măsură ce aceasta parcurge fluxul informațional și determină fluxul decizional.

Din diagrama referitoare la eventuala structură de subordonare, putem spune că cea mai mică încredere o are personalul extern și, cel care nu are acces la informații clasificate, iar cel mai mare nivel de încredere, managementul proiectului, care este format din personal cu acces la informații clasificate. Ca urmare, în asigurarea controlului accesului, confidențialității și integrității datelor prin intermediul încrederii, apare un element nou, și anume *fluxul de date*. Acesta are un rol determinant, prin creșterea nivelului de încredere necesar pentru accesarea datelor și informațiilor cuprinse in documente.

Informațiile trec de la cel mai mic nivel de încredere, către cel mai mare, schimbându-și valoarea la trecerea la nivelul superior, pe măsură ce diverși utilizatori acționează asupra lor.

În exemplul de mai sus se conturează mai multe categorii de date (date clasificate și date generale) și de utilizatori care intervin pe durata desfășurării contractului. În mod normal, elementele de proiect care nu au contact cu date clasificate, vor fi preluate de personalul cu cea mai mică încredere. Pe măsură ce gradul de confidențialitate crește, și nivelul de încredere al personalului implicat trebuie să fie crescut.

2.5.2. Exemplu de proiectare a unui sistem informatic utilizând controlul accesului și acțiunilor utilizatorilor pentru o clinică medicală. Analiza sistemului informațional

Fie o organizație publică de prestări servicii medicale. Pentru prelucrarea datelor unui pacient care se prezintă la un consult, intervin mai mulți subiecți care aparțin unor compartimente diferite.

Vom prezenta un scenariu, privind datele și modul de interacțiune cu acestea:

- Pacientul se prezintă la sediul organizației, este înregistrat și i se comunică ora planificată pentru consultație;
- La întâlnirea cu medicul, după identificarea pacientului prin intermediul datelor de identificare, acesta citește istoricul de sănătate al pacientului, face anamneza și eventual un control sumar al stării de sănătate. Dacă este necesar, recomandă efectuarea de analize de laborator și, dacă consideră că are nevoie de o a doua părere, consultă un coleg de aceeași specialitate sau de altă specialitate. Colegul consultat, poate fi din aceeași organizație sau poate fi extern organizației. La finalul consultației, se eliberează rețeta de tratament, pentru farmacie;
- Pacientul plătește consultația și se duce să-și ridice medicamentele de la farmacie. Farmacistul citește rețeta și eliberează medicamentele, cu recomandările de rigoare.

În tabelul de mai jos s-au sintetizat subiecții, obiectele, acțiunile și contextul în care au loc acțiunile.

În diagrama din Figura A2.1. din Anexa 2, prezentăm acțiunile necesare a fi efectuate.

Dacă cea mai mare parte a acțiunilor au loc în cadrul organizației (care poate fi un spital, o clinică, etc.), consultarea unui al doilea specialist, care poate avea altă specialitate decât medicul la care s-a prezentat inițial pacientul, poate avea loc în cadrul organizației sau în afara ei prin prezentarea istoricului, anamnezei inițiale și a analizelor online, situație în care se dorește protecția identității pacientului.

Tabelul 2.7. Sinteza activităților, obiectelor și contextului de lucru pentru o organizație de prestări de servicii medicale.

Etapă	Subiect	Acțiune	Tipuri de date	Context
1	Personal registratură	Înregistrare pacient	Date identificare	sediu
2	Medic 1	Anamneză	Date privind simptomatologia pacientului, istoric pacient, propunere analize	sediu
3	Asistent laborator registratură	Înregistrare date trimitere laborator, eliberare rezultate	Date identificare pacient, analize de efectuat	sediu
4	Asistent laborator, prelevare probe	Înregistrare probe prelevate	Date identificare, probe prelevate, alte analize	sediu
5	Biochimist	Completare rezultate analiză	Rezultate analize	sediu
6	Medic 1	Citire rezultate, tratament, prescripții medicale, diagnostic	Date identificare, rezultate analize, diagnostic inițial, tratament final.	sediu
7	Medic n	Citire date de identificare, anamneza, istoric pacient, rezultate analize, diagnostic	Date de identificare, istoric pacient, anamneza, rezultate analize	sediu
		Citire anamneza, istoric pacient, rezultate analize	Istoric pacient, anamneza, rezultate analize, diagnostic n, tratament propus.	extern
8	Casierie	Plată consultație	Date identificare, proceduri aplicate	sediu
9	Farmacist	Eliberare medicamente	Date identificare, diagnostic	sediu

Din cele prezentate, se conturează mai multe grupuri de obiecte:

- Datele de identificare,
- Istoric pacient,
- Diagnostic prezumtiv,
- Rezultate analize,
- Diagnostic final,
- Medicație,
- Costuri medicale.

Tabelul 2.8. Categorii de obiecte, personal implicat, drepturi

Nr. crt.	Tipuri de date	Grup de utilizatori	Acțiuni posibile		
			creare	modificare	consultare
1	Identificare	Personal registratură	X	X	X
		Medic cabinet	-	-	X
		Personal laborator	-	-	X
		Personal financiar-contabil	e	-	X
		Personal farmacie	-	-	X
2	Istoric medical	Personal registratură	-	-	X
		Medic cabinet	X	X	X
		Personal laborator	-	-	-
		Personal financiar-contabil	-	-	-
		Personal farmacie	-	-	-
3	Diagnostic prezumtiv, analize propuse	Personal registratură	-	-	-
		Medic cabinet	X	X	X
		Personal laborator	-	-	X
		Personal financiar-contabil	E	-	-
		Personal farmacie	-	-	-
4	Rezultate	Personal registratură	-	-	-
		Medic cabinet	E	-	X
		Personal laborator	X	X	X
		Personal financiar-contabil	-	-	X
		Personal farmacie	-	-	-
5	Diagnostic final, tratamente medicale, medicație	Personal registratură	-	-	-
		Medic cabinet	X	X	X
		Personal laborator	-	-	-
		Personal financiar-contabil	-	-	-
		Personal farmacie	-	-	X
6	Costuri servicii medicale	Personal registratură	-	-	-
		Medic cabinet	X	X	-
		Personal laborator	X	X	-
		Personal financiar-contabil	-	-	X
		Personal farmacie	X	-	-

Asupra acestor grupuri de obiecte acționează următoarele grupuri de subiecți:

- personal registratură;
- medici specialitate;
- personal laborator;
- personal financiar contabil;
- personal farmacie.

Contextele de lucru sunt:

- în cadrul organizației;
- în afara organizației, caz în care se aplică legislația GDPR.

Datele sunt cuprinse într-un singur obiect, fișa de observație.

Pe parcursul duratei de viață a acestui document, diverse grupuri de utilizatori au dreptul să intervină, efectuând diverse acțiuni.

Din tabelul de mai sus, putem concluziona că acțiunile efectuate sunt consecutive, iar participanții sunt limitați numai la informațiile necesare pentru a-și desfășura activitatea.

Datele vehiculate sunt accesate în funcție de utilizator și de context.

După prestarea serviciilor medicale, aceste date pot fi ulterior arhivate, distruse, etc., conform politicilor organizației.

2.6. Obiectele și nivelul de încredere

În general, un obiect necesită același nivel de încredere acordat subiecților în vederea consultării, pe durata existenței sale, dar sunt și momente în care el sau anumite elemente ale lui necesită o scădere a nivelului de încredere, necesar accesării acestuia pentru a putea fi consultat, sau o creștere temporară a nivelului de încredere acordat subiectului. În continuare vom prezenta exemple pentru susținerea celor afirmate mai sus.

- Datele și informațiile financiar-contabile în general, cât și cele de contractare, sunt secrete de serviciu, pe durata unui exercițiu financiar, astfel că nimeni din afara colectivului de subiecți care au ca delegare de competență prelucrarea și utilizarea lor nu are acces la ele. Totuși, la sfârșitul perioadei de exercițiu financiar, conducerea organizației trebuie să facă prezentarea acestora în fata investitorilor sau a personalului companiei. În această situație nu se va crește nivelul de încredere al subiecților, ci se va scădea nivelul de încredere necesar pentru accesul la obiectele ce vor fi diseminate.
- În vederea realizării unei lucrări de sinteză, se cere colaborarea mai multor compartimente, care au un fond comun de elemente de prelucrat, elemente ce interacționează. Astfel, se ajunge ca anumite elemente de informație disparate, din diverse compartimente, să fie analizate și împreună să creeze o imagine a stării de fapt a organizației, dintr-un anumit punct de vedere. Prin urmare, subiecții care lucrează la această raportare, vor lua cunoștință de elementele celorlalte compartimente, elemente la care până acum nu au avut acces. Acest lucru presupune creșterea temporară a nivelului de încredere acordată subiecților pe durata activităților desfășurate în comun.

În literatura de specialitate, se consideră nivelul de încredere absolut (blind trust) ca având valoarea „+1” valoare considerată de neatins [45], iar valoarea de neîncredere este „0”, dar acestea

sunt valori stabilite arbitrar. Se pot folosi orice alte valori, dar pentru noi pentru exemplificare în continuare vom folosi valorile cuprinse între „0” și „1”.

Pe măsură ce scade încrederea într-o persoană, în același timp crește nivelul de neîncredere, astfel menținându-se valoarea constantă de 1 a sumei lor.

În general încrederea nu se manifestă constant față de toate obiectele. Față de anumite obiecte încrederea poate fi „1” iar față de altele poate fi „0”, cu variații între „0” și „1”, funcție de poziția pe care o are subiectul față de obiectele corespunzătoare, poziție care corespunde celei a grupului din care face parte și la care se poate adăuga un coeficient de corecție.

Astfel, față de obiectele create de subiect, nivelul de încredere este „1”, față de obiectele create de un coleg de departament, subiectul poate avea nivelul de încredere „0,5” iar față de obiectele create de un coleg din alt departament, obiecte la care el nu are acces, nivelul de încredere poate fi „0”. În general, o persoană moștenește nivelul de încredere al departamentului din care face parte, dar poate avea față de anumite obiecte un nivel de încredere mai ridicat sau coborât decât cel a departamentului.

În funcție de nivelul de încredere pe care îl are față de un obiect, subiectul, după accesarea obiectului, poate efectua diverse acțiuni acestuia sau asupra grupului de obiecte (documentului) ce îl conține.

Aceste acțiuni sunt:

- Creare (Create);
- Citire (Read);
- Modificare (Modify);
- Comentare (Comment);
- Aprobare (Approvement);
- Imprimare (Print);
- Citare (Quoting);
- Ștergere (Delete);
- Arhivare (Archiving).

Prima acțiune asupra unui obiect este crearea și asamblarea în grupuri de obiecte. Este activitatea prin care se pun bazele obiectului, folosind elementele necesare creării lui.

Următoarea etapă este trimiterea la nivelul superior pentru citire în vederea verificării (eventual a comentării obiectului) și a aprobării temporare sau finale.

În urma verificării, se poate ca obiectul să fie trimis spre modificare, urmând ca ulterior să se reîntoarcă spre reluarea procedurilor menționate mai sus.

În final, după aprobarea acestuia, pe baza unor clasificări bazate pe relația de încredere, acesta poate fi accesat de diverși subiecți pentru citire, citare, comentare.

În urma creării obiectului, acesta conține varii elemente care necesită diverse niveluri de încredere acordate subiecților pentru a fi accesate.

Pentru a ilustra cele afirmate mai sus, vom prezenta un exemplu.

Un grup de obiecte complex, creat cu diferite date și informații (ce constituie obiectele grupului) din diverse compartimente, destinat nivelului de management al instituției, conține obiecte care sunt accesibile anumitor subiecți din compartimente, direcții, celor cu nivel ierarhic de director și manager general al organizației. În acel document, pe lângă obiecte cu un nivel scăzut de încredere sunt și obiecte ce necesită o protecție sporită, ce nu sunt destinate managementului de nivel mediu. Prin urmare, aceste obiecte trebuie protejate, astfel ca orice subiect care nu aparține nivelului de top și care accesează obiectul creat electronic, să nu aibă acces la obiectele care nu îi sunt destinate, obiectele respective fiind considerate confidențiale. Prin acordarea de valori de încredere subiecților, aceștia pot accesa obiectele care au nivelul de încredere corespunzător.

2.7. Concluzii la capitolul 2

Cercetările efectuate până în prezent, referitoare la reputația și recomandările primite de diverși subiecți ținând cont de migrația forței de muncă și de nevoia de cunoaștere a noilor membri ai unei organizații, au condus la integrarea conceptului de *încredere* în cadrul unei organizații. Astfel, au fost cuantificate diversele niveluri de încredere și modele de calcul pentru încredere, risc, competență, și alte valori, toate având ca scop reducerea riscului implicării unei persoane, sau agent, în activitatea unei organizații. De asemenea, au fost create și modele distribuite de recomandare și protocoale ce pot fi implementate în cadrul organizațiilor virtuale și nu numai.

Putem concluziona că teoria încrederii (trust theory) aplicate în relațiile din cadrul unei organizații, are ca fundamente:

- definirea organizației, clasificarea acesteia și modul de organizare;
- încrederea în cadrul organizației, clasificarea încrederii și o etichetare a acesteia;
- relațiile de încredere dintre subiecți și obiectele ce sunt grupate sub forma de documente.

Pe baza acestora se pot crea exemple de implicare a încrederii în procesul formal-decizional al organizațiilor.

Documentele formate în organizație sunt folosite în procesele decizionale prin intermediul acțiunilor utilizatorilor. Aceste documente sunt prezentate sub forma generică de grupuri de obiecte care sunt supuse acțiunilor subiecților prin aplicarea încrederii. Cuantificarea încrederii în cadrul unei organizații determină relațiile de încredere dintre subiecții și obiectele din organizație.

Se poate concluziona că, în cadrul organizațiilor, politicile de securitate se aplică prin asigurarea confidențialității și integrității datelor și informațiilor din cadrul documentelor care circulă în interiorul lor. Prin aplicarea încrederii în relațiile dintre subiecți și obiecte rezultă modalități de aplicare a acestor politici de confidențialitate și integritate.

3. CONDIȚIILE APLICĂRII ÎNCREDERII ÎN CADRUL ORGANIZAȚIILOR, PENTRU ASIGURAREA CONTROLULUI ACCESULUI, ACȚIUNILOR ȘI INTEGRITĂȚII INFOMAȚIILOR

În cele ce urmează vom conceptualiza cele prezentate în capitolele anterioare, prezentând un mod de abordare al controlului accesului, acțiunilor și asigurării integrității, bazat pe încredere.

În calitate de autor, în articolele publicate, am denumit acest concept: „trust-based access and actions control policies", politici de control al accesului bazate pe încredere.

3.1. Concepte și termeni

În general, încrederea acordată unei persoane [45;16;18] pentru a realiza o acțiune, în cadrul unui grup, se bazează pe diverse criterii cum ar fi:

- reputația;
- competența;
- loialitatea;
- experiența;
- bunăvoința;
- curajul;
- etc.

Aceste caracteristici fac parte din bagajul comportamental, cu care vine sau pleacă un membru al unei organizații. Bineînțeles că acestea nu sunt fixe, ci ele evoluează odată cu timpul, odată cu interacțiunea cu ceilalți membri ai organizației și modul de participare la viața organizației. De asemenea, aceste criterii nu sunt identice pentru toate organizațiile. De exemplu, în timp ce unele dintre ele au nevoie de corectitudine, viteză de lucru, în dauna experienței și bunăvoinței, altele s-ar putea să ceară de la membrii lor loialitate și discreție. În funcție de cerințele impuse, criteriile necesare aplicării unei politici de încredere sunt adaptabile, fiecare organizație creându-și propriile principii și metode de evaluare și promovare a membrilor săi.

În cele ce urmează vom analiza un model teoretic de aplicabilitate și impunere a politicilor de acces bazate pe încredere.

Pentru a crea politici de control al accesului pentru utilizatorii unui spațiu virtual, trebuie să definim următoarele:

- Cerințele de evaluare;
- Obiectele;
- Grupul de obiecte;
- Ciclul de viață sau durata de existență a unui obiect;

- Utilizatori;
- Grupuri de utilizatori;
- Domeniile de activitate;
- Valorile de încredere, acordate, corespunzătoare unei acțiuni;
- Cerințele necesare pentru stabilirea nivelului de încredere;
- Nivelul de încredere acordat unui utilizator, pentru un anumit domeniu de activitate sau, pentru unul sau mai multe obiecte din domeniul de activitate;
- Nivelul de încredere acordat unui grup de utilizatori din cadrul unui grup ce activează într-un anumit domeniu de activitate.

Obiectul reprezintă o entitate omogenă și unitară de informație pe suport electronic, asupra căruia se desfășoară acțiunile în vederea realizării scopului pentru care a fost creat [16; 18].

Grupul de obiecte reprezintă o colecție de obiecte ce aparțin unui domeniu de activitate [16; 18].

În general, este dificil de identificat și stabilit că un obiect aparține strict unui grup sau altuia. Se poate întâlni situația când un obiect ar putea să aparțină mai multor domenii de activitate. Pentru o departajare ușoară a obiectelor pe grupuri, vom considera că obiectul aparține domeniului care are cele mai multe interacțiuni cu acesta și eventual se încheie ciclul de viață al obiectului [16; 18].

Grupurile de obiecte pot avea în interiorul lor o organizare ierarhică, adică unele obiecte iau naștere în urma încheierii ciclului de viață al altor obiecte [16; 18].

Ciclul de viață (durata de existență) a unui obiect reprezintă totalitatea etapelor parcurse de un obiect, de la creare până la arhivare sau ștergere [16; 18].

Utilizatorul este persoana care interacționează cu obiectele din cadrul unui domeniu, la care este autorizat să aibă acces, pe parcursul duratei lor de existență și, execută diverse acțiuni asupra acestora [16; 18].

Grupul de utilizatori este format din persoane care interacționează cu un set de obiecte din cadrul unui domeniu de activitate [16; 18].

Domeniul de activitate reprezintă o parte a activităților executate, grupate după caracteristici comune, cum ar fi: cunoștințe tehnice, economice sau științifice comune, interes comun, sferă de aplicare, etc. [16; 18].

Definiție: Numim *valoare de încredere* acordată unui proces, o valoare ce corespunde unui proces ce poate fi aplicat unui obiect [16; 18].

Cerințele necesare stabilirii valorii de încredere sunt un set de condiții pe care un utilizator trebuie să le îndeplinească pentru a căpăta un nivel de încredere în vederea executării unor acțiuni.

Definiție: Nivelul de încredere reprezintă permisiunea acordată unui utilizator sau grup de utilizatori de a interacționa cu un obiect sau mai multe obiecte dintr-un domeniu de activitate și de a executa anumite procese specifice corespunzătoare *valorii de încredere*.

Pentru a crea un mecanism logic de control al accesului la obiecte, vom formaliza principiile expuse anterior. Pentru aceasta, vom face următoarele considerații asupra elementelor cu care vom lucra.

Definim o *ierarhie parțial ordonată,* ca fiind un set finit de valori *(H1 ≤ H2)* ordonate în mod crescător.

Definim o *subierarhie parțial ordonată (I1 ≤ I2)*, ca un subset al unei ierarhii parțial ordonate *(H1 ≤ H2)*, dacă *(I1 ≤ I2) ⊆ (H1 ≤ H2)*.

Între obiecte și utilizatori există posibilitatea de interacțiune, adică un utilizator poate efectua anumite operații asupra unui obiect.

- Creare
- Citire
- Scriere (update)
- Adăugare (append)
- Copiere
- Redenumire
- Ștergere
- Arhivare
- Aprobare
- etc.

Interacțiunea dintre obiect și utilizator o denumim acțiune și o notăm cu a_i. Totalitatea acțiunilor creează mulțimea de acțiuni *A*.

Definim o *relație* [19] ca fiind o legătură ce există între două elemente *x* și *y* care aparțin unor mulțimi disjuncte și care poate fi exprimată sub forma *(r, x, y)*.

O *relație de încredere* este o relație care poate fi cuantificată prin diverse valori ce corespund nivelelor de la „neîncredere” (ex. no trust sau „0”) până la „încredere deplină” (ex. full trust sau „1”) [16; 18; 19].

Valorile pot fi exprimate numeric sau prin literali, iar plaja de valori numerice sau de literali poate fi stabilită arbitrar, la implementare.

În cazul în care *r* are valoarea minimă, între *x* și *y* nu există o relație de încredere, iar când *r* este maxim, încrederea este deplină. Între aceste valori ce reprezintă cele două extreme ale relației, pot fi definite diverse acțiuni ce se pot aplica elementelor, în funcție de valoarea relației

de încredere aplicată unui utilizator sau grup de utilizatori, pentru un element sau categorie de elemente [16; 18].

Definiție: Un proces p a lui x asupra lui y poate avea loc numai dacă valoarea relației de încredere r dintre x și y este egală sau mai mare decât valoarea minimă necesară pentru executarea procesului [16; 18].

Astfel, dacă $r=0 \vee r<v$ (v = valoarea minimă pentru care $\exists p$) $\Rightarrow \neg\exists p$, altfel $r \geq v \Rightarrow p$ [16; 18].

Prin urmare, controlul proceselor p se poate face funcție de valoarea atribuită lui r.

Dacă r are valoarea v egală sau mai mare decât minimul necesar pentru a executa un proces, atunci r poate corespunde tuturor proceselor a căror valoare este mai mare sau egală cu v. Dacă nici o valoare nu este setată pentru r, atunci se consideră că r=0 [16; 18].

În condițiile în care v=valoarea strictă pentru care $\exists p$ atunci dacă $r>v \Rightarrow \neg\exists p$, altfel $r \equiv v \Rightarrow p$. Deci acțiunea se poate executa numai dacă $r \equiv v$.

În prezenta lucrare considerăm relația ca fiind încrederea pe care o capătă un utilizator pentru a efectua o acțiune asupra unui obiect.

Un obiect sau grup de obiecte aparțin, în general, unui domeniu. În funcție de relația de încredere dintre un grup de utilizatori (sau un singur utilizator) ce aparțin unui domeniu și un obiect, se stabilesc acțiunile pe care aceștia (sau acesta) le pot aplica asupra obiectului. Din cele prezentate mai sus rezultă următoarele:

1. Fiecare obiect are atașat un grup de valori de încredere ce corespund unei ierarhii de acțiuni, ce reprezintă ordinea acțiunilor pe care la va suporta obiectul [16; 18];
2. Obiectul face parte dintr-un grup de obiecte care are o valoare de încredere atașată, valoare ce permite accesul la elementele grupului;
3. Fiecare utilizator face parte dintr-un grup de utilizatori, care are un nivel de încredere în cadrul organizației. Utilizatorul, la rândul său are un nivel de încredere, în cadrul grupului;
4. Fiecare utilizator are un nivel de încredere acordat în raport cu un obiect din grupul de obiecte la care are acces, în funcție de încrederea de care se bucură pentru efectuarea de acțiuni asupra unui obiect sau a grupului de obiecte [16; 18];
5. Dreptul de aplicare al unui proces asupra unui obiect este determinat de valoarea de încredere acordată [16; 18].

Accesarea unui obiect și aplicarea acțiunilor poate avea loc într-un context bine determinat, în care securitatea datelor și acțiunilor poate fi asigurată.

Definiție: Numim *context de încredere*, mediul și totalitatea atributelor lui, în care sunt accesate obiectele asupra cărora acționează un utilizator.

Mediul este format din: echipamentul cu care se face accesarea obiectelor, locația, rețeaua prin care se face transferul obiectelor, mediul de stocare, etc.

De aici se observă că se poate crea un prim set tupluri ce reprezintă legătura dintre grupuri de obiecte, grupuri de utilizatori și acțiuni, bazate pe nivelul de încredere, (*GO, D, G, R, C*) pe care o putem numi politică generală de încredere, unde:

- *GO* reprezintă grupul de obiecte;
- *D* reprezintă domeniul grupului de obiecte;
- *G* reprezintă grupul de utilizatori;
- *R* reprezintă nivelul de încredere al grupului;
- *C* reprezintă contextul de lucru al utilizatorului.

Fie un obiect O_i care aparține unui grup de obiecte GO_j dintr-un domeniu de activitate D_l. Un utilizator U_n din grupul G_m accesează obiectul O_i în contextul C_x. Acest utilizator are valoarea de încredere R_u, valoare care nu poate fi decât mai mare sau egală cu valoarea de încredere a grupului R_g. Acestea se transcriu sub forma:

$$R_g(GO_j,D_l,G_m,C_k) \leq R_u\ (O_i,D_l,U_n,C_x)$$

Dacă în relația de mai sus, la nivel de utilizatori și obiecte, se înlocuiește R_u cu procesul corespunzător, se obține următorul tuplu: O_i,D_l,U_x,P_k,C_k. Altfel spus, procesul P_x asupra obiectului O_i este permis pentru că utilizatorul U_n din domeniul D_l are nivelul de încredere R_u pentru contextul C_x care este egal cu nivelul de încredere ce îi permite executarea acțiunii.

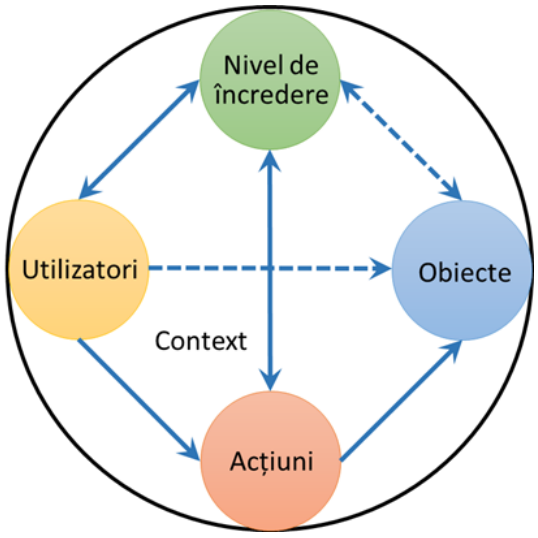


Figura 3.1. Relațiile între utilizator, nivel de încredere, acțiuni, obiecte

Această relație se poate prezenta grafic, ca în figura 3.1 de mai sus.

Pentru simplificarea acțiunilor permise unui utilizator asupra unui obiect într-un context dat, putem folosi numai tuplul (U_x ,P_k), procesele permise fiind cele care corespund nivelelor corespunzătoare de încredere. Aceasta conduce la atașarea unui grup de tupluri *U,P* la un obiect.

Etapele parcurse de un obiect vor fi înregistrate ca ierarhie de seturi de tupluri formată din acțiuni și o valoare întreagă ce poate exprima starea obiectului V_s (Valoare de stare).

Exprimarea unei politici de încredere aplicată asupra unui utilizator față de un anumit obiect ce aparține unui anumit domeniu, în formă simplificată, este de forma (O_i, U_x, P_k), iar în forma completă este (O_i, D_l, U_n, P_k, C_x).

Pot exista situații când drepturile unor grupuri de utilizatori ar putea să nu implice și existența unor acțiuni corespunzătoare atribuite unor utilizatori din grup. Atunci va trebui să instituim niște restricții [17].

Restricții: Numim restricție, limitarea acțiunii unui utilizator asupra unui obiect sau a unei categorii de obiecte, deși acestea aveau nivelul de încredere necesar executării unui proces[16; 18].

Pentru a desemna o restricție privind o acțiune, vom nota cu -P_k o restricție detaliată și cu -R_u ansamblul de politici restrictive. Astfel, avem un set de elemente (O_i, U_x, -P_k) sau (O_i, U_x, -R_u) pentru domeniul D_l.

În general, o restricție trebuie dublată de o delegare către un alt utilizator.

Delegarea este transferul de încredere efectuat de la un utilizator la altul în vederea realizării unor acțiuni asupra obiectelor.

Principiile de bază aplicate în politica de încredere sunt:

- *generalizarea* - permite ca politica de încredere față de un obiect sau categorie de obiecte aplicată unui utilizator să fie aplicată tuturor membrilor din grupul lui ce au același nivel de încredere. Putem spune că relația (O_i, U_n, R_u) dintr-un domeniu D_l se poate transforma în (GO_j, G_m, R_g) sau în (O_i, G_m, R_g) [16; 18];
- *moștenirea* - permite ca politica de încredere a unui grup să fie aplicată implicit unui membru al grupului dacă nu se specifică altfel. În acest caz, politica definită ca (O_i, GO_j, R_g) pentru domeniul D_l poate fi aplicată unui utilizator sub forma (O_i, U_x, P_k) [16; 18].

3.2. Modelarea fluxului de lucru – suport pentru implementarea politicilor bazate pe încredere

Crearea fluxului de lucru este foarte importantă în vederea simplificării implementării politicilor bazate pe încredere, prin relevarea proceselor *P*, fluxului proceselor și nivelurilor de încredere acordate unor diverși utilizatori.

Un obiect suferă pe parcursul duratei de viață, o serie de procese ordonate conform planificării create anterior. Fiecărui proces (*p*), îi corespund acțiuni (*A*), evenimente (*E*), secvențe de flux (*F*), ce determină semantica acestuia. Acestea sunt executate automat sau sunt lansate sau executate de utilizatori.

Fiecare proces are o poziție bine stabilită în fluxul de lucru al obiectului ceea ce ne permite posibilitatea de a realiza o ierarhie de procese, ce conțin la rândul lor ierarhii de acțiuni (A_k), una de evenimente (E_k) și secvențe de flux (F_k).

În cadrul stabilirii fluxului proceselor se determină restricțiile, delegările, nivelurile de încredere necesare grupurilor de utilizatori din diferite domenii pentru accesarea și interacțiunea cu obiectele.

3.2.1. Politici de control al accesului, și acțiunilor implementate pe durata fuxului de lucru

Proiectarea și implementarea politicilor bazate pe încredere presupune determinarea acțiunilor, evenimentelor, secvențelor de flux, ce constituie fiecare proces (*P*) și atribuirea lor utilizatorilor diverselor grupuri în funcție de nivelul lor de încredere și de restricțiile necesare a fi aplicate, într-un context determinat. Prin urmare, putem defini condițiile generale pentru a aplica o politică de încredere [16; 18]:

Fie $O_i \in GO \ \wedge p_k \in H(p)$ unde $H(p)=(p_1,p_2,..,p_k...p_n) \wedge \forall\ p_k=A_k \in H_k(A) \cup E_k \in H_k(E) \cup \sum F_k$ pentru $\forall p_k(O_i)$,

$\exists\ (U_k \in G_m \Rightarrow \exists\ R_u,\ R_u(U_k) \geq R_p(p_k(O_i)) \wedge R_u(U_k) = R_g)$ *sau*

$\exists\ (U_x \in G_m \Rightarrow \exists\ R_u,\ R_u(U_x) \geq R_u(U_k) \wedge \exists\ de_v(U_k)$ *pentru* $U_x)$ *sau*

$\exists\ (U_x \in G_m \Rightarrow \exists\ R_u,\ R_u(U_x) \geq R_u(U_k) \wedge \exists\ de_v(U_k),\ U_x \Rightarrow re_v(U_k) \in RE \wedge \neg \exists\ re_v(U_x) \in RE) \wedge \exists\ C_k \in C_x, \wedge R_g(G_m) \geq V(D_i) \Rightarrow \exists\ p_k\ (O_i)^{t_i}$,

unde:

A_k = o acțiune *k* aplicată unui obiect;

C_k = contextul de încredere *k*, pentru accesarea unui obiect și aplicarea unei acțiuni;

C_x = mulțimea de contexte în care pot fi accesate obiectele din grupul *GO*;

de_v = delegarea *v*, primită de la un utilizator oarecare U_k;

DE = mulțimea delegărilor;

D_i = domeniul căruia îi aparține GO;

F_k = secvențele de flux k (transfer de obiecte de la un utilizator la altul);

G_m = grupul de utilizatori din care face parte un utilizator oarecare U_k;

GO = grupul de obiecte;

$H(A)$ = ierarhie parțială de acțiuni corespunzătoare subprocesului p_k;

$H(E)$ = ierarhie parțială de evenimente;

O_i = Obiectul i;

$H(p)$ = ierarhie parțială de procese;

p_k = procesul k aplicat obiectului O_i prin intermediul unui utilizator U_k;

$p_1..p_n$ = mulțimea de procese ale O_i;

R_u = nivelul de încredere pentru user-ul U_k pentru accesarea obiectului O_i;

R_g = nivelul de încredere pentru grupul G_m pentru accesarea obiectului O_i;

R_p = valoarea de încredere necesară executării unui proces;

re_v = restricția aplicată unui utilizator;

RE = mulțimea de restricții;

t_i = momentul în care un procesul este aplicat unui obiect ($t_{i-1} \leq t_i \leq t_{i+1}$);

U_k = utilizatorul desemnat să execute o acțiune;

U_x = un utilizator oarecare ce aparține grupului G_m;

V = valoarea de încredere necesară a domeniului D_i;

$p_k(O_i)^{t_i}$ = procesul p_k aplicat obiectului O_i la momentul t_i.

Din cele prezentate mai sus rezultă următoarele:

- Pentru oricare obiect O_i ce aparține mulțimii de obiecte GO, există un utilizator ce aparține mulțimii de utilizatori G_m, pentru care nivelul de încredere pentru aplicarea unui proces p_k obiectului O_i este mai mare sau egală cu valoarea de încredere a obiectului ce suferă procesul aplicat într-un anumit context determinat. Utilizatorul este desemnat să execute procesul respectiv sau, face parte dintr-o listă de delegări în condițiile în care utilizatorului inițial desemnat i s-a aplicat o restricție;
- Orice obiect are atașată o ierarhie de procese pe care le poate suporta, iar fiecare proces este format dint-o ierarhie de acțiuni, o ierarhie de evenimente și o ierarhie de fluxuri de date;
- De asemenea, pentru acel obiect, există o ierarhie de utilizatori, ce pot executa procesele atașate obiectului, conform politicii de încredere desemnate.

Din punctul de vedere al modului de implementare, se pot realiza următoarele tipuri de politici:

- politici normale;
- politici stricte;
- politici hibride.

Politicile normale sunt politicile asociate unui obiect, ce permit oricărui utilizator care are o valoare de încredere mai mare sau egală cu nivelul de încredere necesar execuției unui proces, să-l execute.

Politicile stricte sunt politicile asociate unui obiect, prin care utilizatorii sunt restricționați în a executa numai procesele pentru care au valoarea de încredere egală cu nivelul de încredere asociat procesului.

Politicile hibride sunt politicile asociate unui obiect, ce permit aplicarea de politici normale și stricte.

Din punct de vedere al complexității politicilor create, avem următoarea clasificare:

- politici de control simple;
- politici de control derivate.

Numim o *politică de control simplă* a accesului bazat pe încredere, o politică ce nu presupune restricții și delegări ale unui utilizator în cadrul procesului de prelucrare a obiectelor. [16;18].

În principal, o astfel de politică se aplică în prima fază a creării unei organizații, când nu există un istoric al acțiunilor membrilor săi, nu au fost înregistrate evenimente care să perturbe organizația, iar membrii au fost integrați în organizație pe baza criteriilor cerute, aplicate în mod subiectiv, funcție de părerea formată, recomandarea primită, rezultatul obținut în urma unui interviu, propuneri, decizia inițială, etc.

O astfel de politică este cea care este aplicată în mod curent în organizație.

În activitatea ulterioară a organizației, pot apărea diverse evenimente, ce pot determina modificarea modului de implementare a politicilor de acces aplicate. Aceasta se va face prin analiza evenimentelor din cadrul organizației și ajustarea criteriilor de evaluare conform rezultatelor obținute.

Un exemplu de necesitate de modificare a politicilor implementate în cadrul organizației poate fi indisponibilitatea unui utilizator de a efectua diverse acțiuni necesare organizației la un moment dat.

Numim o *politică de control derivată* bazată pe încredere, o politică de tip general căreia i s-au aplicat restricții și delegări [16; 18].

Politicile derivate pot avea caracter temporar sau definitiv.

În cadrul unei organizații, simultan, pot exista atât politici simple cât și politici derivate. Aceste politici sunt aplicate obiectelor prin intermediul aplicațiilor, iar acțiunile și evenimentele ce apar sunt determinate de utilizatori de-a lungul procesului de lucru.

Din condițiile generale pentru a aplica o politică de încredere putem desprinde următoarele concluzii:

- Un obiect suportă un set de procese, ordonate pe baza unei ierarhii parțiale;
- Fiecare proces este executat la un moment t_i unde $t_{i-1} < t_i < t_{i=1}$ prin urmare ierarhia acțiunilor este dependentă de timp;
- Obiectul, după ce suportă un proces, își schimbă valoarea de încredere, prin urmare și utilizatorul care va putea să acționeze asupra lui va trebui să aibă un nivel de încredere corespunzător. Astfel, pentru obiect se creează un flux de lucru, corespunzător ierarhiei proceselor ce îi vor fi aplicate;
- Utilizatorii pot interveni în mod ordonat ierarhic pe parcursul proceselor pe care le suportă un obiect pe parcursul unui flux de lucru.

Definim *flux de lucru* totalitatea proceselor suportate de un obiect pe durata sa de viață, care corespund unei ierarhii de acțiuni întreprinse de o ierarhie de utilizatori.

Pentru ca unui obiect să i se poată aplica un proces, este necesar ca acesta să fie într-un anumit context de încredere.

Definim *contextul de lucru* ca fiind totalitatea elementelor de mediu, de situare geografică și securitate, necesare îndeplinirii acțiunii în bune condiții, ce nu vor putea afecta confidențialitatea, integritatea și disponibilitatea obiectului.

3.2.2. Crearea politicilor de control al accesului și acțiunilor bazate pe încredere

Din cele prezentate mai sus, aplicând condițiile generale pentru a aplica o politică de încredere, pentru a scrie o serie de politici de control al accesului într-un sistem informatic, avem nevoie de următoarele componente:

- ti = momentul în care are loc procesul, $i \in [1,n) \wedge ti < ti_{+1}$
- $C_x i$ = contextul de lucru de la momentul ti.
- O_i = obiectul asupra căruia se aplică procesul.
- D_i = domeniul căruia îi aparține obiectul.
- $U_x i$ = utilizatorul ce are acces la domeniu, ca aparține unei ierarhii parțiale și este membru al grupului G_m
- $p_k i$ = procesul ce se aplică obiectului, la momentul t_i și aparține unei ierarhii parțiale de procese ce se aplică obiectului

- $re_v i$ = restricția ce se aplică utilizatorului $U_x i$ la momentul t_i pentru procesul $p_k i$
- $de_v i$ = delegarea ce se aplică utilizatorului $U_x i$ la momentul t_i pentru procesul p_ki
- $M(O_i)$ = matricea de politici de control al accesului și acțiunilor ordonate temporal și aplicate obiectului *Oi;*
- V =v aloarea de încredere necesară a domeniului D;
- Rg = Nivelul de încredere al grupului de utilizatori $G_{m.}$

Putem descrie o politică de control al accesului și acțiunilor bazată pe încredere prin următoarea matrice de n-tupluri:

$$M(O_i) = \left\| \begin{matrix} \dots & t1, U_x 1, p_{k1}, re_v 1, de_v 1, & C_x 1 & \dots \\ & tn, U_x n, p_{kn}, re_v n, de_v n, & C_x n & \end{matrix} \right\|,$$

cu condiția ca $R_g(G_m) \geq V(D_i)$

3.3. Asigurarea confidențialității și integrității datelor prin intermediul politicilor de control al accesului și acțiunilor bazate pe încredere

Asigurarea securității și confidențialității datelor, reprezintă o cerință din ce în ce mai importantă, în ultimele decenii. În cele ce urmează, vom arăta cum politicile de control al accesului și acțiunilor bazate pe încredere pot modela politicile de securitate Bell-LaPadula și politicile de integritate Biba.

3.3.1. Utilizarea încrederii în modelarea politicilor de confidențialitate Biba

Aplicarea politicilor de control al accesului și acțiunilor bazate pe încredere permite asigurarea confidențialității și respectarea cerințelor de integritate de bază Biba, oricărui utilizator ce accesează un obiect la un moment dat *t*, astfel:

- Starea de integritate simplă

  $s \in S$ poate observa $o \in O$, dacă și numai dacă $i(s) \leq i(o)$.

  Comentariu

Din condițiile generale pentru a aplica o politică de încredere, pentru $\forall U_x \Rightarrow \exists\ p_k(O_i)$ dacă $R_u(U_k) = R_p(P_k)$,

unde:

- U_x =s;
- $Gm = S$;
- $R_u(U_k) = i(s)$;
- $R_p(p_k) = i(o)$;
- $O_i = o$;
- GO = O;

- p_k = *procesul k.*

- Proprietatea de integritate stea *

  $s \in S$ poate modifica $o \in O$, dacă și numai dacă $i\,(o) \leq i\,(s)$.

  Comentariu

  Condițiile generale pentru a aplica o politică de încredere impun că $\exists\ p_k(O_i)$ pentru U_x dacă $R_u(U_k)=R_p(p_k)$

- Invocarea proprietății

  $s_1 \in S$ poate invoca $s_2 \in S$ dacă și numai dacă $i\,(s_2) \leq i\,(s_1)$.

Nici un utilizator cu $R_u(U_k)$ mai mic nu poate accesa obiectele pe care le accesează un utilizator cu $R_u(U_k)$.

Prin restricțiile aplicate politicilor, funcție de nivelul de încredere care pentru unele aplicații poate fi considerat drept nivel de autorizare, se pot modela politici de tip MAC, relaxând politicile și permițând utilizatorilor să-și modeleze propriile politici pentru anumite aplicații colaborative, modelându-se politici de tip DAC.

3.3.2. Aplicații, utilizatori, obiecte

Crearea politicilor de control al accesului și acțiunilor utilizatorilor permite un control mult mai amplu al aplicațiilor, prin restricționarea accesului și acțiunilor utilizatorilor asupra obiectelor din cadrul aplicaților.

Procesele pe care le suportă un obiect sunt parte a aplicațiilor proiectate, ce sunt lansate sau planificate să se lanseze automat de către utilizatori.

Definim o *aplicație* ca fiind un set de procese proiectate pentru a fi aplicate de un utilizator sau grup de utilizatori, asupra unui obiect sau un grup de obiecte.

Un obiect sau un grup de obiecte care nu suportă un proces este considerat stocat sau arhivat.

Orice obiect (grup de obiecte) aparține unui domeniu care este atașat unui grup de utilizatori specifici. Dar și alte grupuri de utilizatori, din alte domenii de activitate, pot avea acces la obiecte sau grupuri de obiecte din domeniu, pe o durată mai scurtă de timp sau pe termen nelimitat, în funcție de politica de încredere.

În funcție de politica de încredere, utilizatorilor ce nu aparțin domeniului corespunzător grupului de obiecte, li se poate acorda un nivel diferit de încredere, necesar efectuării de acțiuni de consultare, creare sau modificare a acestora.

Pentru exemplificarea modului de aplicare a unui standard de modelare a proceselor de lucru, în cele ce urmează vom prezenta modelul de elaborare a analizei proceselor la care sunt

supuse obiectele în vederea determinării acțiunilor, evenimentelor și a „stack flow”-ului, necesare pentru modelarea controlului accesului.

În prima etapă, cunoscându-se organizarea internă, este necesar a se face o inventariere a tuturor obiectelor ce sunt supuse diverselor procese din cadrul unei organizații.

Ca o primă măsură de sistematizare a efortului de analiză, este necesar:

- să se grupeze obiectele în funcție de domeniul de activitate corespunzător;
- să se stabilească obiectele aspra cărora se acționează;
- să se stabilească ierarhia de obiecte;
- să se stabilească procesele ce acționează asupra obiectelor;
- să se determine ordinea lor, creând ierarhia de procese;
- să se atribuie utilizatorilor ce interacționează cu obiectele valorile de încredere necesare accesării proceselor asupra obiectelor.

Ca exemplu vom prezenta un sistem informatic de acordare și evidență a concediilor de odihnă a personalului [15]. Aplicația, care aparține domeniului „personal” și permite fiecărui membru al organizației să creeze o cerere de concediu de odihnă, deși acesta, ca utilizator, nu aparține domeniului „personal” și va crea astfel începutul unui flux informațional.

Răspunsul la cerere aparține de asemenea utilizatorilor care au formulat cererea, deși datele vor fi arhivate de utilizatorii domeniului „personal”. Utilizatorii din cadrul domeniului „personal” vor completa datele privind drepturile pe care le au solicitanții, drepturi care se referă la zilele de odihnă și valoarea drepturilor bănești pe perioada solicitată.

În cadrul sistemului informatic creat, subiecții (utilizatorii) din cadrul domeniului „financiar-contabil”, sunt cei care vor completa datele pentru plata prin bancă sau casierie a drepturilor financiare pentru concediul de odihnă. Bineînțeles că nu orice subiect (utilizator) din domeniul financiar-contabil va avea acces la date și le va putea completa, ci numai aceia care au fost investiți cu nivelul de încredere ce permite acțiunea respectivă.

Fiecare subiect (utilizator) va exercita drepturile care-i revin din politica de încredere. Propunerea spre aprobare ține de competența șefilor solicitantului iar managerul organizației decide aprobarea sau nu a solicitării.

Pentru realizarea sistemului vom etapiza activitatea de proiectare a acestuia.

În prima etapă vom analiza acțiunile utilizatorilor și vom crea fluxul de lucru inițial.

Din cele prezentate rezultă o secvență de acțiuni ordonate care sunt parte a proceselor derulate pe parcursul fluxului de lucru, ce pot fi introduse într-un tabel (tabelul 3.1) pentru o mai bună vizualizare [15].

Din analiza acestui tabel, observăm o primă succesiune de acțiuni, pe care o putem transpune într-un flux de lucru.

Tabelul 3.1. Acțiunile ordonate

Nr. etapa	Activitate	Stare aplicație	Locații	Actor
1	Completare cerere de concediu odihnă	Indecisă	Loc de muncă	Angajat aplicant
2	Completare punct de vedere manager angajat	Indecisă	Management loc munca angajat	Manager angajat aplicant
3	Înregistrare cerere	Indecisă	Registratură	Angajat registratură (secretariat)
4	Verificare drepturi de concediu de odihnă	Indecisă	Resurse Umane (evidență personal)	Resurse Umane (evidență personal)
5	Completare număr zile concediu de odihnă la care are drept angajatul, numărul de zile de concediu efectuate și numărul de zile rămase de efectuat.	Indecisă	Resurse Umane (evidență personal)	Resurse Umane (evidență personal)
6	Validare dare	Indecisă	Management Resurse Umane	Manager
7	Aprobare/Respingere concediu de odihnă	Indecisă	Management întreprindere	Manager general (Director general)
8	Înregistrare soluție cerere	Aprobat/ Refuzat	Registratură	Angajat registratură (secretariat)
9	Primire soluționare cerere	Aprobat/ Refuzat	Registratură	Angajat aplicant
10	Primire soluționare cerere	Aprobat/ Refuzat	Resurse Umane	Manager Resurse Umane
11	Înregistrare concediu odihnă,	Cerere aprobată	Personal - salarizare	Angajat personal (evidență personal)
12	Arhivare cerere concediu odihnă	Cerere aprobată	Resurse Umane	Resurse Umane (evidență personal)
13	Completare venit brut angajat	Cerere aprobată	Resurse Umane (salarizare)	Resurse Umane (salarizare)
14	Calculare indemnizație concediu odihnă	Cerere aprobată	Resurse Umane	Resurse Umane (salarizare)
15	Înștiințare Contabilitate	Cerere aprobată	Resurse Umane	Resurse Umane (salarizare)
16	Aprobare plată indemnizație	Cerere aprobată	Contabilitate	Manager contabilitate
17	Ordin de plată bancă	Cerere aprobată	Contabilitate	Angajat contabilitate

Aplicațiile nu sunt proiectate, în general, pentru a executa un singur proces, ci sunt proiectate modular, pentru a permite execuția unui set de procese asupra unui set de obiecte. Acest lucru permite ca mai mulți utilizatori să poată folosi aceeași aplicație instalată, dar fiecare să execute module diferite, conform politicilor de încredere create pentru fiecare utilizator în parte.

Următoarea etapă în analiza sistemului manual de aprobare/respingere a cererii va fi crearea fluxului de lucru rezultant.

- cererea de concediu de odihnă, ce conține datele de identificare ale aplicantului (nume, prenume, loc de muncă), numărul de zile solicitat, data de la care se solicită, și data de sfârșit a concediului;
- punctul de vedere al managerului locului de muncă; datele de certificare ale dreptului de repaos solicitate, completate și validate de departamentul de resurse umane;
- aprobarea managerului general;
- valoarea de plată;
- înștiințare contabilitate;
- aprobare plată;
- ordin de plată bancar.

În cadrul aplicației avem următoarele obiecte:

- obiectul „cerere” care are ca elemente datele de identificare și punctul de vedere al managerului locului de muncă, aparține grupului general „Organizație”;
- obiectele „validare date”, „înștiințare contabilitate” și „înștiințare aplicant” aparțin grupului „Resurse umane”;
- obiectul „aprobare” aparține managementului organizației;
- obiectul „ordin de plată bancar” aparține grupului „Contabilitate”.

Ierarhia de obiecte este următoarea:

- cerere;
- date validate;
- decizie aprobare;
- înștiințare aplicant;
- valoare drepturi bănești;
- înștiințare contabilitate;
- ordin plată.

Fluxul de lucru și procesele corespunzătoare se regăsesc în tabelul 3.2, sintetizate pe fiecare utilizator în parte [15].

Din Tabelul 3.2 și Figura 3.2 observăm că același actor, pe parcursul fluxului de procesare a datelor, îndeplinește mai multe sarcini.

Ulterior etapelor de analiză a procedurilor manuale, le vom optimiza, vom proiecta un nou flux de lucru, vom crea o nouă sinteză a acțiunilor utilizatorilor în urma cărora vom obține ierarhiile de acțiuni pentru utilizatori și documente.

În etapa a 2-a vom proiecta sistemului informatic și optimiza fluxul de lucru

Pentru crearea sistemului informatic vom elimina procedurile manuale nenecesare și vom optimiza restul procedurilor, pe care le vom automatiza [15].

Tabelul 3.2. Sinteza activităților utilizatorilor

Actor	Etapa în care intervine	Locație	Activitate
Angajat aplicant	1,9	Loc muncă	Creare cerere
Manager aplicant	2	Loc muncă	Completare cerere,
Angajat registratură	3,8	Registratură	Înregistrare cerere
Angajat personal evidență personal	4,5,11,12	Personal	Verificare, completare date, înregistrare, arhivare
Angajat personal salarizare	14,15	Personal	Calcul îndemnizație, informare contabilitate
Manager personal	6,10	Personal	Recepție cerere, validare date
Manager general	7	Management întreprindere	Aprobare
Manager contabilitate	16	Financiar-Contabilitate	Aprobare plată indemnizație
Angajat contabilitate	17	Financiar-Contabilitate	Completare ordin plată

Din tabelul 3.3, în primă fază, vom elimina locația „Registratură” și procedurile corespunzătoare ei, acestea fiind preluate de sistemul informatic nou creat. De asemenea vom renunța la procedura de verificare a documentelor privind evidența concediului de odihnă, creând o procedură automată pentru aceasta.

Vom păstra validarea datelor de către managerul compartimentului personal. De asemenea, considerăm nenecesare:

- înregistrarea cererii de concediu;
- arhivarea cererii de concediu;
- completarea venitului brut;
- înștiințarea serviciului „Contabilitate” – aceasta se va face prin intermediul sistemului informatic;
- aprobarea plății indemnizației de concediu.

Urmare a optimizării procedurilor și înregistrării acestora în Tabelul 3.4, vom trece la pasul următor și vom proiecta fluxul de lucru corespunzător sistemului informatic. Acest flux este prezentat în Figura 3.3, iar sinteza acestuia nu mai este necesară întrucât Tabelul 3.3 prezintă atât procedurile simplificate cât și ordinea acestora.

În etapa a 3-a vom trata excepțiile din cadrul sistemului informatic [15].

Pentru început, analizăm persoanele care intervin pe parcursul fluxului de lucru, iar dintre acestea, cele care au și rol decizional

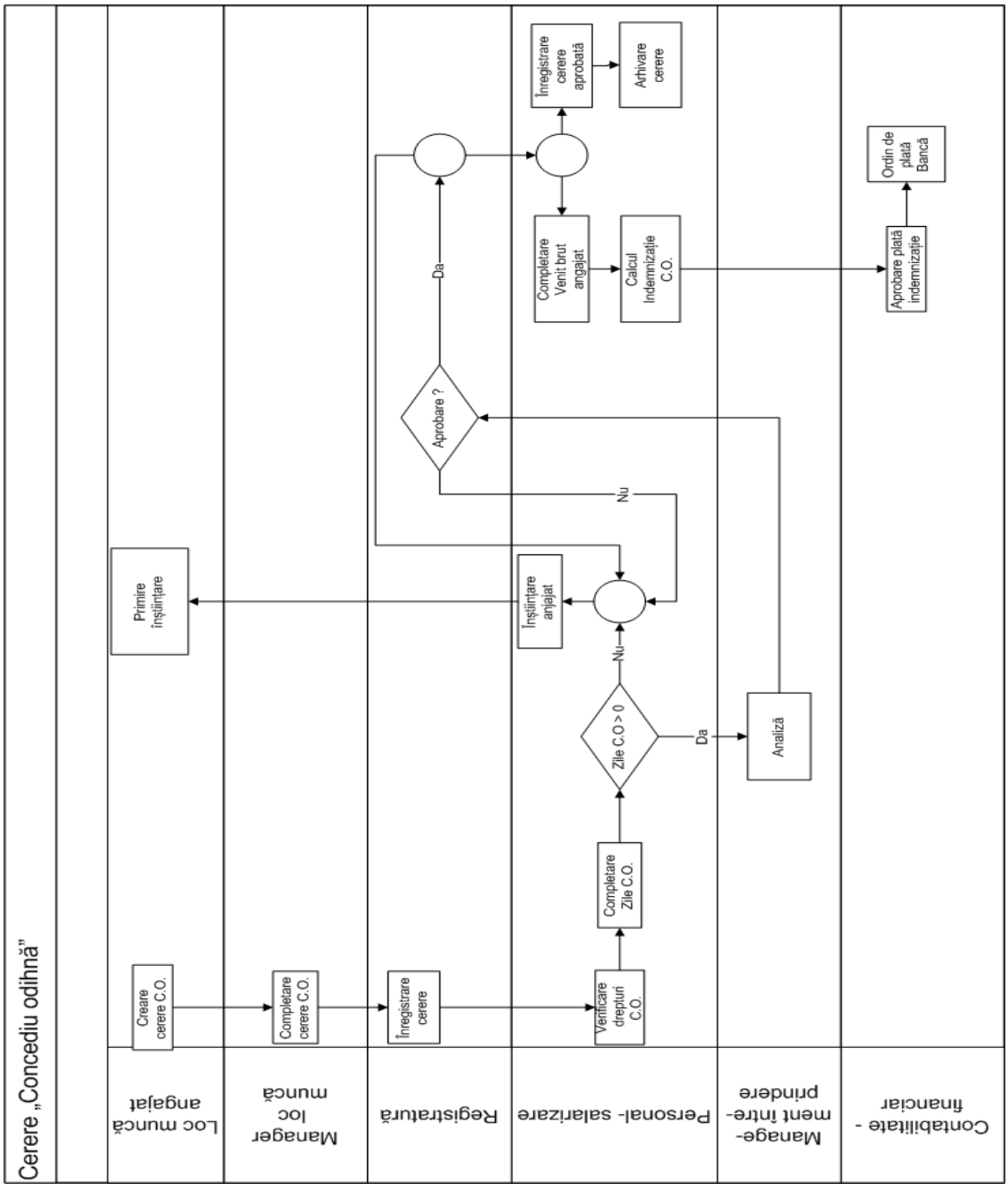


Figura 3.2. Fluxul de lucru pe durata unei aplicații de concediu de odihnă

Excepțiile pot apărea atunci când o persoană ce intervine în cadrul fluxului de lucru este cea care inițiază o cerere de concediu de odihnă.

În Etapa 4 -a vom crea ierarhiile de procese atașate documentului În această etapă se analizează și se stabilesc restricțiile și delegările de acțiuni ale utilizatorilor. Din Tabelul 3.4 se extrag elementele necesare creării ierarhiilor de procese ale sistemului informatic, care permit alocarea acestora actorilor implicați, la care se adaugă delegările de competențe și restricțiile. Odată ce au fost create ierarhiile proceselor, se pot crea politicile pentru obiectul nou creat. Aceasta presupune că, pentru aplicația nou creată O_i, se creează o ierarhie de procese permise $H_k(p_k)$, o ierarhie de acțiuni care sunt atribuite unor utilizatori din cadrul întreprinderii și care sunt organizați într-o o ierarhie Hg(Gm).

Tabelul 3.3. Acțiunile prin intermediul sistemului informatic

Nr. etapa	Activitate	Stare aplicație angajat	Locații	Actor
1	Completare cerere de concediu de odihnă	Indecisă	Loc de muncă	Angajat aplicant
2	Completare punct de vedere manager	Indecisă	Management loc munca angajat	Manager angajat aplicant
3	Completare nr. zile concediu de odihnă la care are dreptul, nr. zile C.O. efectuate, nr. zile C.O. rămase de efectuat.	Indecisă	Personal salarizare (personal)	Angajat personal (evidență personal)
4	Validare date, înaintare cerere conducere sau aplicant	Indecisă	Management personal	Manager personal
5	Aprobare/Respingere concediu de odihnă	Indecisă	Management întreprindere	Manager general (Director general)
6	Înștiințare soluționare cerere/ Înștiințare angajat personal	Aprobat/Respins	Loc de muncă / Personal	manager personal
7	Înregistrare concediu odihnă aprobat	Cerere aprobată	Personal - salarizare	Angajat personal (evidență personal)
8	Calculare indemnizație concediu odihnă	Cerere aprobată	Personal - salarizare	Angajat personal (salarizare)
9	Ordin de plată bancă	Cerere aprobată	Contabilitate	Angajat contabilitate

Ierarhia de procese permise creată $H_k(p_k)$ este:

p_1 = completare cerere, trimitere cerere manager angajat;

p_2 = completare punct de vedere manager, trimitere personal;

p_3 = completare date, înaintare manager personal;

p_4 = validare date, înaintare manager general sau înștiințare imposibilitate concediu de odihnă;

p_5 = aprobare/respingere, trimitere rezoluție compartiment personal, creare înștiințare;

p_6 = trimitere înștiințare către angajat aplicant, trimitere către personal responsabil evidență concedii;

p_7= înregistrare concediu;

p_8= calcul indemnizație, trimitere înștiințare contabilitate;

p_9 = completare ordin bancă, actualizare date contabile, transmitere ordin bancă.

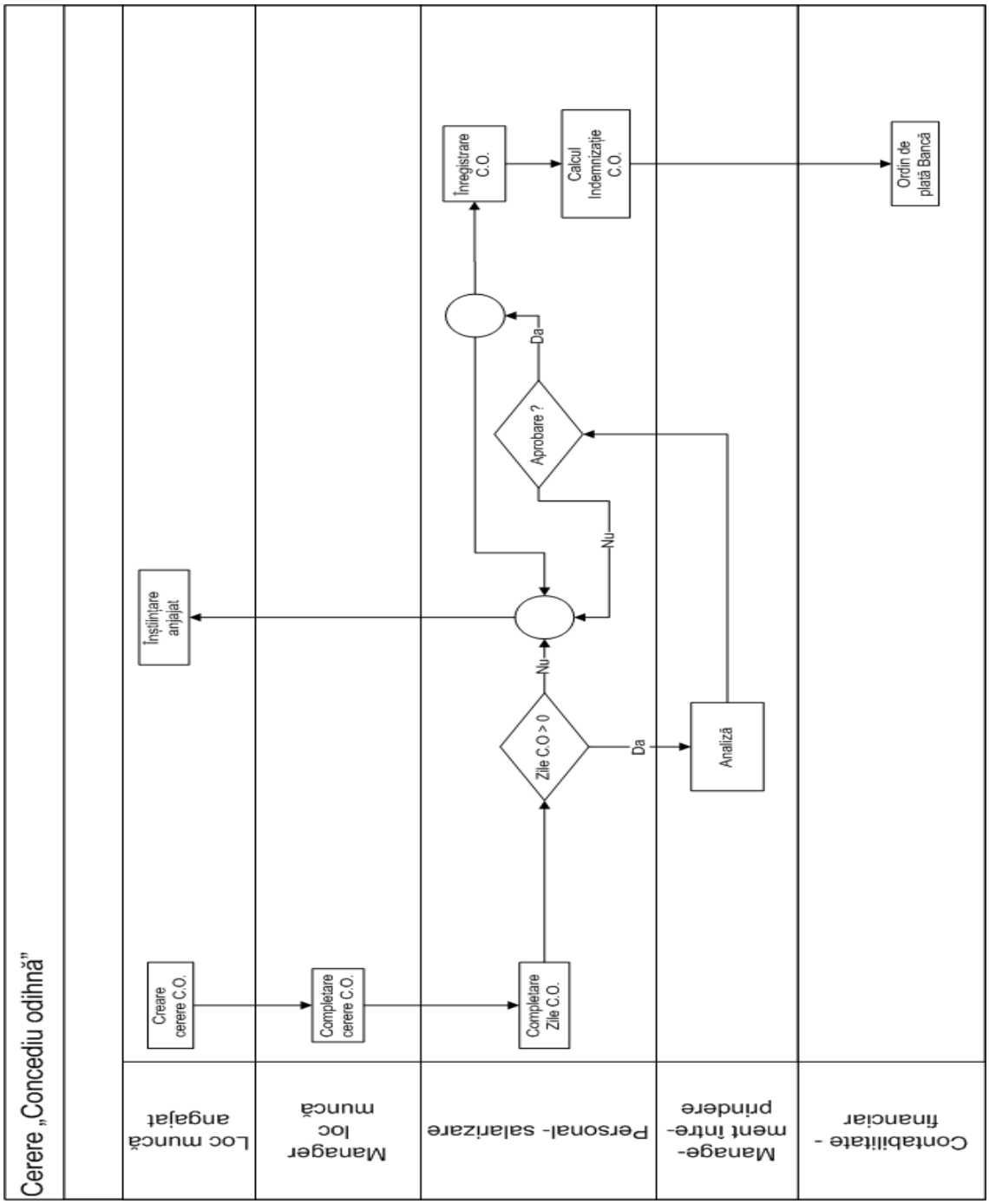


Figura 3.3. Fluxul sistemului informatic nou proiectat

La aceste acțiuni adăugăm condițiile de restricție $re_1...re_7 \in RE(Oi)$ și delegările $de_1..de_v7 \in DE(Oi)$ stabilite în tabelul 3.4.

Stabilim grupul de utilizatori Gm format din $U_1,U_2,U_3,U_4,U_5,U_6,U_7,U_8,U_9,U_{10}$ utilizatori, care au următoarele poziții în cadrul organizației:

- U_1 = angajat întreprindere;
- U_2 = manager angajat;
- U_3 = angajat personal (evidență personal);
- U_4 = manager personal;
- U_5 = manager general;
- U_6 = angajat personal (salarizare);
- U_7 = angajat contabilitate (ordine banca);
- U_8 = manager contabilitate;
- U_9 = delegat manager general;
- U_{10} = angajat contabilitate.

Acum putem construi matricea politicilor de control al accesului și acțiunilor necesare aplicației, conform condițiilor generale pentru a aplica o politică de încredere.

Aceasta va arăta astfel:

1,	U_1,	p_1,	re_1,	de_1	C_1
2,	U_2,	p_2,	re_2,	de_2	C_2
3,	U_3,	p_3,	re_3,	de_3	C_3
4,	U_4,	p_4,	re_4,	de_4	C_4
5,	U_5,	p_5,	re_5,	de_5	C_5
6,	U_6,	p_6,	re_6,	de_6	C_6
7,	U_7,	p_7,	re_7,	de_7	C_7
8,	U_8,	p_8,	re_8,	de_8	C_8
9,	U_9,	p_9,	re_9,	de_9	C_9

Pe lângă matricea de procese, trebuie construită matricea de restricții și delegații pentru tratarea eventualelor excepții.

U_3	U_x	p_3
U_4	U_y	p_4
U_5	U_z	p_5
U_6	U_u	p_6
U_3	U_x	p_7
U_8	U_v	p_8
U_9	U_w	p_9

Odată create aceste politici, vor fi înregistrate și implementate pentru a fi aplicate pe durata fluxului de lucru aplicat cererii angajatului.

Tabelul 3.4. Restricții și delegări

Nr. etapa	Activitate	Actor inițial	Condiție excepție	Restricție	Delegare	Actor delegat
3	Completare nr. zile C.O total, nr. zile C.O. efectuate, nr. zile C.O. rămase	Angajat personal (evidență personal)	Concediu odihnă, Concediu medical, Personal lipsă (neangajat, alte situații)	Da	Da	Utilizator desemnat de managementul unității (angajat personal – evidentă personal sau contabilitate)
4	Validare date	Manager personal	Concediu odihnă, Concediu medical, Personal lipsă (neangajat, delegații, alte situații)	Da	Da	Utilizator desemnat de managementul unității (angajat personal sau responsabil compartiment contabilitate)
5	Aprobare/Respingere concediu de odihnă	Manager general (Director general)	Concediu odihnă, Concediu medical, alte situații	Da	Da	Utilizator desemnat de managementul unității (persoana desemnată de managerul unității)
6	Înștiințare soluționare cerere	Manager personal	Concediu odihnă, Concediu medical, delegații, alte situații	Da	Da	Utilizator desemnat de managementul unității (angajat personal sau responsabil compartiment contabilitate)
7	Înregistrare concediu odihnă aprobat	Angajat personal (evidență personal)	Concediu odihnă, Concediu medical, Personal lipsă (neangajat, delegații, alte situații)	Da	Da	Utilizator desemnat de managementul unității (angajat personal sau responsabil compartiment contabilitate)
8	Calculare indemnizație concediu odihnă	Angajat personal (salarizare)	Concediu odihnă, Concediu medical, Personal lipsă (neangajat, delegații, alte situații)	Da	Da	Utilizator desemnat de managementul unității (personal contabilitate, sau manager personal, persoană)
9	Ordin de plată bancă	Angajat contabilitate	Concediu odihnă, Concediu medical, Personal lipsă (neangajat, delegații, alte situații)	Da	Da	Utilizator desemnat de managementul unității (personal contabilitate ce înlocuiește persoana lipsă sau manager compartiment)

3.4. Concluzii la capitolul 3

Pentru utilizarea încrederii la crearea politicilor de control al accesului și integrității datelor și informațiilor, este necesar a fi definite elementele care concură la realizarea acestor politici.

Determinarea obiectelor, a grupurilor de obiecte din care fac parte, a subiecților și a contextului în care acestea interacționează, reprezintă un prim pas în analiza în vederea asigurarea securității

Aceste politici trebuie să respecte diverse condiții pentru controlul accesului la procesele aplicate obiectelor și grupurilor din care fac parte. Pentru aceasta, este necesar a stabili valoarea de încredere atribuită unui obiect ce aparține unui grup de obiecte și, nivelul de încrederea atribuit unui utilizator. De asemenea este necesar a se stabili eventualele restricții și delegări.

În cadrul procesului de proiectare și implementare a politicilor de control al accesului și integrității un element important, este fluxul de lucru Determinarea acestuia și eventual optimizarea lui, ajută la realizarea politicilor, prin construirea matricelor de acces la procese le ce pot fi aplicate obiectelor, cât și matricele de restricții și de delegări..

4. MODELAREA CONTROLULUI ACCESULUI ȘI ACȚIUNILOR BAZATE PE ÎNCREDERE,PRIN INTERMEDIUL TEHNOLOGIILOR XML

Crearea și implementarea politicilor de control al accesului și acțiunilor bazate pe încredere reprezintă o sarcină relativ complexă. Realizarea și utilizarea acestor politici solicită un efort considerabil, asigurând un control de o granularitate deosebită asupra acțiunilor utilizatorilor. Pentru faptul că fiecare aplicație este unică, nu se poate crea o structură unitară de stocare și regăsire a informațiilor necesare aplicărilor acestor politici. Prin urmare, pentru realizarea acestora s-a utilizat aplicarea tehnologiile *xml*, întrucât acestea au cea mai mare flexibilitate în modelarea și stocarea datelor.

În continuare, se vor relua exemplele discutate anterior și, se vor crea modelele de implementare a politicilor de control al accesului și acțiunilor bazate pe încredere.

4.1. Exemplu de proiectare a unui sistem informatic utilizând controlul accesului și acțiunilor utilizatorilor pentru o clinică medicală. Proiectarea sistemului informațional

În capitolul 2 subcapitolul 2.5.2 s-au prezentat procesele aplicate pe parcursul unei consultații ale unui pacient.

Datele de identificare ale pacienților sunt date confidențiale, aplicându-se în cazul lor legislația privind G.D.P.R. De asemenea, datele medicale sunt date confidențiale, date ce țin de relația pacient-medic și legislația G.D.P.R.

În cadrul acestui exemplu, presupunem că este necesară o a doua părere a unui medic privind diagnosticul pacientului. Acest medic nu aparține clinicii unde se desfășoară consultația, iar fișa cu datele de identificare ale pacientului nu poate fi accesată din afara unității medicale. Prin urmare, datele de identificare ale pacientului nu pot fi transmise medicului extern, acesta având acces doar la datele privind istoricul medical, anamneza, analizele medicale și diagnosticul prezumtiv.

În primă instanță, se va folosi ca punct de pornire datele de identificare ale pacientului: sex, vârstă, profesie, loc de muncă. Pentru datele medicale se vor completa antecedentele heredo-colaterale și istoricul personal. Se completează datele medicale cu anamneza, măsurătorile necesare și controalele ce se pot efectua în cabinet, după care pe baza unui diagnostic prezumtiv, se cere eventual efectuarea de analize suplimentare. După parcurgerea pașilor mai sus prezentați se cere părerea unui medic extern privind diagnosticul final. Pentru diagnosticul final, medicul extern are nevoie de datele medicale, fără datele de identificare.

În tabelele din 2.5.5 s-au prezentat pe scurt actorii, obiectele și procesele suportate de obiecte. În capitolul 3.3.2 s-a prezentat construirea ierarhiilor de procese pe baza fluxului de lucru. În continuare se va demonstra cum construim un model teoretic bazată pe cele prezentate anterior, urmând pașii de mai jos:

1. stabilirea *scopului modelului*;

2. stabilirea *domeniilor* din cadrul organizației, ce concură la realizarea serviciului;

3. stabilirea *grupurilor de obiecte* din cadrul documentelor, care sunt create/modificate și căror domenii le aparțin;

4. stabilirea *proceselor* suportate de grupurile de obiecte și fluxul de lucru;

5. *proiectarea obiectelor*;

6. utilizarea tehnologiei *xml* pentru implementarea politicilor bazate pe încredere.

În următoarele rânduri vom face o descriere a celor expuse mai sus, având ca bază exemplul dat.

1. *Scopul exemplului* este *modelarea* unui sistem informatic pentru planificarea, consultarea și evidența pacienților.

Se va face o prezentare a datelor principale utilizate, apartenența la diverse domenii și repartizarea lor pe grupuri de lucru.

2. *Domeniile* participante sunt:

- evidență pacienți-consultații;
- medical:
  - consultații medici;
  - laborator.
- farmacie – eliberare tratamente;
- financiar-contabil – evidența contabilă a prestărilor medicale și a tratamentelor eliberate.

3. *Documentele* care se creează/actualizează sunt:

- registrul de evidență și planificare consultații;
- fișele medicale;
- registrul evidențe servicii medicale;
- trimiteri analize;
- rezultate analize;
- trimiteri consultații specialitate;
- rețete, prescripții medicale;
- evidență tratamente eliberate;
- scrisori medicale;

1. chitanțe, facturi.

Din cele arătate anterior, cât și în tabelele din capitolul 3.2 putem atribui documentele domeniilor participante, prezentate mai sus.

Pentru o mai ușoară sistematizare vom utiliza o prezentare tabelară.

Din tabelul 4.1 putem observa că unele documente aparțin unui singur domeniu în timp ce alte documente care aparțin mai multor domenii. În cazul celor din a doua categorie, în cadrul fiecărui domeniu sunt accesate sau adăugate/modificate alte seturi de date. Astfel, datele privind identificarea pacienților, deși sunt comune mai multor domenii fiind înregistrate în mai multe documente (registrul de evidență și planificare consultații, fișa medicală, analize trimiteri, rezultate analize, registrul de evidențe servicii medicale, rețete, prescripții medicale, scrisori, medicale, chitanțe și facturi), nu sunt la fel de detaliate în toate documentele, întrucât nu este necesară completarea lor în toate aceste documente și, pe de altă parte, unele dintre categoriile de utilizatori din domeniile de mai sus nu au acces la toate informațiile

Tabelul 4.1. Relația dintre documente și domenii

Document	Domeniu
Registrul de evidență și planificare consultații	Evidență pacienți-consultații
Fișa medicală,	Evidență pacienți-consultații
	Medical - medici
Analize trimiteri	Medical – medici, laborator
Rezultate analize	
Registru analize medicale	Medical – medici, laborator, financiar – contabil
Registrul consultații medicale	Medical - medici, laborator Financiar - contabil
Rețete, prescripții medicale	Medical - medici, Farmacie, Financiar - contabil
Scrisori medicale	Medical - medici
Evidențe medicamente eliberate	Farmacie Financiar - contabil
Chitanțe, facturi	Financiar - contabil

Datele complete de identificare ale unui subiect cuprind: *prenume, nume, vârstă, sex, adresa, profesia, loc de muncă, categorie de beneficiar al serviciilor medicale*.

Pentru toate domeniile mai sus enunțate, sunt necesare datele despre: *prenume*, *nume*, *vârstă*, *sex*. Dar, pentru domeniile: *farmacie, laborator* și *financiar contabil*, datele: *locul de muncă, profesia* și *adresa* nu sunt necesare și, nici disponibile.

Datele privind: *istoricul medical, istoricul heredo-colateral, anamneza, diagnosticul prezumtiv, diagnosticul final* nu sunt disponibile pentru domeniile: *evidență pacienți-consultații, financiar-contabil*.

Datele privind *diagnosticul prezumtiv* sunt accesibile laboratorului, iar datele privind *diagnosticul final* sunt accesibile farmaciei.

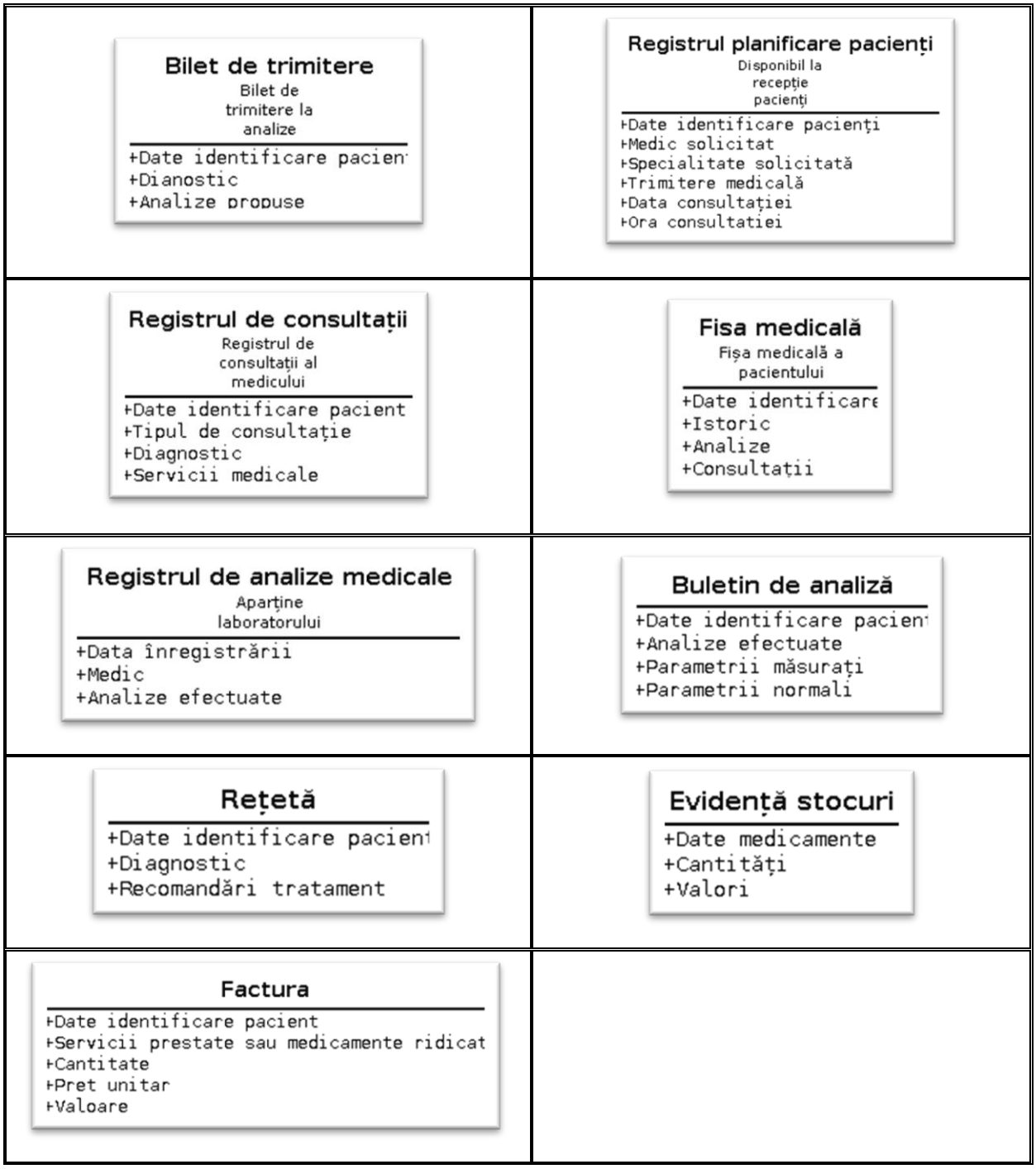


Figura 4.1. Structura generală a macro obiectelor implicate în procesul consultației pacientului

Datele privind *rezultatele analizelor* sunt necesare medicului și pacientului.

Recomandările privind medicația sunt disponibile domeniilor*: medical, farmacie, financiar-contabil*, dar pentru fiecare domeniu sunt disponibile alte elemente. Astfel, prețurile medicamentelor nu sunt importante pentru medic, ci doar pentru farmacie (în condiția unui tratament gratuit sau compensat) și compartimentul financiar-contabil.

Scrisoarea medicală este necesară pentru medicul de familie.

În imaginea de mai sus sunt prezentate structurile obiectelor care sunt documentele de lucru din cadrul organizațiilor.

Fluxul informațional a fost prezentat anterior, în capitolul 3, Figura 3.5.

Din cele prezentate mai sus, se poate deduce că unele dintre documente au un grad sporit de confidențialitate și de asemenea au acces multiplu. Fiecare dintre utilizatori va trebui să acceseze numai partea care îi este destinată.

Procesele aplicate obiectelor ce conțin date sunt formate din acțiuni și fluxuri (transmiterea acestora către următorul grup de utilizatori), și sunt constituite într-o ierarhie de încredere, după cum urmează:

1. Creare;
2. Consultare;
3. Modificare;
4. Adăugare;
5. Imprimare;
6. Arhivare.

Relațiile de încredere corespunzătoare între obiecte și utilizatorii pentru aplicarea proceselor din domeniile prezentate mai sus, $R_g(GO_j, D_l, G_m, C_k) – R_g$, GOj, D_l și C_k fiind definite în 3.1. Pentru sintetizarea acesora, ele se pot centraliza sub formă tabelară.

În tabelul A3.1. din Anexa 3 sunt prezentate grupurile de obiecte (din documente), grupurile de utilizatori, contextul de lucru al utilizatorilor care au acces la acestea, cu procesele de încredere ce le sunt permise acestora. Am folosit forma tabelară pentru o vedere de ansamblu mai succintă, permițând un control mai eficient al proceselor atribuite obiectelor și utilizatorilor.

Obiectele fiind stocate în baze de date și documente.

Ca urmare a celor prezentate anterior, putem face o ierarhie a datelor privind sensibilitatea informațiilor conținute în documente, grupate pe domenii de activitate.

Date generale comune tuturor domeniilor sunt datele de identificare pacient, medic curant, ora și data planificată și, sunt comune pentru domeniile:

- evidență pacienți-consultații;
- medical;

- laborator;
- financiar-contabil.

Date specifice anumitor domenii:

- analizele efectuate de laborator, date ce comune pentru domeniile:
  - medical;
  - laborator;
  - financiar contabil;
- diagnostic prezumtiv și valorile analizelor, ce sunt comune domeniilor:
  - medical;
  - laborator;
- diagnostic final, ce este comun pentru domeniile:
  - medical;
  - farmacie;
- medicație recomandată pacient, date comune pentru domeniile:
  - medical;
  - farmacie;
  - financiar-contabil;
- valoarea serviciilor prestate de medic și laborator este numai pentru domeniul financiar contabil;
- valoarea medicamentelor sunt date comune pentru domeniile:
  - farmacie;
  - financiar-contabil;
- costul final al serviciilor prestate este numai pentru serviciul financiar-contabil.

4.1.1.Proiectarea obiectelor

Domeniile: *medical, farmacie* și *financiar-contabil* au în comun datele legate de tratamentele eliberate, iar valoarea acestora este comună numai domeniilor *farmacie* și *financiar contabil.*

În cele ce urmează, vom căuta să exemplificăm cele prezentate mai sus, prin aplicarea politicilor de control al accesului și acțiunilor asupra unor exemple prezentate anterior.

În general, datele utilizate într-o organizație mică, ce nu are o structură ierarhică, nu necesită o bază mare de date și un sistem centralizat, sofisticat. Cantitatea de date manipulate pe parcursul unei zile este destul de redus, ceea ce duce la realizarea unui sistem informatic bazat pe mesaje și documente, care ulterior va permite centralizarea datelor rezultate în urma prestării

serviciilor de investigație propuse și efectuate cât și a medicamentelor prescrise și furnizate, pe fiecare compartiment în parte.

O parte din documente sunt utilizate temporar, altele sunt utilizate pentru centralizarea activității compartimentelor. Documentele temporare care sunt utilizate pentru procesele din cadrul organizației, sunt: *fișa pacientului, biletul de trimitere pentru analize, buletinul de analize medicale, rețeta medicală, factura*.

Documentele care vor fi centralizate sunt:

- pentru recepție, „Registrul planificare consultații" și „Fișa de consultații";
- pentru cabinetul medicului, „Registrul de consultații";
- pentru laboratorul de analize, „Registrul analizelor medicale";
- pentru farmacie, „Registru de liberări" și „Evidența stocurilor";
- pentru financiar-contabil, „Evidență facturi".

Pentru aceste documente, vom utiliza stocarea, transferul și prelucrarea datelor în format *xml*, utilizând doar o parte din datele pe care acestea le conțin (cele importante pentru evidența internă) pentru a fi stocate în bazele de date.

4.1.2. Analiza proceselor

În continuare vom prezenta principalele procese ale aplicației.

Planificarea pacienților (figura A2.2.- Anexa 2) presupune următoarele procese*:*

- prezentarea pacientului la clinică;
- solicitarea planificării la consultație;
- completarea datelor de identificare;
- verificarea existenței fișei pacientului; dacă aceasta nu există, completarea unei fișe noi iar dacă există, identificarea și pregătirea pentru consultație.

Consultația medicală presupune următoarele procese (Figura A2.3.- Anexa 2):

1. prezentare pacient și identificare;
2. citire fișă medicala, completare fișă, anamneza pacientului și înregistrarea simptomatologiei acestuia, control medical local, investigații locale, completarea fișei;
3. creare înregistrare nouă în registrul de consultații;
4. verificarea analizelor, dacă sunt analize noi;
5. recomandarea de noi analize dacă sunt necesare, cu diagnostic prezumptiv;
6. consultarea unui alt specialist extern, dacă este necesar;
7. stabilire diagnostic final, cu completarea fișei și a registrului de consultații, completarea recomandărilor medicale și a tratamentului.

Analizele de laborator presupun următoarele procese (figura A2.4.- Anexa 2):

1. Prezentare pacient;
2. Identificare pacient și analize de efectuat;
3. Pregătire probe;
4. Prelevare probe;
5. Efectuare analize, înregistrare analize în registrul de laborator, completare buletin de analize, înștiințare compartiment financiar-contabil despre analizele efectuate pentru pacient.

Eliberarea tratamentelor de la farmacie presupune următoarele procese (Figura A2.5- Anexa 2):

1. Prezentarea pacientului la farmacie;
2. Identificarea acestuia pe baza actelor de identitate;
3. Citirea rețetei;
4. Înmânarea medicamentelor;
5. Completarea registrului de eliberări
6. Înștiințarea compartimentului financiar-contabil privind medicamentele și valoarea pentru completarea devizului pacientului.

Facturarea și încasarea valorilor serviciilor prestate presupune următoarele procese (Figura A2.6.- Anexa 2):

1. prezentarea pacientului la compartimentul financiar-contabilitate;
2. verificarea serviciilor prestate la cabinetul medical, lista analizelor efectuate de laborator, tratamentul eliberat;
3. întocmirea facturii cu datele de identificare necesare, și predarea către pacient;
4. plata serviciilor prestate și a tratamentului ridicat, de către pacient.

4.1.3. Utilizarea tehnologiei Xml în implementarea politicilor de control al accesului și acțiunilor bazate pe încredere

În documentele prezentate mai sus, unele date sunt comune (ce pot fi vizualizate de toți cei din clinică) și date confidențiale (pe care le pot accesa numai anumite grupuri). Aceste date sunt create numai de membrii personalului special desemnat și, în mod fizic, sunt stocate în documente.

Prin intermediul formatului de date *xml*, putem implementa elementele de control ale politicii de control al accesului și acțiunilor asupra datelor cu care interacționează utilizatorii prin intermediul sistemului informatic.

În Anexa 4 este prezentat un model de completare a documentelor medicale, numit *fisa_medicală.xml*, cu prezentarea permisiunilor și restricțiilor pentru domeniile de activitate.

În cadrul fișierului *fisa_medicală.xml*, cu datele pacientului, au fost specificate pe lângă domeniul căruia îi aparțin, domeniile de acces, nivelul de încredere, procesul permis de nivelul de încredere, cât și contextul de aplicare a vizibilității datelor.

În modelul prezentat, nu se pune problema creării de restricții la nivel de utilizator, restricțiile fiind la nivelul domeniului de activitate. În cazul fișei medicale, orice medic intern al clinicii are acces la toate datele din fișă, dar un medic consultant din exterior, nu are acces la datele de identificare ale pacientului. Crearea fișei se face de către compartimentul evidență pacienți-consultații, care nu are acces la datele medicale ale pacienților, iar medicii pot completa datele medicale, dar nu pot modifica datele de identificarea ale pacientului.

Restricționarea accesului la datele care sunt confidențiale și țin de relația pacient-medic, se va face prin intermediul interfeței grafice. Proiectarea interfeței grafice va ține cont de elementele enumerate anterior și va aplica politicile de control al accesului și al proceselor necesare.

Prin urmare politicile de încredere cerate sunt la nivel de grup, conform celor prezentate

Utilizarea datelor în format *xml* permite construirea de interfețe dinamice, care reacționează la context.

În majoritatea limbajelor de programare, există procese de încărcare, inițializare ale obiectelor grafice pentru interfețe și proprietăți ce pot fi modificate dinamic și permit controlul lor, prin intermediul proprietăților cum ar fi:

- disponibilitatea (Enable);
- vizibilitatea (Visible);
- modificarea datelor (ReadOnly);

care ne ajută la crearea conținutului dinamic.

Pentru modelul de mai sus, în cadrul unei proceduri „LOAD” a interfeței grafice, vom avea următoarele grupuri elemente ce vor fi active sau inactive, vizibile sau nu, și „read only” sau nu funcție de contextul aplicației și domeniul de activitate din care face parte utilizatorul care a accesat aplicația. Astfel, pentru grupul de date de identificare ale pacientului care este creat de compartimentul „evidență pacienți-consultații”, vom avea:

If domain= „evidenta_pacienti_consultatii”

Txtbox.pacient_lastname.visible=”true”

Txtbox.pacient_lastname.enable=”true”

Txtbox.pacient_lastname.readonly=”false”

Txtbox.pacient_firstname.visible=”true”

Txtbox.pacient_firstname.enable=”true”

Txtbox.pacient_firstname.readonly=”false”

Txtbox.pacient_gender.visible=”true”

Txtbox.pacient_gender.enable=”true”

Txtbox.pacient_gender.readonly=”false”

Txtbox.pacient_age.visible=”true”

Txtbox.pacient_age.enable=”true”

Txtbox.pacient_age.readonly=”false”

Txtbox.pacient_birthday.visible=”true”

Txtbox.pacient_birthday.enable=”true”

Txtbox.pacient_birthday.readonly=”false”

Txtbox.pacient_marital_status.visible=”true”

Txtbox.pacient_marital_status.enable=”true”

Txtbox.pacient_marital_status.readonly=”false”

Txtbox.pacient_cnp.visible=”true”

Txtbox.pacient_cnp.enable=”true”

Txtbox.pacient_cnp.readonly=”false”

Endif

If domain= „medical”and contex=”intern”

Txtbox.pacient_lastname.visible=”true”

Txtbox.pacient_lastname.enable=”true”

Txtbox.pacient_lastname.readonly=”true”

Txtbox.pacient_firstname.visible=”true”

Txtbox.pacient_firstname.enable=”true”

Txtbox.pacient_firstname.readonly=”true”

Txtbox.pacient_gender.visible=”true”

Txtbox.pacient_gender.enable=”true”

Txtbox.pacient_gender.readonly=”true”

Txtbox.pacient_age.visible=”true”

Txtbox.pacient_age.enable=”true”

Txtbox.pacient_age.readonly=”true”

Txtbox.pacient_birthday.visible=”true”

Txtbox.pacient_birthday.enable=”true”

Txtbox.pacient_birthday.readonly=”true”

Txtbox.pacient_marital_status.visible=”true”

Txtbox.pacient_marital_status.enable=”true”

Txtbox.pacient_marital_status.readonly=”true”

Txtbox.pacient_cnp.visible=”true”

Txtbox.pacient_cnp.enable=”true”

Txtbox.pacient_cnp.readonly=”true”

Endif

If domain= „medical”and contex=”extern”

Txtbox.pacient_lastname.visible=”false”

Txtbox.pacient_lastname.enable=”false”

Txtbox.pacient_lastname.readonly=”true”

Txtbox.pacient_firstname.visible=”false”

Txtbox.pacient_firstname.enable=”false”

Txtbox.pacient_firstname.readonly=”true”

Txtbox.pacient_gender.visible=”false”

Txtbox.pacient_gender.enable=”false”

Txtbox.pacient_gender.readonly=”true”

Txtbox.pacient_age.visible=”false”

Txtbox.pacient_age.enable=”false”

Txtbox.pacient_age.readonly=”true”

Txtbox.pacient_birthday.visible=”false”

Txtbox.pacient_birthday.enable=”false”

Txtbox.pacient_birthday.readonly=”true”

Txtbox.pacient_marital_status.visible=”false”

Txtbox.pacient_marital_status.enable=”false”

Txtbox.pacient_marital_status.readonly=”true”

Txtbox.pacient_cnp.visible=”false”

Txtbox.pacient_cnp.enable=”false”

Txtbox.pacient_cnp.readonly=”true”

Endif

Acest model se va aplica și pentru celelalte date, ținând cont de domeniul de acces, de context, de domeniul care procesează datele și de procesul de încredere alocat.

S-a prezentat aici modelarea pentru primul grup de date, cele de identificare.

Pentru modelul descris, s-a specificat anterior că sistemul nu are un server de domeniu și echipamentele sunt independente, astfel că nu există un punct singular de aplicare a politicii, ele fiind distribuite în fiecare punct de accesare a documentelor.

În momentul accesării documentelor se aplică politicile de control al accesului și proceselor aplicate datelor, la nivelul aplicației, prin controlul interfeței grafice utilizate de aceasta.

Acest exemplu, prezintă un model de aplicare a politicilor de control al acțiunilor și accesului bazate pe încredere la nivel de grup de utilizatori.

4.2. Un exemplu de aplicare a politicilor de control al accesului și acțiunilor în cazul unei cereri de concediu de odihnă

În cazul organizațiilor medii și mari, unde sunt mai multe domenii de activitate structurate pe ierarhii organizaționale, o arhitectură ca cea descrisă mai sus este neproductivă, întrucât administrarea acesteia va ridica probleme personalului desemnat pentru aplicarea politicilor de control.

Este de preferat utilizarea unei arhitecturi ce are un controler de domeniu. Pentru a ilustra aplicarea politicilor de control în acest caz, ne vom întoarce la exemplele anterioare și vom prezenta aplicarea politicilor de control în cadrul unor organizații medii, asupra cererii de concediu de odihnă a unui angajat.

Cum s-a arătat, pe parcursul procesului de aprobare a documentului, acesta trece prin diverse departamente, unde suferă completări din partea personalului autorizat. În fiecare departament prin care trece, se verifică domeniul, contextul, utilizatorul, și procesul autorizat.

Pentru exemplificare, pornim de la analiza efectuată în 3.3.2.

Fie următoarele date ale unei cereri de concediu in format *xml*.

<document>

<nume_document>Cerere concediu odihna</nume_document>

<nume> </nume>

<prenume> </prenume>

<loc_munca>sectia, atelierul </loc_munca>

<functia> </functia>

<nr_zile_concediu> </nr_zile_concediu>

<anul> </anul>

<de_la_data> / / </de_la_data>

<pana_la_data> / / </pana_la_data>

<comentariu> </comentariu>

</document>

Documentul care se creează pe baza unui template predefinit, va conține următoarele elemente suplimentare:

- descrierea domeniilor care au acces la aceste date pe toată durata existenței documentului (citirea lor);
- contextul în care poate fi accesat documentul (intern - în cadrul organizației, sau extern);
- domeniul unde i se pot aplica diverse procese, altele decât citirea datelor conținute;
- utilizatorul ce poate aplica un proces;
- procesul ce poate fi aplicat.

<domain_access>loc_munca,loc_munca_manager,personal,management</domain_access>
<context>intern</context>
<domain_process>loc_munca</domain_process>
<trust_process>create, modify, promote</trust_process>

În final, formatul documentului, după ce trecut prin toate etapele, va fi:

```
<?xml version="1.0" encoding="utf-8"?>
<document>
    <nume_document>Cerere concediu odihna</nume_document>
    <nume> </nume>
    <prenume> </prenume>
    <loc_munca> </loc_munca>
    <functia> </functia>
    <nr_zile_concediu> </nr_zile_concediu>
    <anul> </anul>
    <de_la_data> </de_la_data>
    <pana_la_data> </pana_la_data>
    <domain_access>loc_munca,loc_munca_manager,personal,management</domain_acce
ss>
    <context>loc_munca</context>
    <domain_process>loc_munca</domain_process>
    <trust_process>create,read,modify,promote</trust_process>
    <manager_loc_munca>
        <nume> </nume>
        <prenume> </prenume>
          <punct_de_vedere>    </punct_de_vedere>
```

<domain_access>loc_munca_manager,personal,management</domain_access>

<context>loc_munca_manager,personal,management</context>

<domain_process>loc_munca_manager</domain_process>

<user>userid</user>

<trust_processs>read,modify</trust_processs>

</manager_loc_munca>

<personal>

<verificat_nume> </verificat_nume>

<verificat_prenume> </verificat_prenume>

<zile_de_concediu_restante> </zile_de_concediu_restante>

<stare_concediu> </stare_concediu>

<domain_access>personal,management</domain_access>

<context>presonal,management</context>

<domain_process>personal</domain_process>

<user>userid</user>

<trust_processs>read,modify</trust_processs>

</personal>

<management>

<aprobare> </aprobare>

<domain_access>

loc_munca,loc_munca_manager,personal,management

</domain_access>

<context>management</context>

<domain_process>management</domain_process>

<user>userid</user>

<trust_processs>read/modify</trust_processs>

</management>

</document>:

La crearea lui, documentul conține numai elementele primare, necesare cererii de concediu, anume: datele de identificare ale angajatului, anul pentru care solicită concediul de odihnă (e posibil să aibă concediu de recuperat din ultimii ani), data de început a concediului și data de sfârșit a acestuia.

Odată completate datele, ele sunt transmise unui server de validare a proceselor, pentru transfer și înregistrare, care:

- analizează documentul;
- identifică domeniul din care face parte documentul;
- identifică nivelul de încredere al documentului;
- identifică utilizatorul;
- identifică ierarhia de procese ce trebuie aplicate;
- identifică ierarhia de utilizatori conform valorii de încredere necesare pentru aplicarea procesului;
- înregistrează tipul de document;
- identifică utilizatorul care a trimis documentul;
- determină data și procesul următor ce va fi aplicat documentului;
- completează documentul cu datele necesare pentru etapa următoare;
- trimite documentul către compartimentul corespunzător.

Odată ce procesul permis este aplicat documentului, acesta este din nou transferat către același server, care:

- analizează documentul;
- verifică utilizatorul care l-a trimis, prin validarea domeniului din care face parte;
- validează etapa parcursă și procesul aplicat;
- înregistrează noul proces ce va fi aplicat;
- completează documentul cu datele necesare pentru etapa următoare;
- îl trimite către compartimentul corespunzător.

Pe parcursul existenței documentului, acesta nu va putea să fie transferat decât ierarhic ascendent sau descendent, conform ierarhiei de domenii și procese necesare a fi executate. Starea acestuia va fi înregistrată prin înregistrarea procesului următor ce urmează a fi aplicat documentului. Fiecare utilizator, va avea acces numai la datele și informațiile ce-i sunt destinate conform modelului creat.

În cazul curent, în ceea ce privește ierarhia de procese, aceasta este formată din:

1. completarea documentului de către angajat;
2. completarea punctului de vedere al managerului locului de muncă;
3. completarea datelor și validarea concediului de către compartimentul personal-salarizare;
4. aprobare de către manager.

Serverul de validare a proceselor, transfer și înregistrare, va verifica de fiecare dată politicile de control al accesului și acțiunilor create pentru documentul respectiv, și în funcție de

acestea va completa documentul și va face transferul către utilizatorul desemnat, ținând cont de eventualele restricții și delegări.

Pe parcursul duratei de existență a obiectului, acesta va putea fi accesat de cei îndreptățiți dar fiecare va avea acces numai la elementele destinate lui.

În acest exemplu s-a prezentat o posibilă aplicare a politicilor de control al accesului și acțiunilor bazate pe încredere, pentru utilizatori.

4.3. Un exemplu de construire a unor rapoarte dinamice

În continuare vom prezenta un exemplu de raport dinamic creat cu ajutorul *xml*, într-o organizație ce are o politică internă de clasificarea informațiilor bazată de niveluri de acces în funcție de sensibilitatea acestora, informațiile aparținând diverselor domenii de activitate ale organizațiilor.

Pentru a crea un document centralizator *(DC)*, adresat tuturor membrilor organizației, document ce trebuie să țină cont de clasificarea informațiilor conținute, de domeniile de activitate din organizație și, de drepturile de accesare a acestora de către membri, stabilim următoarele:

- documentul este format din secțiuni (părți) de document, ce pot fi texte, imagini, tabele, grafice, slide-uri, etc. ce sunt creația unui colectiv format din membrii ai domeniilor organizației ce au acces la informațiile transpuse;
- secțiunile le vom considera pe fiecare în parte a fi un obiect;
- fiecare secțiune poate conține informații ce aparțin unui domeniu sau mai multor domenii;
- fiecare secțiune are un nivel de clasificare care determină dreptul de accesare în vederea citirii raportului.

Conform condițiilor generale pentru a aplica o politică de încredere, pentru oricare obiect O_i ce are un nivel de încredere minim necesar pentru a fi accesat de un utilizator, există un utilizator ce are o valoare de încrederea ce permite executarea de procese asupra acestuia. Aceasta poate fi prezentată astfel:

Dacă *D* este mulțimea domeniilor de activitate ale organizației,

$D=\{D_1, D_2, \ldots D_i, \ldots D_n\}$ (D_i definit în condițiile generale pentru a aplica o politică de încredere)

GM= mulțimea de grupuri de utilizatori ce aparțin organizației,

$GM=\{Gm_1, Gm_2 \ldots Gm_i .. Gm_n\}$ (Gm_i definit în condițiile generale pentru a aplica o politică de încredere) și, se respectă următoarele condiții:

1. Pentru $\forall Gm_i \Rightarrow \exists Di$
2. $\forall U_{ki} \in Gm_i$

3. $\forall U_{ki} \in H(Gm_i)$, *unde* $H(Gm_i)$ reprezintă ierarhia de încredere a grupului Gm_i, pentru ca Uk_i să acceseze *Oi*, atunci:

acesta trebuie să aibă:

$R_u(U_k) \geq R_o(O_i)$, adică „trust_value" ≥ „trust_level" al obiectului O_i;

$H_p(p_k(Oi)) \neq \emptyset$.

Prin urmare dacă $Rp(O_i) \leqq Ru(U_{ki})$ atunci obiectul O_i poate fi accesat de către utilizatorul U_k..

În rândurile de mai jos, avem structurat un astfel de exemplu de document.

```
<?xml version="1.0" encoding="utf-8"?>
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="document.xsd">
  <name> </name>
  <abstract> </abstract>
    <context> </context>
  <content>
   <section>
    <content> </content>
    <domain> </domain>
    <trust_level> </trust_level>
      <contex> </context>
   </section>
.
.
.
.
    <section>
     <content> </content>
     <domain> </domain>
     <trust_level> </trust_level>
       <contex> </context>
    </section>
  </content>
</Document>
```

Cu următoarea schemă de validare:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
 <xs:element name="Document">
  <xs:complexType>
   <xs:sequence>
    <xs:element name="name" type="xs:string"/>
    <xs:element name="abstract" type="xs:string"/>
    <xs:element name="context" type="xs:string"/>
    <xs:element ref="content"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="content">
  <xs:complexType>
   <xs:sequence minOccurs="0">
    <xs:element ref="section" minOccurs="0" maxOccurs= „unbounded"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
 <xs:element name="section">
  <xs:complexType>
   <xs:sequence>
    <xs:element ref="content"/>
    <xs:element name="domain" type="xs:string"/>
    <xs:element name="trust_level" type="xs:string"/>
    <xs:element name="context" type="xs:string"/>
   </xs:sequence>
  </xs:complexType>
 </xs:element>
</xs:schema>
```

Acest exemplu poate constitui un model de implementare a unui sistem de raportare dinamic.

În acest exemplu s-a prezentat un model complex de utilizare a politicilor de control al accesului și acțiunilor bazate pe încredere, pentru utilizarea în organizații cu informațiile clasificate pe niveluri de accesare.

4.4. Comparație a RBAC, ABAC și a „Controlului accesului și acțiunilor bazat pe încredere" (Trust Based Access and Action Control - TBAAC)

În cele ce urmează vom face o prezentare a principalelor trăsăturii ale celor trei metode de proiectare [17].

RBAC pleacă de premisa că fiecare membru al unei organizații are un rol bine definit în cadrul acesteia. Acest rol determină exercitarea unor drepturi și obligații clare în cadrul organizației. Bazat pe existența acestor drepturi și obligații, este determinat și controlul accesului la date și al acțiunilor utilizatorilor (vezi capitolul 1.5).

Aplicațiile proiectate pe baza RBAC sunt aplicații statice, în care pentru fiecare tip de aplicație se creează o interfață, ce permite un număr de acțiuni determinate, pentru un anumit rol ce este caracteristic unui utilizator sau grup de utilizatori.

Prezentat de către N.I.S.T. în 2014, ABAC este o nouă metodă de control al accesului, ce permite o abordare dinamică a interacțiunii dintre obiect și subiect prin primirea de răspunsuri legate de posibilitatea utilizatorului de a întreprinde diverse acțiuni prin răspunsuri de tip Da /Nu.

Acest lucru presupune o interogare permanentă a serverului ce deservește Policy Enforcement Point, punctul unde este aplicată politica (vezi capitolul 1.6).

Spre deosebire de cele două modele de mai sus, politicile de control al accesului și acțiunilor bazate pe încredere sunt politici predeterminate, ce sunt aplicate pentru aplicațiile client/server pe echipamentul client unde se execută cererile și aplicația client, iar pentru aplicațiile de tip web se execută pe server, ținând cont de politicile implementate pentru un anumit utilizator sau grup de utilizatori.

Din punctul de vedere al aplicării politicilor și al dinamicii aplicațiilor, RBAC este de folosit pentru organizații unde rolurile sunt stabilite aprioric și nu apar evenimente ce presupun crearea și implementarea de politici modificate pentru diverse perioade de timp.

ABAC [17] permite crearea de politici dinamice, ce presupun un trafic de interogare a serverului de autorizare crescut, ceea ce într-o organizație mare poate crea probleme privind suportabilitatea numărului mare de utilizatori și necesitatea de capabilități sporite de procesare.

Controlul accesului și acțiunilor utilizatorilor bazate pe încredere, permite crearea de aplicații cu comportament dinamic, care poate fi modificat foarte ușor, ce nu necesită un trafic continuu suplimentar, și care poate înlocui atât RBAC cât și ABAC.

Ținând cont de cele prezentate mai sus, de simplitatea proiectării politicilor de control al accesului și acțiunilor utilizatorilor, de ușurința modificării comportamentului unei aplicații în exploatarea de către un utilizator, considerăm că „Controlul accesului și acțiunilor bazate pe încredere” (TBAAC) este de preferat în crearea aplicațiilor stand alone, client/server sau web.

4.5. Concluzii la capitolul 4

În cadrul lucrării de față, s-a abordat controlul accesului și al acțiunilor utilizatorilor unui sistem informatic bazat pe încredere.

Prin utilizarea limbajului xml, pentru implementarea politicilor de control al accesului și acțiunilor utilizatorilor, se creează un mecanism foarte flexibil de stocare și modelare a politicilor. Modelarea politicilor de control prezentată pe parcursul capitolului, prin diverse exemple de aplicare pentru diferite tipuri de organizații, cu diferite arhitecturi ale sistemului informațional, prezintă ușurința implementării de soluții de control al accesului și controlul acțiunilor utilizatorilor, de la o aplicare simplă în care politicile sunt aplicate la nivel de grupuri de lucru, până la o aplicare complexă în cadrul organizațiilor cu informații clasificate.

Flexibilitatea politicilor de control al accesului și acțiunilor bazate pe încredere, în implementarea și utilizarea lor, permite implementarea ușoară a unor soluții de creșterea securității aplicațiilor.

Considerăm că spectrul de implementare și utilizare este mult mai larg, și că ceea ce s-a prezentat în capitolul curent, este o bază de pornire în experimentarea aplicării acestor politici.

CONCLUZII GENERALE ȘI RECOMANDĂRI

Rezultatul obținut, modelarea controlului accesului și a acțiunilor utilizatorilor asupra documentelor în format electronic, prin aplicarea politicilor bazate pe încredere, ce contribuie la soluționarea unei probleme științifice importante, privind confidențialitatea datelor și informațiilor, cât și controlul interacțiunii utilizatorilor cu acestea, constă în fundamentarea din punct de vedere științific și metodologic a condițiilor de acordare a încrederii utilizatorilor în vederea interacțiunii cu datele și informațiile dintr-un sistem informatic, asigurând controlul accesului și acțiunilor acestora.

Pentru a pune bazele teoretice ale sistemelor de contol ale accesului și acțiunilor bazate pe încredere, au fost necesari mai mulți pași de întreprins:

1. S-a stabilit importanța încrederii în utilizatori din cadrul organizațional, încredere impersonală (calculată) sau personală (atribuită pe baza cunoșterii directe), ce permite participarea utilizatorului la fluxul informațional-decizional.(Cap.2.5 pag. 60-71).
2. Pentru prima dată în cercetarea informatică, s-au stabilit elementele necesare formalizării condițiilor de aplicare ale politicilor de încredere, pentru accesarea și interacționarea cu obiectele sistemului informatic. (Cap. 3.1 pag. 73-78)
3. Pentru prima dată, am propus un concept complex al modelului de control al accesului și acțiunilor în sistemele informaționale, mai extins decât cele existente anterior (propuse în lucrări anterioare de către autor), în baza formalizării nivelurilor de încredere acordate utilizatorilor și identificarea metodelor de aplicare a valorilor de încredere (Cap. 3 pag. 79-83).
4. Modelul dezvoltat, permite o abordare dinamică a aplicării politicilor de control al accesului și acțiunilor utilizatorilor, mutând sarcina implementării acestora de la dezvoltatorul aplicației, către responsabilul de securitate al organizației. Prin aplicarea lui, se pot crea rapid politici de acces și control al acțiunilor utilizatorului, pe parcursul evoluției fluxului informațional.

Scopul lucrării a fost atins prin crearea modelului teoretic complex, ce stă la baza aplicării politicilor de control al accesului și acțiunilor utilizatorilor.

Valoarea aplicativă a modelului TBAAC este demonstrată prin demonstarea aplicării în modelarea politicilor Biba, MAC și DAC (Cap. 3.1 pag. 83-84) (politici recunoscute pentru valoarea lor științifică și practică), cât și prin cele trei exemple de aplicare prezentate:

- Primul exemplu prezentat (Cap. 4.1 pag/ 95-106), se referă la o organizație medicală, care are n departamente, ce corespund unor domenii de activitate. S-au prezentat simplificat, modelele de date care corespund acestor domenii ,ce sunt obiecte ale proceselor aplicate de utilizatori, cât și fluxul de lucru pe baza căruia se stabilesc ierarhiile de procese aplicate, flux ce rezultă în urma analizei proceselor suportate de obiecte. S-a prezentat un prim model de document în format *xml*, document ce conține integrate elementele ce specifică domeniile de acțiuni, domeniul de procesare, contextul și tipul proceselor care pot fi aplicate obiectelor desemnate, obiectele fiind grupate pe domenii de activitate. Acest exemplu a prezentat aplicarea politicilor pentru organizații funcționale, de mici dimensiuni, unde deși cantitatea de date vehiculată este mică, sunt cerințe legale de protejare a datelor și informațiilor existente.
- În al doilea exemplu de implementare a politicilor prin intermediul documentelor în format *xml*, este reluat obiectul „cerere de concediu**”** care a fost prezentat anterior (Cap. 3.3.2 pag 84-93) în vederea demonstrării construirii politicilor. Obiectul construit utilizându-se formatul *xml*, conține la fel ca cel anterior construit elementele ce specifică domeniile de acțiuni, domeniul de procesare, contextul și tipul proceselor ce pot fi aplicate obiectelor desemnate, având în plus utilizatorul desemnat care poate aplica procesul. Acest exemplu (Cap. 4.2 pag. 106-110) a demonstrat aplicarea politicilor într-o organizație în care politicile se aplică la nivel de utilizatori.
- În al treilea exemplu (Cap. 4.3 pag.110-112), este prezentată implementarea politicilor în cadrul unei organizații care utilizează informații clasificate. Informațiile sunt clasificate pe domenii de activitate și grad de sensibilitate. Documentul creat specifică cine poate accesa obiectele, ce obiecte poate accesa, și procesele pe care le poate aplica acestora.

Modelul nou creat, de impunere a politicilor de confidențialitate și securitate a datelor și informațiilor din sistemele informaționale, prin controlul accesului și acțiunilor utizlatorului bazate pe încredere, ține cont de condițiilor necesare de îndeplinit de către utilizator, cât și de contextul în care acțiunile se defășoară, permițând crearea de politici de securitate flexibile, aplicate dinamic.

Aplicarea practică a acestei lucrări, a fost realizată în cei 10 ani de parteneriat cu Institutul de Cercetare - Dezvoltare pentru Ecologie Acvatică, Pescuit și Acavacultură în cadrul proiectelor dezvoltate în comun.

Pentru realizarea acestor politici, am proiectat și realizat aplicația „Trust analist”, aplicație ce permite crearea politicilor bazate pe încredere și, implementează conceptele și modelele

dezvoltate în urma cercetărilor efectuate, fiind utilizată în activitatea de proiectare a aplicațiilor realizate, pentru implementare a politicilor ce trebuiau impuse.

Direcții de cercetare pentru viitor

- Cercetări privind extinderea aplicării politicilor de control al accesului și acțiunilor bazate pe încredere asupra bazelor de date, în vederea controlării accesului și acțiunilor utilizatorilor asupra tupluri-lor de date, cât și a proiecțiilor tabelelor.
- Cercetări privind utilizarea framework-uri de aplicare a politicilor pentru diverse tipuri de aplicații (standalone, client-server și web).
- Cercetări privind crearea unui limbaj pentru impunerea politicilor de control bazate pe încredere.
- Crearea de modele de implementare în cadrul diverselor aplicații de tip ERP.
- Cercetarea aplicării TBAAC în domeniul senzorilor și IoT.

BIBLIOGRAFIE

1. ADOMNICAI Cosmin, **DANILESCU Marcel**, Assurance model behavior in social networks based on trust. În: *IACSIT (Ed.), 2011 3rd International Conference on Computer technology and Development.* Chengdu, 2011 China, IACSIT. Diponibil http://dx.doi.org/10.1115/1.859919.paper183
2. ALFAREZ Abdul-Rahman, HAILES Stephen, A Distributed Trust Model. În: *New Security Paradigms Workshop, ACM,* 1998, (pp. 48-60), New York, U.S.A. Disponibil https://doi.org/10.1145/283699.283739 .
3. ALFAREZ Abdul-Rahman, HAILES Stephen, Supporting Trust in Virtual Communities, *Proceedings of the 33rd Hawaii International Conference on System Sciences* - 2000, 7-7 Jan, Print ISBN:0-7695-0493-0. Disponibil DOI: 10.1109/HICSS.2000.926814
4. ASHLEY Paul, HADA Satoshi, KARJOTH Günter, POWERS Calvin, SCHUNTER Matthias, Enterprise Privacy Authorization Language (EPAL 1.2), *W3C*, 2003, noiembrie, 10. Disponibil https://www.w3.org/Submission/2003/SUBM-EPAL-20031110/
5. BAIER Annette, Trust and Antitrust, În: *Ethics* Vol. 96, No. 2 ianuarie., 1986, pp. 231-260 (30 pages) Published By: The University of Chicago Press. Disponibil https://doi.org/10.1086/292745 https://www.jstor.org/stable/2381376
6. BANYAL Rahitash Kumar, JAIN Vijendra Kumar, JAIN Pragya,Dynamic Trust Based Access Control Framework for Securing Multi-Cloud Environment. În: *ICTCS '14: Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies*, 2014, octombrie. Article No.: 29 Pages 1–8 Diponibil https://doi.org/10.1145/2677855.2677884
7. BELL David Elliott., LAPADULLA Leonard J., *Computer security model: Unified exposition and multics interpretation. Technical report*. Bedford, MA: MITRE Corp 1975, iunie U.S.A. Disponibil https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings -of-the-21st-nissc-1998/documents/early-cs-papers/bell76.pdf
8. BELL David Elliott., LAPADULLA Leonard J., *Secure Computer Systems: Mathematical Foundations.* Bedford, MA: MITRE Corp 1973. Disponibil https://web.archive.org/web/20060618092351 http://www.albany.edu/acc/courses/ia/classics/belllapadula1.pdf
9. BIBA, Kenneth J., *Integrity considerations for secure computer systems*. MITRE. Bedford, MA 1973: MITRE. U.S.A. Disponibil https://apps.dtic.mil/sti/pdfs/ADA039324.pdf
10. BISHOP, Matt, *Computer security: Art and Science*. Boston, Masachusets, U.S.A.: Addison Wesley 2002, decembrie. ISBN-10: 0201440997 ISBN-13: 9780201440997 .

11. BOON Susan D., HOLMES John G., The dynamics of interpersonal trust: resolving uncertainty in the face of risk. In: Hinde, R. and Gorebel, J., Eds. *Cooperation and Prosocial Behaviour* 1991 pp.190-211. Cambridge: Cambridge University Press, U.K..
12. CASTANO Silvana, FUGINI Mariagrazia, MARTELLA Giancarlo, SAMARATI Pierangela., *Database Security* Addison-Wesley & ACM Press, 1995, ISBN 0-201-59375-0 U.S.A.
13. COLEMAN James S., Foundations of Social Theory. În: *Social Forces*, Oxford University Press, Oxford, U.K. Volume 69, Issue 2, December 1990, pp. 625–633, https://doi.org/10.1093/sf/69.2.625.
14. CHIREGI Matin, NAVIMIPOUR Nima Jafari, A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities. În: *Computers in Human Behavior*, Netherlands, 2016, Volume 60, pp. 280-292, ISSN 0747-5632, https://dl.acm.org/doi/abs/10.1016/j.chb.2016.02.029
15. **DANILESCU Marcel**, Modeling Access Control And User Actions Using Trust - Based Access Control Policies. *Journal of Social Sciences* Vol. III, no.3 (2020), pp.72-84, Universitatea Tehnică A Moldovei, Chișinău, Republica Moldova. ISSN 2587-3490, eISSN 2587-3504. Disponibil https://jss.utm.md/wp-content/uploads/sites/21/2020/09/JSS-3-2020_72-84.pdf DOI: 10.5281/zenodo.3971967
16. **DANILESCU Marcel**, Data security management applying trust policies for small organizations, ad-hoc organizations and virtual organizations. In: *The Journal of Accounting and Management*, 2(3) 2012 pp. 47-64, Universitatea Danubius, Galați, România, Print ISSN: 2284 – 9459, On-line ISSN: 2392 – 8778. Disponibil http://journals.univ-danubius.ro/index.php/ jam/ article/view/1592
17. **DANILESCU Marcel**, Comparative study of access control methods in enterprise information systems, based on RBAC, ABAC, and TBAC policies, *Danubius International Conferences, 15th International Conference on European Integration - Realities and Perspectives*, Vol 15, No1 (2020) Galați, România, Universitatea Danubius, Print ISSN: 2067 - 9211, Online ISSN: 2069 – 9344, http://proceedings.univ-danubius.ro/index.php/eirp.
18. **DANILESCU Marcel**, BESLIU Victor, Creating Trust Based Access Policies to Control User Actions on Documents" „Information Technologies and Security2012", Intern.Conf. (2012; Chisinau). Proceedings of ITSEC-2012 International Conference on Information Technologies and Security 2012, 15-16 Oct. 2012,388p, Ed.Veacheslav Perju– NCAA, 2013, Chisinau Republica Moldova. ISBN 978-9975-4172-3-5. Disponibil https://ibn.idsi.md/sites/default/ files/imag_file/ Information%20Technologies%20and%20Security%202012.pdf
19. **DANILESCU Marcel**, DANILESCU Laura, Control Access To Information By Applying Trust Policies. *Conferința Internațională „Educație și creativitate pentru o societate bazată pe*

cunoaştere" ediția a IV-a, 2010,pp. 49-54, Universitatea „Titu Maiorescu", Bucuresti, România. ISBN 978-606-8002-47-7.

20. DANILESCU Laura, **DANILESCU Marcel**, Xml Based Techniques For Data Privacy In E-Business. Bucuresti: *Conferința Internațională „Educație și creativitate pentru o societate bazată pe cunoaștere" ediția a III-a*, 2009, pp. 15-19, Universitatea „Titu Maiorescu", București, România. ISBN 078-606-8002-36-1.
21. DANILESCU Laura, **DANILESCU Marcel**, Algorithm for defining trust hierarchies to control access to information, In: *International Conference on Informatic in Economy. Bucuresti: The Tenth International Conference on Informatics in Economy IE 2010*. A.S.E. (Ed.) 2011Bucuresti, România. ISSN 2247-1470.
22. DANILESCU Laura, **DANILESCU Marcel**, Organization's data access control policies based on trust. *EuroEconomica* 2, 2010, pp. 113-122. Universitatea Danubius, Galați, România. Print ISSN: 1582-8859, Online ISSN: 2065-3883.
23. DANILESCU Laura, **DANILESCU Marcel**, Control Access To Information By Applying Policies Based On Trust Hierarchies. *International Conference on Computer and Software Modeling, ICCSM 2010,* (pp. 285-290). Manila, Philippine: Institute of Electrical and Electronics Engineers, Inc.
24. DAOUD Wided Ben, OBAIDAT Mohammad S., Meddeb-Makhlouf Amel, *et al.* TACRM: trust access control and resource management mechanism in fog computing. In: *Hum. Cent. Comput. Inf. Sci.* **9,** 28 (2019). Disponibil https://doi.org/10.1186/s13673-019-0188-3
25. DASGUPTA Partha, Trust as a Commodity, In: *Trust:Making and Breaking Cooperative Relations*. Electronic edition 2000, Department of Sociology, University of Oxford, chapter 4, pp. 49-72.
26. DEUTSCH Morton, The Resolution of Conflict: Constructive and Destructive Processes, Yale University Press, November 1, 1973, Volume: 17 issue: 2, page(s): 248-248 ISBN 0-300-02186-0, https://doi.org/10.1177/000276427301700206
27. DEUTSCH Morton, Cooperation and trust: Some theoretical notes. In: *Nebraska Symposium on Motivation*, Lincoln, Univer. Nebraska Press, M. R. Jones (Ed.),. 1962.
28. DEUTSCH Morton and others, *The effects of training in cooperative learning and conflict resolution in an alternative high school*, Columbia Univ., New York, NY. Teachers Coll. International Center for Cooperation and Conflict Resolution, Martie, 1992. Disponibil https://eric.ed.gov/?id=ED359272
29. DOROTHY Denning, A lattice model of secure information flow. In: *Communications of the ACM*, Vol. 19, Issue 5 Mai, 1976, pp. 236–243. Diponibil https://doi.org/10.1145/360051.360056

30. DUMITRU Iacob, CISMARU Diana-Maria, *Organizația Inteligentă - Zece Teme De Managementul Organizațiilor* - ediția a doua, revăzută și adăugită (Vol. 1). (E. Comunicare.ro, Ed.) 2010 București, Romania: SNSPA, Facultatea de Comunicare si Relații Publice. Disponibil http://edituracomunicare.ro/pdf/pdf_518.pdf?id=1507777392 .
31. FERRAIOLO David F., KUHN D. Richard, Role-Based Access Controls. In: *15th National Computer Security Conference 1992*. (pp. 554-563). Baltimore MD: National Institute Of Standards And Technology/National Computer Security Center. Disponibil https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1992/10/13/proceedings-15th-national-computer-security-conference-1992/documents/1992-15th-NCSC-proceedings-vol-2.pdf .
32. FERRAIOLO David F., KUHN Richard, CHANDRAMOULI Ramaswamy, *Role-Based Access Control (ed. Second edition).* 2007, ARTECH HOUSE, INC., Norwood, Massachusets, U.S.A. ISBN-13: 978-1596931138 , ISBN-10: 1596931132 .
33. FERRAIOLO David, CHANDRAMUOULI Ramaswamy, HU Vincent, KUHN Richard A comparison of Attribute Based Access Contol (ABAC) Standards for Data Service Applications [Report]. In: *NIST Special Publication*, 2016. pp. 1-68 Gaithersburg, Maryland, U.S.A. Disponibil https://www.nist.gov/publications/comparison-attribute-based-access-control-abac-standards-data-service-applications , http://dx.doi.org/10.6028/NIST.SP.800-178 .
34. INDRAJIT Ray, SUDIP Chakraborty, A Vector Model of Trust for Developing Trustworthy Systems. In: *Lecture Notes in Computer Science Ser., Computer Security –ESORICS 2004*. pp. 260-275. Springer Verlag, Berlin, Heidelberg, Germany. ISBN 978-3-540-30108-0 https://doi.org/10.1007/978-3-540-30108-0_16 .
35. JONES Sara, WILIKENS Marc, MORRIS Philip, MASERA Marcelo, Trust requirements in e-business. In: *Communications of the ACM* Vol. 43, no. 12, 2000, dec., pp. 81–87. DOI: 10.1145/355112.355128. Disponibil https://doi.org/10.1145/355112.355128 .
36. KATSIKAS Sokratis K., LOPEZ Javier, PERNUL Gunther, Trust, privacy and security in e-business: Requirements and solutions. In: *Lecture Notes in Computer Science 3746 Conference: Proceedings of the 10th Panhellenic conference on Advances in Informatics*, 2005, Volas, Greece.. Disponibil https://www.researchgate.net/publication/29863409Trust_Privacy_and_Security_in_E-Business_Requirements_and_Solutions DOI: 10.1007/11573036_52.
37. KESARWANI Abhishek și KHILAR Mohan Pabitra, Development of trust based access control models using fuzzy logic in cloud computing. In: *Journal of King Saud University - Computer and Information Sciences*, 2019, ISSN: 1319-1578 . Disponibil https://plu.mx/plum/a/?DOI=10.1016/

j.jksuci.2019.11.001&theme=plum-sciencedirect-theme&hideUsage=true DOI: 10.1016/j.jksuci.2019.11.001.

38. KHILAR Mohan Pabitra, CHAUDHARI Vijay, SWAIN Rakesh Ranjan, Trust-Based Access Control in Cloud Computing Using Machine Learning. In: *Cloud Computing for Geospatial Big Data Analytics. Studies in Big Data*, vol 49. 2019 Springer Verlag, Germany. Disponibil https://doi.org/10.1007/978-3-030-03359-0_3 .
39. GOLEMBIEWSKI Robert T., MCCONKIE Mark Lewis, The centrality of interpersonal trust in group processes. In: *Theories of group processes* 1975 pp. 131-185. John Wiley & Sons Cooper, G. L. (Ed.), London, U.K.
40. HU Vincent C., FERRAIOLO David, KUHN Rick, SCHNITZER Adam, SANDLIN Kenneth, MILLER Robert, SCARFONE Karen. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. In: *NIST Special Publication 800 – 162*, 2014. (N. I. Publication, Ed.) Gaithersburg, Maryland, USA. Disponibil https://doi:10.6028/NIST.SP.800-162 și https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-162.pdf .
41. LANDWEHR Carl E., Formal models for computer security. *ACM Computing Surveys,Volume 13, Issue 3,Sept. 1981, pp 247–278*. Disponibil https://doi.org/10.1145/356850.356852 .
42. LEWICKI Roy J., MCALLISTER Daniel J, BIES Robert j., Trust And Distrust: New Relationships And Realities. In: *The Academy of Management Review 1998*. Vol. 23, No. 3, pp. 438-458. Ohio State University. USA. Disponibil https://doi.org/10.2307/259288 și https://www.jstor.org/stable/259288 .
43. LUHMANN Niklas, *Trust and Power Studies in Soviet Thought* Vol. 23, No. 3 Apr., 1982, pp. 266-270 Published By: Springer ISBN: 978-1-509-51945-3.
44. MAYER Roger C., DAVIS James H., SCHOORMAN F. David, An Integrative Model of Organizational Trust. In: *The Academy of Management Review* Vol. 20, No. 3 Jul., 1995, pp. 709-734 Disponibil https://www.jstor.org/stable/258792 și https://doi.org/10.2307/258792 .
45. MARSH, Stephen P. *Formalising Trust as a Computational Concept* ,University of Stirling 1994 Disponibil http://www.cs.stir.ac.uk/~kjt/techreps/pdf/TR133.pdf .
46. MATT Blaze, Ioannidis John, Keromytis Angelos D., Experience with the KeyNote Trust Management System: Applications and Future Directions. In: *Trust Management, First International Conference, Heraklion Crete, Greece*, May 28-30, 2002, Proceedings Publisher Springer Berlin / Heidelberg 2003. Disponibil https://doi.org/10.1007/3-540-44875-6_21 .
47. MUI, Lik. *Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks* (Vol. 1). Ed. M. I. Technology, 2002 Cambridge, MA: Massachusetts Institute Of Technology. Disponibil https://dspace.mit.edu/handle/1721.1/87343 .

48. MUI Lik, MOHTASHEMI Mojdeh, HALBERSTADT Ari. A computational model of trust and reputation. In: *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 2002, pp. 2431-2439. ISBN:0-7695-1435-9. Disponibil https://ieeexplore.ieee.org/document/994181 .
49. *xacml-3.0-core-spec-os-en22*. OASIS. January 2013 Standards. 2013. Disponibil https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf.
50. *About the Object Management Group* Object Management Group. 1997, 11. Disponibil: https://www.omg.org/about/index.htm .
51. *BPMN Information Home*. Object Management Group. 2004, May 3 Disponibil: http://www.bpmn.org/ .
52. *Organizație*. DEX online. Disponibil: https://dexonline.net/definitie-organizație
53. *Organization.* University Cambridge Dictionary: Disponibil https://dictionary.cambridge.org/dictionary/english/organization .
54. *Organization.* Oxford University Disponibil https://www.lexico.com/definition/organization .
55. POPA Ion, BURDUS Eugen. *Fundamentele managementului organizației* ed.3, 2013, Editura Pro Universitaria, București ISBN 978-606-647-770-3
56. PANJUN Sun - Research on cloud computing service based on trust access control International. In: *Journal of Engineering Business Management*. 2020,Volume 12, 1–13 Disponibil https://journals.sagepub.com/doi/pdf/10.1177/1847979019897444 .
57. PITSILIS Georgios, MARSHALL Lindsay. Trust as a key to improving Recommendation Systems. In: *iTrust'05: Proceedings of the Third international conference on Trust Management* ,2005, pp. 210–223. Berlin: Springer-Verlag Berlin, Heidelberg, Germany. Disponibil https://assets.cs.ncl.ac.uk/TRs/875.pdf .
58. Prof. univ. dr. SCHNEIDER Dieter J. G., FLADNITZER Marliese, BIDMON Sonja - Universitatea din Klagenfurt, Austria. Importanța încrederii în companiile virtuale. (E. Economica, Ed.) Management & Marketing(2) (2006)., pp. 37-52. Disponibil http://www.managementmarketing.ro/pdf/articole/12.pdf și https://www.ceeol.com/search/article-detail?id=42742
59. PUSTCHI, Navid , SANDHU Ravi, MT-ABAC: A Multi-Tenant Attribute-Based Access Control Model with Tenant Trust. In: *NSS 2015 - Network and System Security*. 2015, Pag. 206- 220 publisher- Springer International Publishing ISBN - 978-3-319-25645-0, DOI - 10.1007/978-3-319-25645-0_14. Disponibil https://link.springer.com/chapter/10.1007/978-3-319-25645-0_14 .
60. RAJPOOT Qasim Mahmood, JENSEN Christian Damsgaard, KRISHNAN Ram. Integrating Attributes into Role-Based Access Control. In: *DBSec 2015 : 29th Annual IFIP WG 11.3*

Conference on Data and Applications Security and Privacy. 2015, iulie 13-15, pp. 242-249. Fairfax, Virginia, U.S.A. Disponibil https://link.springer.com/chapter/10.1007/978-3-319-20810-7_17 .

61. *RFC 1457* .IEEE . 1993, MAY 25. Disponibil https://www.rfc-archive.org/getrfc?rfc=1457&tag=Security-Label-Framework-for-the-Internet#gsc.tab=0 .
62. RIAD Khaled, YAN Zhu, Hu Honhxin and AHN Gail-Joon. AR-ABAC: A New Attribute Based Access Control Model Supporting Attribute-Rules for Cloud Computing. In: *2015 IEEE Conference on Collaboration and Internet Computing (CIC)*, 2015, pp. 28-35, Hangzhou, R.P. China. doi: 10.1109/CIC.2015.38. Disponibil https://ieeexplore.ieee.org/document/7423062 .
63. RIAD Khaled și YAN Zhu, Multi-Factor Synthesis Decision-Making for Trust-Based Access Control on Cloud. In: *International Jurnal of Cooperative Informations Systems* .2017, Vol. 26 no.04. Disponibil https://doi.org/10.1142/S0218843017500034 .
64. SANDHU Ravi, Lattice-based access control models. In : *Computer*. IEEE. Volume: 26, Issue: 11, Nov. 1993. Print ISSN: 0018-9162 Electronic ISSN: 1558-0814 DOI: 10.1109/2.241422. Disponibil https://dl.acm.org/doi/10.1109/2.241422 .
65. SANDHU Ravi, FERRAIOLO David, KUHN Richard, The NIST Model for Role-Based Access Control: Towards a Unified Standard. In: Proceedings of the fifth ACM workshop on Role-based access control. 2000 pp. 47–63. Berlin: Association for Computing Machinery, New York, NY U.S.A. Disponibil https://doi.org/10.1145/344287.344301 și https://csrc.nist.gov/CSRC/media/Publications/conference-paper/2000/07/26/the-nist-model-for-role-based-access-control-towards-a-unified-/documents/sandhu-ferraiolo-kuhn-00.pdf .
66. SANDHU Ravi, COYNEK Edward J., FEINSTEINK Hal L., YOUMANK. Charles E. Role-Based Access Control Models. In: *Computer*, 1996, octombrie 26, 29(2), pp. 38-47, IEEE. doi:10.1109/2.485845. Disponibil https://csrc.nist.gov/CSRC/media/Projects/Role-Based-Access-Control/documents/sandhu96.pdf .
67. SINGH Ashish și CHATTERJEE Kakali. Trust based access control model for securing electronic healthcare system. In: *Journal of Ambient Intelligence and Humanized Computing*. 2019, Vol. 10**,** pp. 4547–4565. Disponibil https://doi.org/10.1007/s12652-018-1138-z .
68. SINGH Ashish și CHATTERJEE Kakali, An adaptive mutual trust based access control model for electronic healthcare system. In: *Journal of Ambient Intelligence and Humanized Computing*. 2020, Vol 11 **,** pp. 2117–2136 . Disponibil https://doi.org/10.1007/s12652-019-01240-2 .
69. SMARI W.Waleed, CLEMENTE Patrice și LALANDE Jean-Francois, An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system - Future Generation Computer Systems. In: *Future Generation Computer*

Systems. 2014, Volume 31, pp. 147-168. ISSN 0167-739X. Disponibil https://doi.org/10.1016/j.future.2013.05.010 .

70. THIMBLEBY Harold, MARSH Steve, JONES Steve, COCKBURN Andy., Trust in CSCW. In : *Computer-supported Cooperative Work* 1994 pp. 253-271. ISBN 9780429462276. Disponibil https://www.routledge.com/Computer-supported-Cooperative-Work/Scrivener/p/book/9781138616295
71. VOLOCH Nadav., NISSIM Priel, ELMAKIES Mor, GUDES E. A Role and Trust Access Control Model for Preserving Privacy and Image Anonymization in Social Networks. In: *IFIPTM 2019. IFIP Advances in Information and Communication Technology*. 2019 , vol 563, pp. 19-27. Springer. Disponibil https://doi.org/10.1007/978-3-030-33716-2_2 .
72. WATSON Robert, MORRISON Wayne, VANCE Chris, FELDMAN Brian. The Trusted BSD MAC Framework: Extensible Kernel Access Control for FreeBSD 5.0. *In :Proceedings Freenix Track at the 2003 USENIX Annual Technical Conference*. 2003, iunie. pp. 285 -296, USENIX, San Antonio, Texas, USA. Disponibil https://papers.freebsd.org/2003/rwatson-mac_framework.files/rwatson-mac_framework-paper.pdf .
73. Wang Junshee, Wang Han, Zhang Hongbing and Cao Ning. Trust and Attribute-Based Dynamic Access Control Model for Internet of Things. In : *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*. 2017, octombrie 12-14, pp. 342-345. Nanjing, R.P.China . Disponibil https://ieeexplore.ieee.org/document/8250381 .
74. WILSON David R., CLARK David D. A comparison of commercial and military computer security policies; In : *Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP'87)*. 1987 ,mai 27-29, pp. 184–193. Oakland, California U.S.A.
75. *Workflow Patterns. Process Definition Interface -- XML Process Definition Language.* The Workflow Management Coalition. © 2005 [Citat 2019]. Disponibil http://www.workflowpatterns.com/documentation/documents/TC-1025_xpdl_2_2005-10-03.pdf
76. *WORKFLOW CONTROL-FLOW PATTERNS A Revised View* . The Workflow Management Coalition. © 2005 [Citat 2019]. Disponibil http://www.workflowpatterns.com/documentation/documents/BPM-06-22.pdf
77. ZUO Yanjun, PANDA Brabjendra, Component based trust management in the context of a virtual organization. În : *SAC '05: Proceedings of the 2005 ACM symposium on Applied computing*. 2005, martie 13 – 17, pp. 1582-1588. Santa Fe, New Mexico, U.S.A Disponibil https://dl.acm.org/doi/proceedings/10.1145/1066677 .

78. YAMAMOTO Yutaka, 1990.A morality based on trust: some reflections on japanese morality. In : *Philosophy east and west*, Vol. 40, No. 4, Understanding Japanese Values Oct., 1990, pp. 451-469. Honolulu, Hawaii , U.S.A. Disponibil https://www.jstor.org/stable/1399351 .

Anexa 1. Aplicația „Trust analist” pentru crearea politicilor bazate pe încredere

În cadrul firmei Aswic s.r.l. a fost proiectată aplicația „Trust analist” ce are ca scop asistența proiectanților de aplicații în crearea de politici bazate pe „trust”.

Aplicația permite realizarea structurilor xml, necesare implementării politicilor de control bazate pe „trust”. Aplicația a fost realizată pe parcursul anului 2020 și este varianta 1.0.0.

În cele ce urmează vom prezenta succint manualul de utilizare al aplicației.

La pornirea aplicației se lansează fereastra principală ce conține meniul de acces la modulele acesteia.

În imaginea A1, este prezentată fereastra principală.

Figura A1.1. Fereastra principală a aplicației „Trust analist”

Meniul principal este format din următoarele opțiuni:

- Domenii – permite accesarea modulului de actualizare a domeniilor de activitate din cadrul unei organizații.
- Aplicații - accesează modulele de actualizare ale aplicațiilor, proceselor, grupurilor de obiecte și ale obiectelor.
- Administrare utilizatori – permite actualizarea utilizatorilor, și a grupurilor de utilizatori.
- Generare politici – realizează fișierele xml necesare implementării.

- Despre – prezentare a datelor de identificare ale aplicației – vezi figura A2
- Ieșire – închiderea aplicației

Figura A1.2. Despre aplicație

Actualizarea domeniilor de activitate

La selectarea elementului de meniu „Domenii”, se deschide fereastra din figura 3

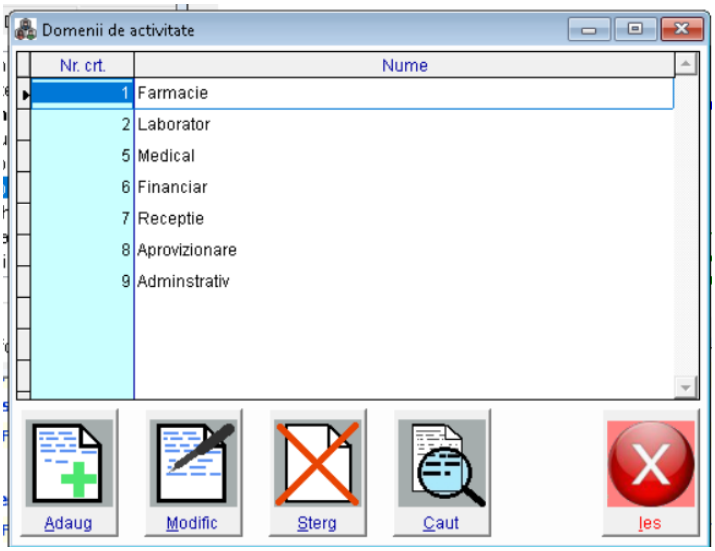


Figura A1.3. Vizualizare/Actualizare domenii de activitate

Fereastra deschisă conține un grid cu numărul curent al domeniului de activitate și denumirea acestuia.

În partea de jos a ferestrei avem butoanele ce permit:

- Adăugarea de domenii noi.
- Modificarea denumirii domeniilor.
- Ștergerea domeniilor.

- Căutarea unui domeniu.
- Închiderea ferestrei.

Prin click pe coloana „Nr. crt.” (număr curent), este selectată înregistrarea ce poate fi modificată sau ștearsă. Pentru toate ferestrele de vizualizare-actualizare utilizate în cadrul proiectului, coloana ce permite selectarea înregistrării asupra căreia se dorește a se acționa este de culoare azur. ( )

Adăugarea/modificarea domeniului se face prin intermediul ferestrei prezentate în figura A4.

Aceasta conține o căsuță text, ce permite adăugarea unui nou domeniului sau permite editarea acelui existent.

Figura A1.4. Fereastra de adăugare-modificare domenii

Butonul „Salvez” permite salvarea datelor adăugate sau modificate, cu închiderea ferestrei.

Butonul „Renunț” permite închiderea ferestrei fără salvarea datelor.

În cadrul aplicației, acest tip de ferestre:

- Vizualizare/actualizare.
- Adăugare/modificare.

a fost aplicat pentru toate modulele ce permit actualizarea datelor necesare generării politicilor de „trust”.

Modulul de actualizare a aplicațiilor.

Fereastra de „Vizualizare/actualizare” (a aplicațiilor are în plus față de fereastra domenii un buton ce permite trecerea către modulul de actualizare a proceselor ce aparțin unei aplicații.

Selecția înregistrărilor ce vor fi adăugate/editate, se face la fel ca la modulul de actualizare a domeniilor de activitate.

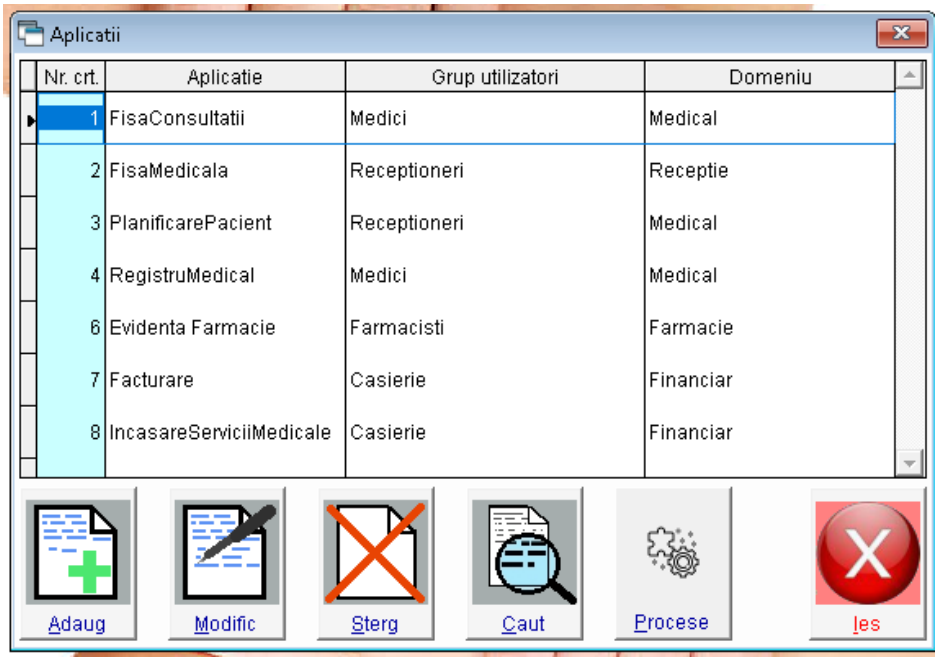


Figura A1.5. Vizualizare-actualizare aplicații

În figura A6 este prezentată fereastra de adăugare/editare aplicații.

Funcționalitatea acesteia este asemănătoare celei descrise anterior, pentru modulul domenii.

Figura A1.6. Adăugare-editare aplicații.

Selecția domeniului, și a grupului de utilizatori asignat aplicației se face prin intermediul unor combo box-uri. (Figurile 7 și 8)

Figura A1.7. Selectare a domeniului căruia îi aparține aplicația.

Figura A1.8. Selectarea grupului de utilizatori ce au acces la aplicație

Butoanele „Salvez” și „Renunț” au aceleași semnificații ca cele descrise mai sus.

Modulul „Procese”

Permite adăugarea și actualizarea proceselor care aparțin aplicației ce este actualizată. Din acest motiv, a fost plasat pe interfața de „Vizualizare/actualizare” a aplicațiilor un buton ce permite vizualizarea/actualizarea proceselor.

În urma apăsării butonului se deschide fereastra de „Vizualizare/actualizare” a proceselor. (Figura A9.)

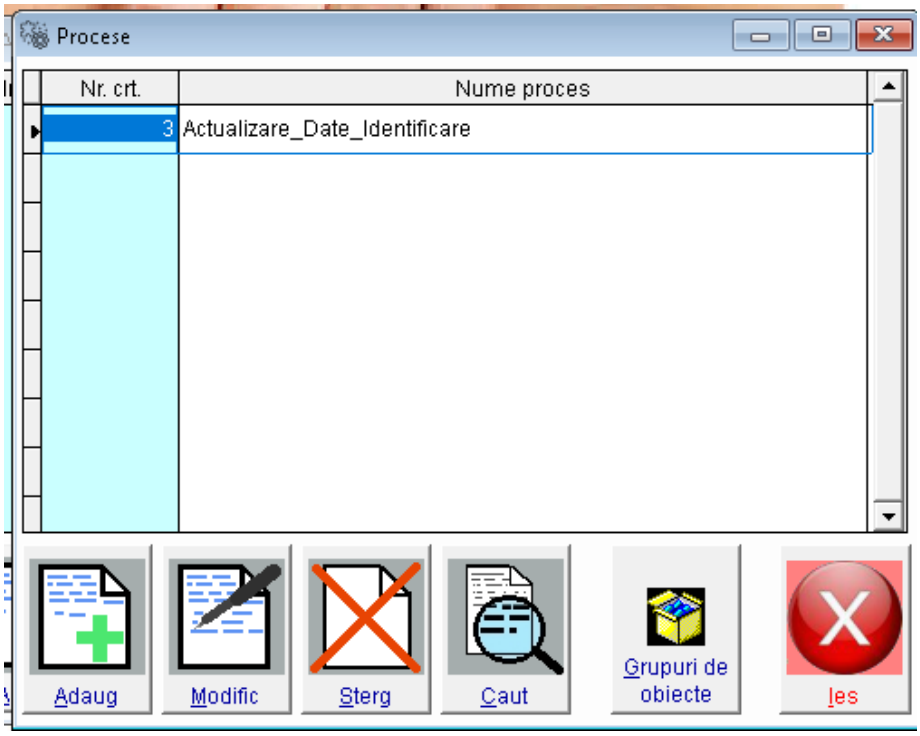


Figura A1.9. Fereastra ”Vizualizare/actualizare” a proceselor unei aplicații

Ca și fereastra ce corespunde aplicațiilor, această fereastră conține un buton de comandă ce permite deschiderea ferestrei de „Vizualizare/actualizare” a grupurilor de obiecte.

Grupurile de obiecte grafice, în cadrul unui proces vizual (de exemplu de „Vizualizare/ actualizare” a datelor), poate fi format din diverse controale și elemente de prezentarea ale datelor, cum ar fi:

- Grid-uri;
- Etichete;
- Casete text;
- Imagini;
- Liste derulante;
- Etc.

Pentru adăugarea/editarea proceselor, a fost creată o fereastră ce permite aceste funcționalități.

Fereastra de adăugare/editare date este prezentată în figura A10, butoanele având funcționalitățile descrise anterior.

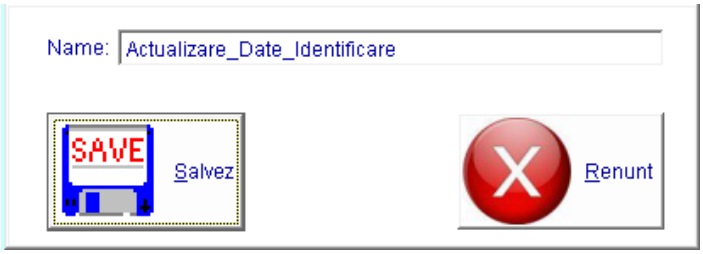


Figura A1.10. Adăugare-editare procese

Modulul de „Vizualizare/actualizare” grupuri de obiecte.

În cadrul unui proces vizual al unei aplicații, sunt grupuri de obiecte ce pot fi supuse sau nu proceselor de vizualizare și interacțiune cu acestea în scopurile vizualizarea, adăugare și modificare a datelor și informațiilor pentru care au fost proiectate.

Aceste grupuri sunt formate din elementele grafice care au fost descrise mai sus și al căror număr este de la 1 la n.

Prin apăsarea butonului 

se deschide fereastra din figura A11 ce conține elementele ce contribuie la aplicarea politicilor ce se aplică grupurilor de obiecte ce participă la procesul căruia îi sunt atribuite.

Aceste elemente sunt tipul de politică, contextul și grupul de utilizatori căruia i se aplică politica.

În cadrul ferestrei de „Vizualizare/actualizare” grupuri de obiecte există butonul 

ce permite accesarea modulului de „Vizualizare/actualizare” obiecte.

Prin apăsarea butoanelor „Adaug” și „Modifica” se deschide fereastra de adăugare-editare grupuri de obiecte se deschide fereastra 12. În această fereastră, prin intermediul unui combo box se selectează grupul de utilizatori ce acționează asupra grupului de obiecte.

Grupul de utilizatori poate avea de la 1 la n membri.

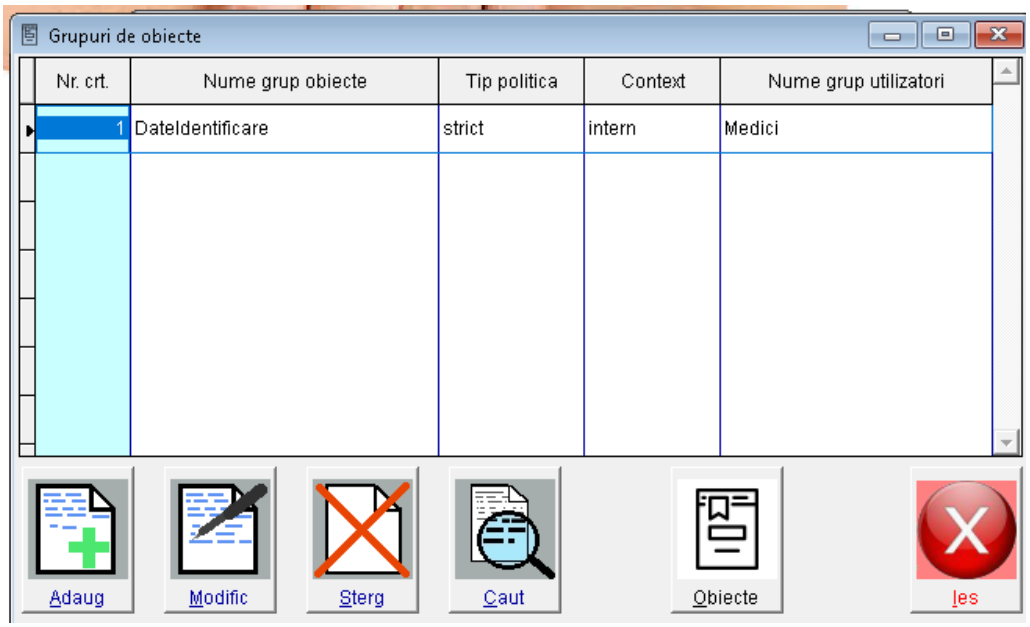


Figura A1.11. ”Vizualizare/actualizare” grupuri de obiecte

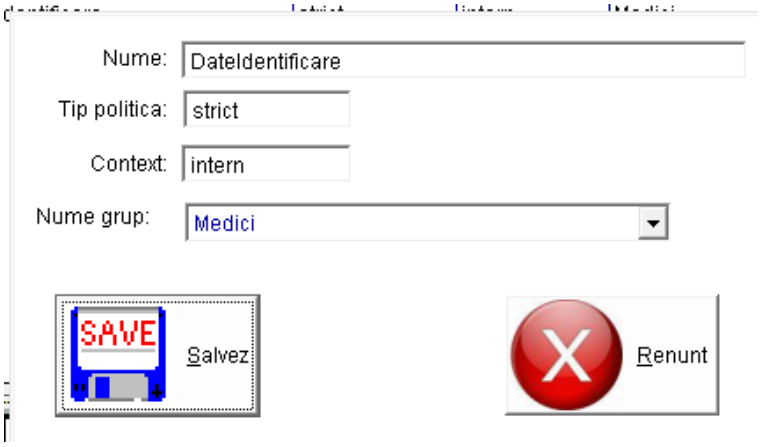


Figura A1.12. Adăugare-editare grupuri obiecte

Modulul de „Vizualizare/actualizare” obiecte

Prin intermediul acestui modul se actualizează obiectele ce aparțin unui grup.

Interfața de „Vizualizare/actualizare” este prezentată în figura A13.

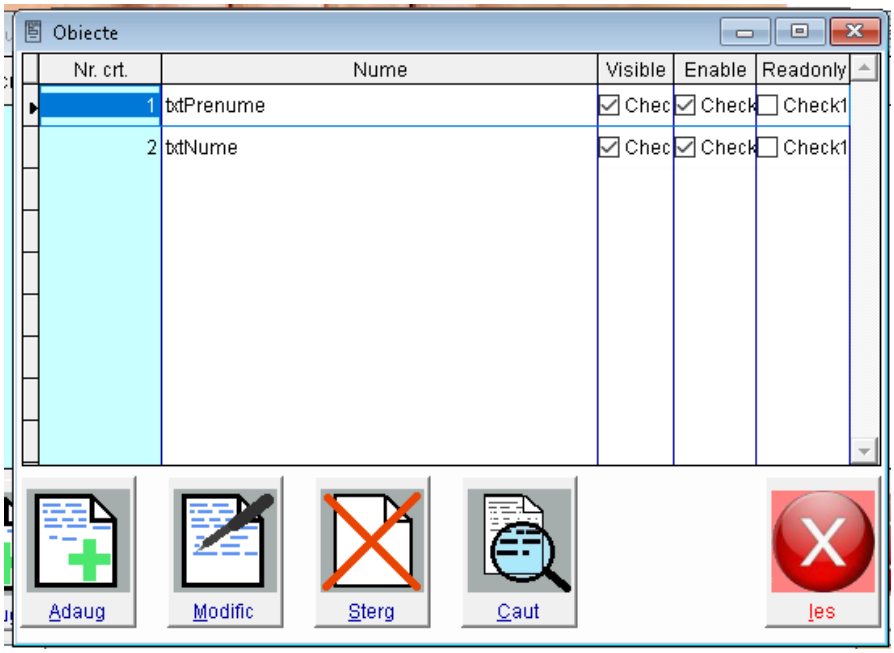


Figura A1.13. Interfața de ”Vizualizare/actualizare”

Funcționalitatea acesteia este asemănătoare cu a celor anterioare, cu excepția faptului că aceasta are în interiorul grid-ului check box-uri ce arată starea proprietăților obiectului ce va fi accesat de un grup de utilizatori, ce are de la 1 la n membri.

În figura A14 este prezentată interfața grafică ce permite adăugarea-editarea datelor unui obiect.

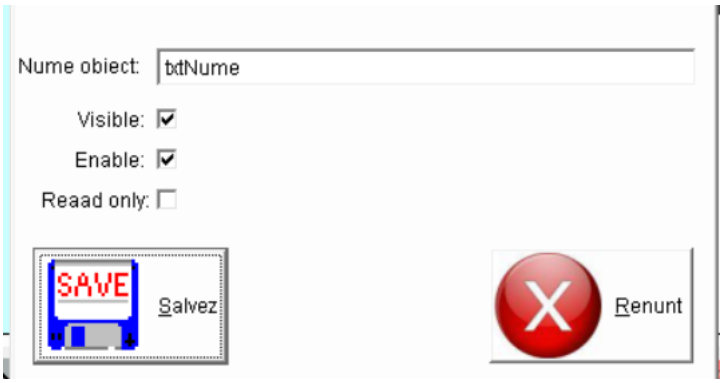


Figura A1.14. Adăugare-editare a datelor necesare unui obiect

Administrarea utilizatorilor aplicației

Pentru gestionarea utilizatorilor și a grupurilor de utilizatori, se utilizează butonul 3 al meniului din fereastra principală. (figura A15)

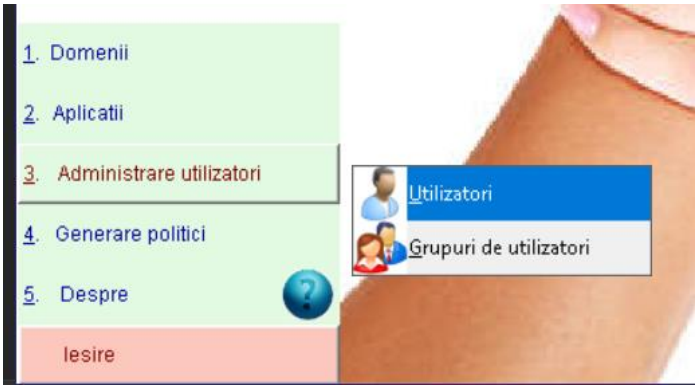
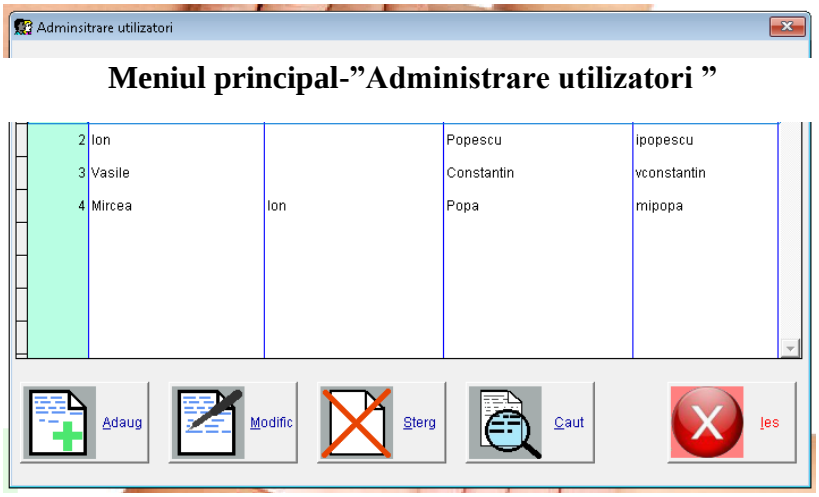


Figura A1.15. Meniul principal-"Administrare utilizatori "

Modulul pentru utilizatori

In figura A16 este prezentată interfața de „Vizualizare/actualizare" a datelor utilizatorilor.



Meniul principal-"Administrare utilizatori "

Figura A1.16. Fereastra de "Vizualizare/actualizare" utilizatori

Funcționalitatea butoanelor cât și selecția înregistrărilor, se fac cum am prezentat mai sus.

În figura A17, este prezentată interfața de adăugare-editare a utilizatorilor aplicației.

Butoanele de comandă au aceeași funcționalitate ca la interfețele anterioare.

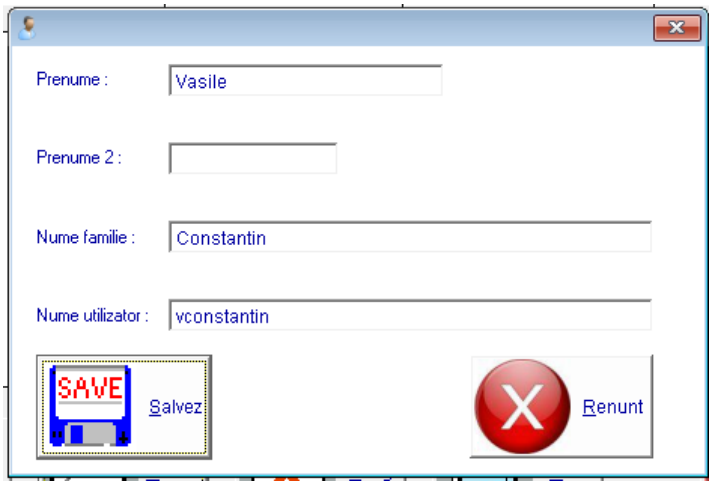


Figura A1.17. Interfața de adăugare-editare utilizator

Modulul pentru grupuri de utilizatori

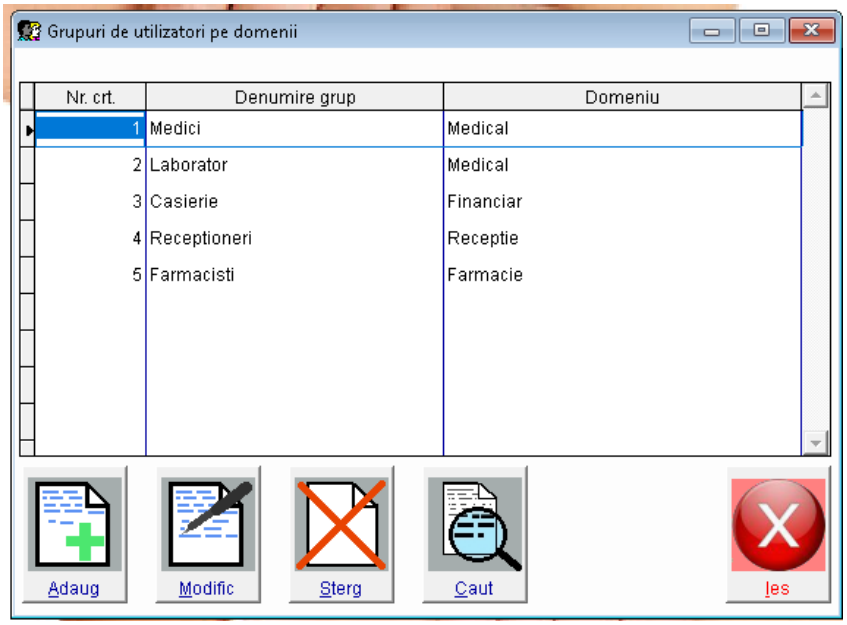


Figura A1.18. Vizualizare-actualizare" grupuri de utilizatori

În figura de mai sus prezentăm interfața pentru grupurile de utilizatori, modulul de „Vizualizare/actualizare” iar în figura A19 interfața grafică pentru „adăugare-editare” grupuri de utilizatori.

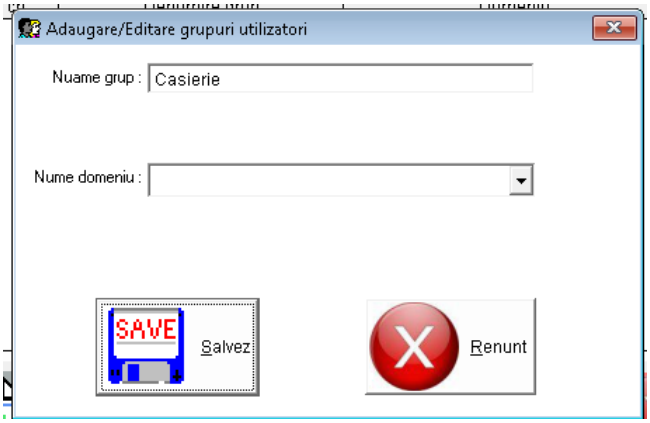


Figura A1.19. Adăugare-editare grupuri de utilizatori

Selectarea domeniului căruia îi aparține grupul de utilizatori, se face prin intermediul unui combo box, cum a fost arătat mai sus.

Generarea politicilor de control al accesului și acțiunilor

Prin selecția elementului 4 din meniul principal din pagina principală a aplicației „Trust analist” se generează din înregistrările din baza de date politicile pentru aplicațiile înregistrate.

În lista de mai jos prezentăm un exemplu de fișier xml.

```
<?xml version="1.0" encoding="utf-8"?>
<Domain>Receptie
  <applications>fisa_medicala
    <usersgroups>receptie</usersgroups>
    <processes>actualizare_date_identificare
      <objectsgroups policytype="strict" context="intern">date_identificare
        <object1 name="lblfirstname" visible=".t." enabled=".t." readonly=".t."/>
        <object2 name="txtfirstname" visible=".t." enabled=".t." readonly=".f."/>
        <object3 name="lblname" visible=".t." enabled=".t." readonly=".t."/>
        <object4 name="txtname" visible=".t." enabled=".t." readonly=".f."/>
        <object5 name="lbladdress" visible=".t." enabled=".t." readonly=".t."/>
        <object6 name="txtaddress" visible=".t." enabled=".t." readonly=".f."/>
        <object7 name="lblciseria" visible=".t." enabled=".t." readonly=".t."/>
        <object8 name="txtciseria" visible=".t." enabled=".t." readonly=".f."/>
        <object9 name="lblcinr" visible=".t." enabled=".t." readonly=".t."/>
```

```
            <object10 name="txtcinr" visible=".t." enabled=".t." readonly=".f."/>
            <object11 name="lbltelefon1" visible=".t." enabled=".t." readonly=".t."/>
            <object12 name="txttelefon1" visible=".t." enabled=".t." readonly=".f."/>
             <object13 name="lbltelefon2" visible=".t." enabled=".t." readonly=".t."/>
            <object14 name="txttelefon2" visible=".t." enabled=".t." readonly=".f."/>
            <object15 name="cmdSave" visible=".t." enabled=".t." readonly=".t."/>
            <object16 name="txtExit" visible=".t." enabled=".t." readonly=".t."/>
        </objectsgroups>
    </processes>
  </applications>
</Domain>
```

Anexa 2. Imagini

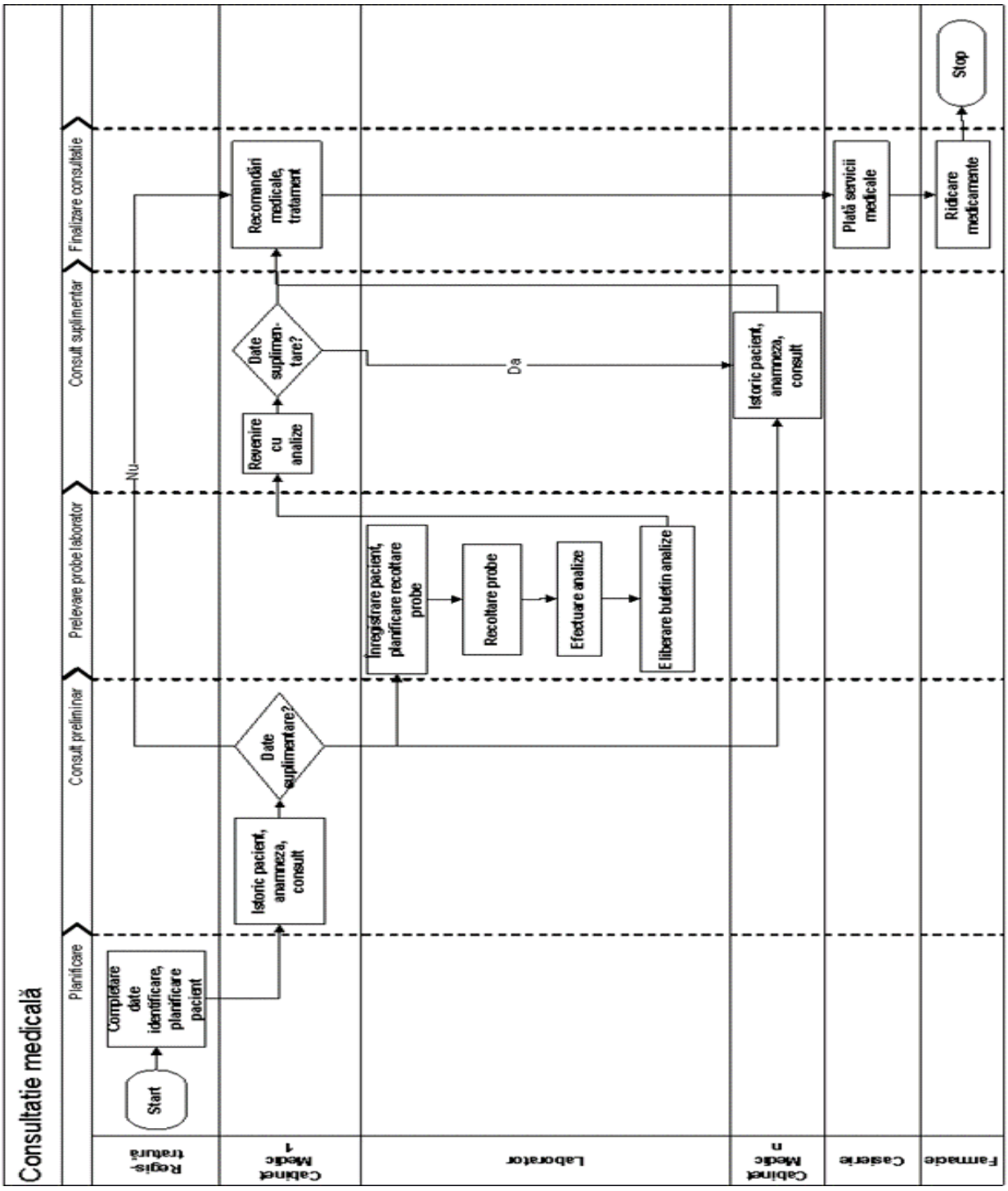


Figura A2.1. Fluxul de lucru într-o organizație medicală

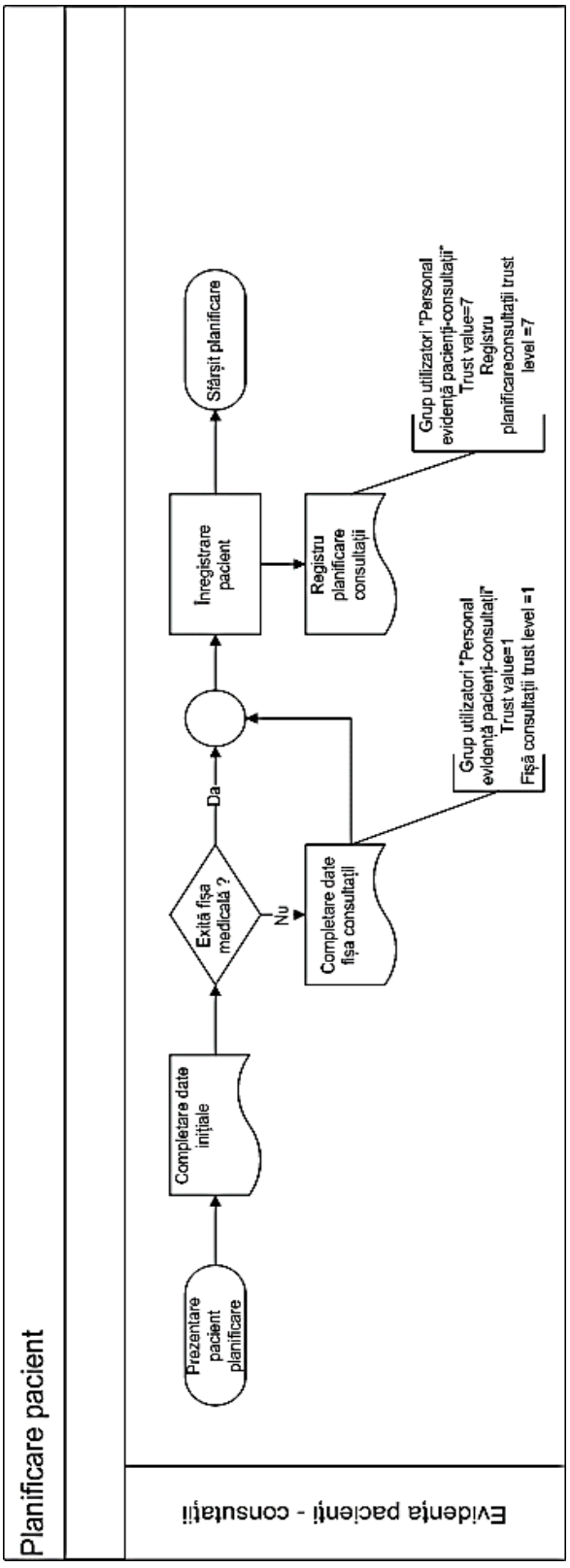


Figura A2.2. Procesul de înregistrare planificare pacient

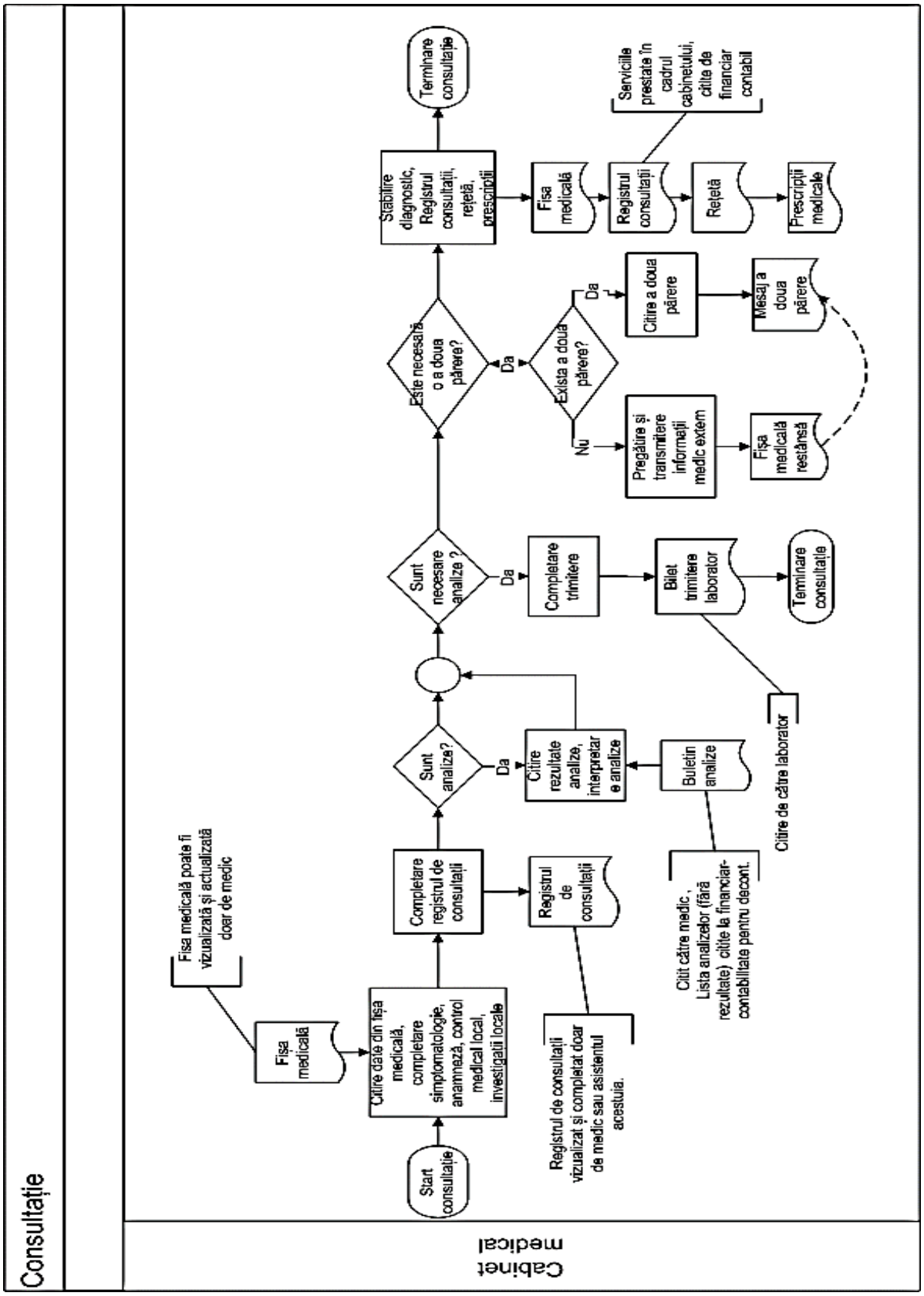


Figura A2.3. Procesele controlului medical

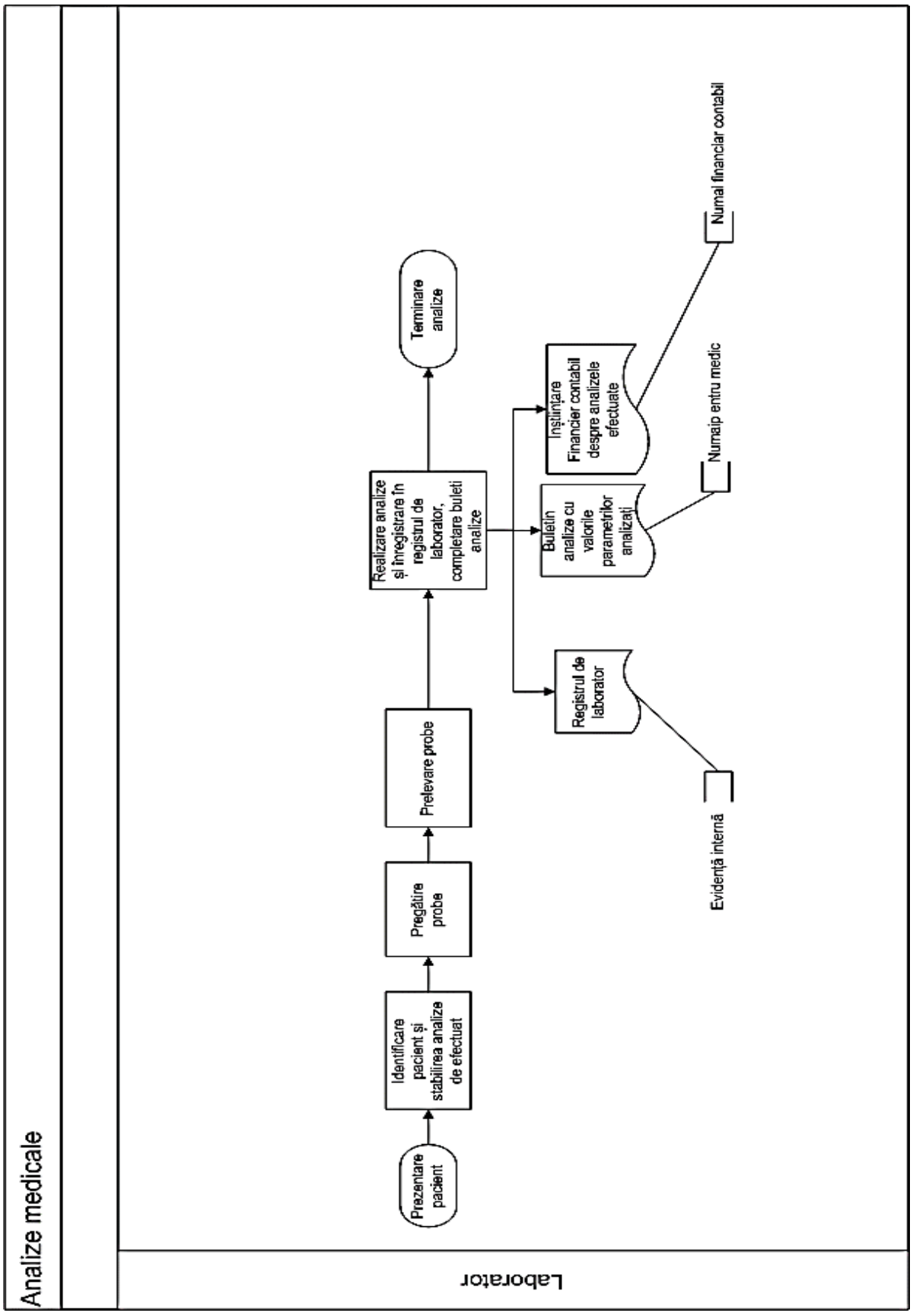


Figura A2.4. Procesele analizelor medicale

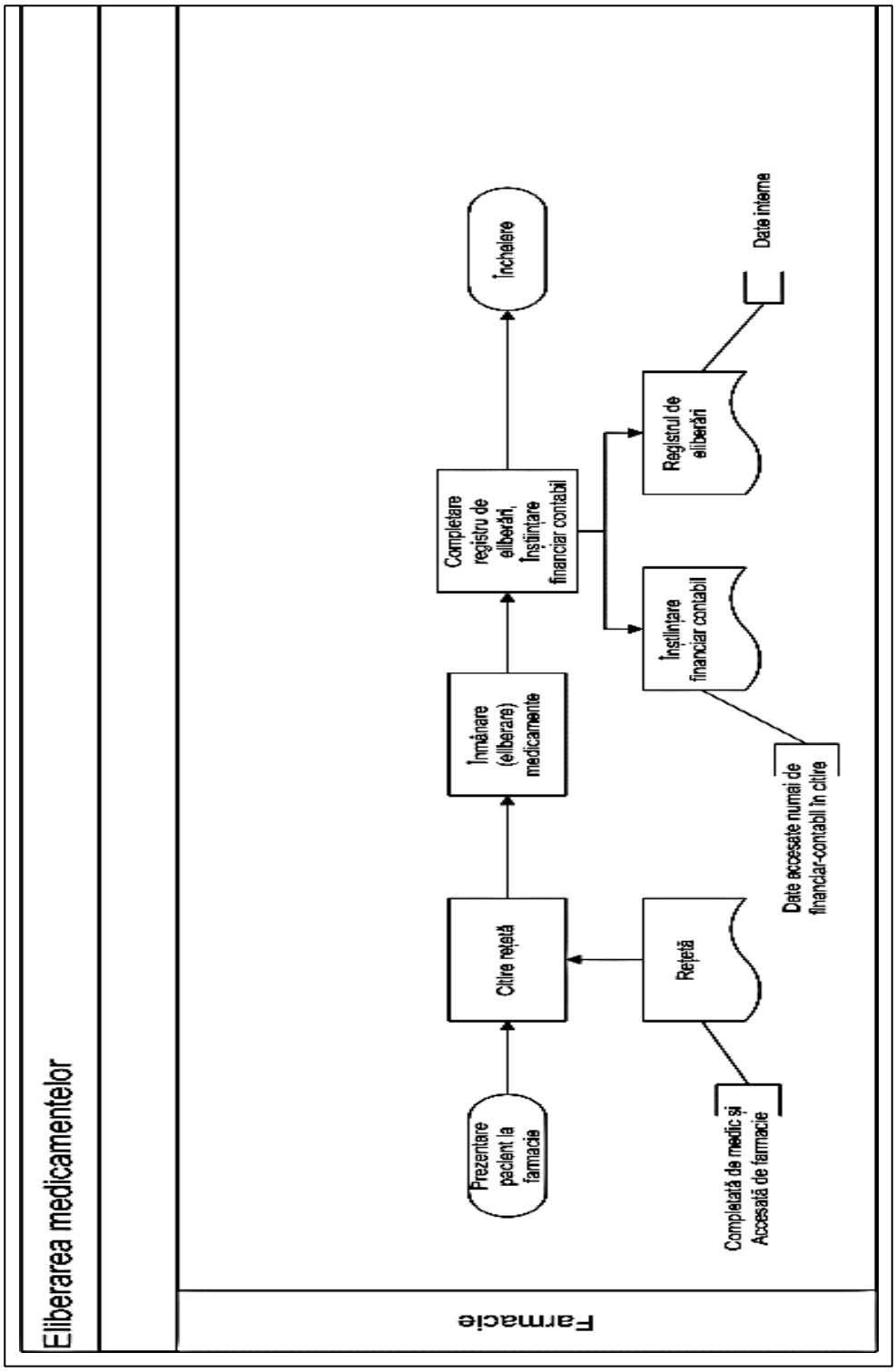


Figura A2.5. Procesele de eliberare a tratamentelor din farmacie

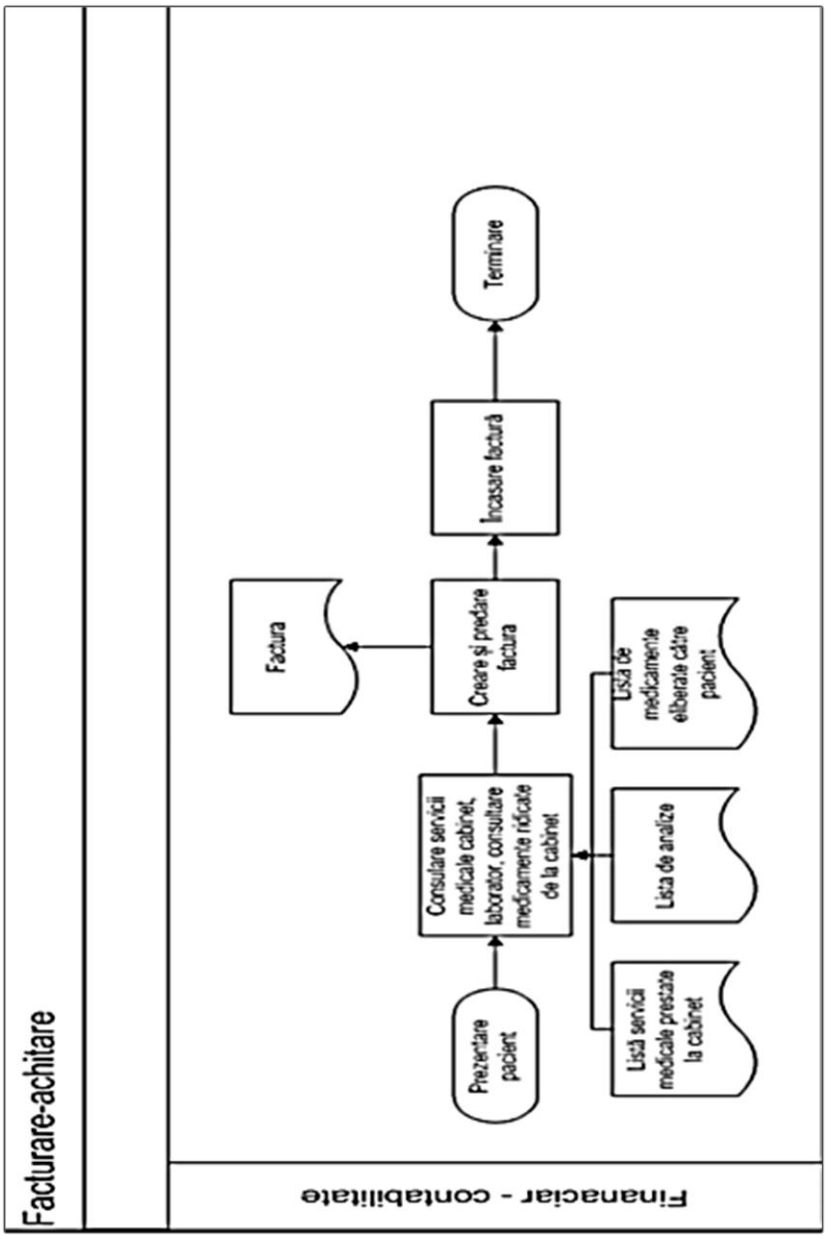


Figura A2.6. Procesele de facturare

Anexa 3. Tabele

Tabelul A3.1. Grupurile obiectelor la care au acces grupurile de utilizatori, și acțiunile permise

Nr. crt.	Date	Tipuri de date	Grup de utilizatori	Procese posibile					
				creare	consultare	modificare	adăugare	imprimare	arhivare
1	Date identificare pacient, date planificare consultație, date specialitate și medic	Inițiale și identificare	evidență pacienți-consultații	X	X	X	X	X	X
			medic (context intern)	-	X	-	-	-	-
			medic (context extern)	-	-	-	-	-	-
			laborator	-	X	-	-	-	-
			financiar-contabil	-	X	-	-	-	-
			farmacie	-	X	-	-	-	-
2	Completare date despre pacient, date medicale istoric familial și personal, simptomatologie.	Istoric medical	registratură	-	X	-	-	-	X
			medic cabinet	X	X	X	X	X	-
			medic extern	-	X	-	-	-	-
			laborator	-	-	-	-	-	-
			financiar-contabil	-	-	-	-	-	-
			farmacie	-	-	-	-	-	-
3	Diagnostic prezumtiv, investigații necesare	Diagnostic prezumtiv, analize propuse	registratură	-	-	-	-	-	X
			medic cabinet	X	X	X	X	X	-
			medic extern	-	X	-	-	-	-
			laborator	-	X	-	-	-	-
			financiar-contabil	-	-	-	-	-	-
			farmacie	-	-	-	-	-	-
4	Date de identificare buletin analize, parametrii analizați valori obținute	Rezultate	registratură	-	-	-	-	-	X
			medic cabinet	-	X	-	-	-	-
			medic extern	-	X	-	-	-	-
			laborator	X	X	X	X	X	-
			financiar-contabil	-	X	-	-	-	-
			farmacie	-	-	-	-	-	-
5	Date de identificare rețetă, diagnostic, medicamente prescrise cu cantitatea și modul de administrare, recomandări și prescrieri medicale, concediul medical și serviciile prestate în cabinet.	Diagnostic final, tratamente medicale, medicație	registratură	-	-	-	-	-	X
			medic cabinet	X	X	X	X	-	-
			medic extern	X	X	X	X	-	-
			laborator	-	-	-	-	-	-
			financiar-contabil	-	-	-	-	-	-
			farmacie	-	X	X	X	X	-

Tabelul A3.1. Grupurile obiectelor la care au acces grupurile de utilizatori, și acțiunile permise (continuare)

Nr. crt.	Date	Tipuri de date	Grup de utilizatori	Acțiuni posibile					
				creare	consultar	modificar	adăugare	imprimar	arhivare
6	Datele de identificare plătitor, facturare a costurilor serviciilor efectuate.	Costuri servicii medicale	registratură	-	-	-	-	-	-
			medic cabinet	-	-	-	-	-	-
			medic extern	-	-	-	-	-	-
			laborator	-	-	-	-	-	-
			financiar-contabil	-	X	X	X	X	X
			farmacie	-	-	-	-	-	-

Anexa 4. Fișierul *fisa_medicală.xml*

```
<?xml version="1.0" encoding="utf-8"?>
<document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="fisa_medicala.xsd">
  <document_type>fisa_medicală</document_type>
  <domains>medical,evidenta_pacienti_consultatii</domains>
  <sensivity>medium</sensivity>
  <general_trust_level_process>read</general_trust_level_process>
  <policy>hibrid</policy>
  <patient>
    <firstname> </firstname>
    <lastname> </lastname>
    <gender> </gender>
    <age> </age>
    <birthday> </birthday>
    <marital_status </marital_status>
    <cnp> </cnp>

<domains_access>medical,evidenta_pacienti_consultatii</domains_access>
    <context>local</context>
    <domain_process>evidenta_pacienti_consultatii</domain_process>
    <trust_process>read,modify</trust_process>
  </patient>
  <patient_address>
    <street> </street>
    <number> </number>
    <block> </block>
    <building_stairs> </building_stairs>
    <floor> </floor>
    <apartment> </apartment>

<domain_access>medical,evidenta_pacienti_consultatii</domain_access>
    <context>local</context>
```

```
    <domain_process>evidenta_pacienti_consultatii</domain_process>
    <trust_process>modify</trust_process>
  </patient_address>
  <medical_data>
    <workplace> </workplace>
    <job> </job>
    <job_condition> </job_condition>
    <antecedent_collateral_inheritance>
</antecedent_collateral_inheritance>
    <personal_background>s </personal_background>

<domains_access>medical,evidenta_pacienti_consultatii</domains_access>
    <context>any</context>
    <domain_process>medical</domain_process>
    <trust_process>modify</trust_process>
  </medical_data>
  <consultatii>
    <record>
      <current_number> </current_number>
      <consulting_date> </consulting_date>
      <symptoms> </symptoms>
      <diagnostic> </diagnostic>
      <prescriptions>   </prescriptions>
      <remarks> </remarks>
    </record>
    <record>
      <current_number> </current_number>
      <consulting_date> </consulting_date>
      <symptoms>simptome  </symptoms>
      <diagnostic> </diagnostic>
      <prescriptions> </prescriptions>
      <remarks> </remarks>
    </record>
```

```
    <domains_access>medical</domains_access>
    <context>any</context>
    <domain_process>medical</domain_process>
    <trust_processs>create,read,modify</trust_processs>
  </consultatii>
</document>
```

Schema de validare pentru fișei medicale a pacienților este prezentată mai jos.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault = „qualified">
  <xs:element name="document">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="document_type" type="xs:string"/>
        <xs:element name="domains" type="xs:string"/>
        <xs:element name="sensivity" type="xs:string"/>
        <xs:element name="general_trust_level_process"
type="xs:string"/>
        <xs:element name="policy" type="xs:string"/>
        <xs:element ref="patient"/>
        <xs:element ref="patient_address"/>
        <xs:element ref="medical_data"/>
        <xs:element ref="consultatii"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="patient">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="firstname" type="xs:string"/>
        <xs:element name="lastname" type="xs:string"/>
        <xs:element name="gender" type="xs:string"/>
```

```
      <xs:element name="age" type="xs:string"/>
      <xs:element name="birthday" type="xs:string"/>
      <xs:element name="marital_status" type="xs:string"/>
      <xs:element name="cnp" type="xs:string"/>
      <xs:element name="domains_access" type="xs:string"/>
    <xs:element name="context" type="xs:string"/>
      <xs:element name="domain_process" type="xs:string"/>
      <xs:element name="trust_process" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="patient_address">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="street" type="xs:string"/>
      <xs:element name="number" type="xs:string"/>
      <xs:element name="block" type="xs:string"/>
      <xs:element name="building_stairs" type="xs:string"/>
      <xs:element name="floor" type="xs:string"/>
      <xs:element name="apartment" type="xs:string"/>
      <xs:element name="domain_access" type="xs:string"/>
    <xs:element name="context" type="xs:string"/>
      <xs:element name="domain_process" type="xs:string"/>
      <xs:element name="trust_process" type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="medical_data">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="workplace" type="xs:string"/>
      <xs:element name="job" type="xs:string"/>
      <xs:element name="job_condition" type="xs:string"/>
```

```
        <xs:element name="antecedent_collateral_inheritance"
type="xs:string"/>
        <xs:element name="personal_background" type="xs:string"/>
        <xs:element name="domains_access" type="xs:string"/>
     <xs:element name="context" type="xs:string"/>
        <xs:element name="domain_process" type="xs:string"/>
        <xs:element name="trust_process" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="consultatii">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="record" maxOccurs="unbounded"/>
        <xs:element name="domains_access" type="xs:string"/>
     <xs:element name="context" type="xs:string"/>
        <xs:element name="domain_process" type="xs:string"/>
        <xs:element name="trust_processs" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="record">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="current_number" type="xs:string"/>
        <xs:element name="consulting_date" type="xs:string"/>
        <xs:element name="symptoms" type="xs:string"/>
        <xs:element name="diagnostic" type="xs:string"/>
        <xs:element name="prescriptions" type="xs:string"/>
        <xs:element name="remarks" type="xs:string"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
```

```
</xs:schema>
```

Anexa 5. Certificat de implementare a controlului accesului și acțiunilor utilizatorilor bazat pe ierarhii de încredere

ROMÂNIA
Academia de Ştiinţe Agricole şi Silvice „Gheorghe Ionescu - Şişeşti"
INSTITUTUL DE CERCETARE – DEZVOLTARE PENTRU ECOLOGIE ACVATICĂ, PESCUIT ŞI ACVACULTURĂ – GALAŢI
CUI: 14785680, Str. Portului nr.54, 800211, Galaţi, ROMÂNIA
Tel: 0236 416 914, Fax: 0236 414 270,
email: ICDEAPA.Galati@asas.ro / website: www.icdeapa.ro

Institutul de Cercetare - Dezvoltare pentru Ecologie Acvatică, Pescuit și Acvacultură Galați
Intrare ..... Ieșire 5.03....
Anul 2021 Luna 02 Ziua 09

Către,

S.C. ASWIC S.R.L. Galați

În atenția d-lui ing. Marcel DANILESCU

Prin prezenta adeverim faptul că dl ing. Marcel DANILESCU, reprezentat al firmei S.C. ASWIC S.R.L. Galați, a proiectat și implementat soluții de control al accesului și acțiunilor utilizatorilor bazate pe apartenența la domenii de activitate și pe ierarhii de acțiuni în cadrul contractelor desfășurate în parteneriat cu instituția noastră.

DIRECTOR GENERAL,

CS III dr. ing.
Floricel Maricel DIMA

COORDONATOR P.N.C.D.

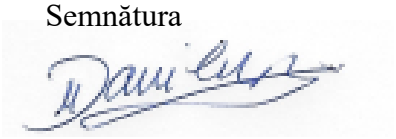
CS III dr. ing.
Magdalena TENCIU

DECLARAȚIA PRIVIND ASUMAREA RĂSPUNDERII

Subsemnatul, declar pe proprie răspundere că materialele prezentate în teza de doctorat sunt rezultatul propriilor cercetări și realizări științifice, în caz contrar urmând să suport consecințele, în conformitate cu legislația în vigoare.

Danilescu Marcel

Semnătura



Data: 07.10.2020

CURRICULUM VITAE

Informații personale	
Nume/prenume	**Marcel Danilescu**
Adresa	800173 Galați, România, Str. Luceafărului nr. 15
Telefon	00 40 721042950 Fax 00 40 236415034
E-mail	marcel.danilescu@aswic.ro
Naționalitate/Cetățenie	Română/Română
Data nașterii	27.05.1957
Domenii de interes științific	Modelarea și auditul sistemelor de securitate informatică. Analiză, proiectare și implementare de sisteme informatice. Analiză, proiectare și implementare de aplicații complexe de baze de date.

Educație și formare	
Perioada	**2008 - prezent**
Calificarea/diploma	Doctorand
Competențe profesionale	Cercetări în domeniul „Tehnologii XML aplicate în securitatea datelor”
Instituția	Universitatea Tehnică a Moldovei Facultatea de Calculatoare, Informatică și Microelectronică
Perioada	**2003-2005**
Calificarea/diploma	Masterat în informatică aplicată
Competențe profesionale	Programare: SQL, Java, Inteligență Artificială, Sisteme de operare
Instituția	Universitatea „Dunărea de Jos” Galați - Facultatea de Știința Calculatoarelor
Perioada	**1977 - 1983**
Calificarea/diploma	Inginer diplomat
Competențe profesionale	Inginer mecanic
Instituția	Universitatea „Dunărea de Jos” din Galați - Facultatea de Mecanică
Perioada	**2013**
Calificarea/diploma	Auditor în domeniul calității / Auditor al sistemelor de management al securității informaționale conform cerințelor standardelor SR EN ISO 19011:2011 și SR ISO CEI 27001:2006 –
Instituția	SUNCERT – Organism de Certificare Sisteme de Management
Perioada	**1999**
Calificarea/diploma	Certificate of Excellence „**Microsoft Certified Professional**”
Competențe profesionale	Supporting Microsoft Windows NT Core Technologies Administering Microsoft Windows NT Internetworking Microsoft TCP/IP on Microsoft Windows NT Supporting Microsoft Windows NT Enterprise Technologies
Instituția	LOGIMAX

Activitatea profesională	
Perioada	**2009 - Prezent**
Funcția / Instituția	Research manager / ASWIC srl
Perioada	**2008 - 2009**
Funcția / Instituția	Inginer de sistem - Șef stație calcul / Institutul de Cercetare-Dezvoltare pentru Ecologie Acvatică, Pescuit și Acvacultură Galați
Perioada	**2004 - 2008**
Funcția / Instituția	Consilier superior / Agenția Regională de Protecția Mediului (REPA) – Galați
Perioada	**2002 –2004**

Funcția / Instituția	ECDL (European Computer Driving License) -ROMANIA – reprezentant regional
Perioada	**2000 –2002**
Funcția / Instituția	Referent specialitate informatician / Banca Națională a României – sucursala Galați
Perioada	**1999 - 2000**
Funcția / Instituția	Analist programator / BANKCOOP – Galați
Perioada	**1996 - 1999**
Funcția / Instituția	Analist programator / R.A. Loteria Națională Română – Sucursala Galați
Perioada	**1994 - 1996**
Funcția / Instituția	General Manager / INFOLINX SRL
Perioada	**1992 - 1994**
Funcția / Instituția	șef oficiu de calcul- analist programator / Direcția de Poștă Galați
Perioada	**1990 - 1992**
Funcția / Instituția	Analist programator / Direcția de muncă și protecție socială – Galați
Perioada	**1990**
Funcția / Instituția	inginer de sistem / Centrul de Calcul al Centralei Industriale Navale
Perioada	**1983 - 1990**
Funcția / Instituția	Inginer proiectant / MENAROM S.A. Galați
Perioada	**1983**
Funcția / Instituția	Inginer stagiar / KOYO - RULMENTUL Alexandria
Limba maternă	**Româna**
Limbi străine cunoscute	**Engleza, Franceza**

Auto-evaluare	Înțelegere				Vorbire				Scriere	
Nivel european (*)	Ascultare		Citire		Participare la conversație		Discurs oral		Exprimare scrisă	
Engleză	C1	Proficient user	C1	Proficient user	B2	Independent user	B2	Independent user	B2	Independent user
Franceză	B2	Independent user	B2	Independent user	B1	Independent user	B1	Independent user	B1	Independent user
(*) Common European Framework of Reference for Languages										

Proiecte recente

- PNCD din sectorul pescuitului 2008-2011
- PNCD 2010 – Dezvoltare de software pentru baze de date
- PNCD 2009-2010 - Proiectarea si realizarea sistemului de securizare a datelor de pe serverul I.C.D.E.A.P.A. Galați, aferent Bazei de date a PNCD
- PNCD din sectorul pescuitului 2011-2013
- PNCD 2012 – Revizuire software pentru sistem integrat de culegere si raportare a datelor
- PNCD 2013 - Sistem dinamic pentru crearea de rapoarte în baza de date
- PNCD 2014 - Implementarea programului național pentru colectarea, gestionarea și utilizarea datelor în sectorul pescăresc al României pentru anul 2014, programului de lucru și rapoartelor anuale – tehnic și financiar., Obiectivul V - *Gestionarea și utilizarea datelor:*
- PNCD 2015-2018 - Contract de cercetare pentru realizarea si implementarea Programului Național pentru Colectarea, Gestionarea și Utilizarea Datelor din sectorul pescăresc al României pentru perioada 2015-2018 (PNCD), Obiectivul V-Gestionarea si utilizarea datelor