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 ŞI SISTEME INFORMAŢIONALE

Rezumatul tezei de doctor în informatică

CHIŞINĂU, 2021
Teza a fost elaborată în cadrul departamentului ”Inginerie software și automatică”
Facultatea ”Calculatoare, Informatică şi Microelectronică”
a Universităţii Tehnice a Moldovei

Conducător ştiinţific:
Beşliu Victor – doctor în științe tehnice, profesor universitar
Referenţi oficiali:
PALADI Florentin - doctor habilitat in științe fizico-matematice, profesor universitar,
ARITON Viorel - doctor inginer, profesor universitar, Universitatea "Danubius" din Galați, (România).
Componenţa Consiliului Ştiinţific Specializat:
BOSTAN Viorel – doctor habilitat în științe tehnice, profesor universitar, UTM– **preşedinte CŞS**,
FIODOROV Ion, doctor în științe tehnice, conferențiar universitar, UTM - **secretar ştiintific**,
GAINDRIC Constantin, doctor habilitat în informatică, profesor universitar, Membru Corespondent al AŞM, Institutul de Matematică şi Informatică "Vladimir Andrunachievici",
BOLUN Ion, doctor habilitat în informatică, profesor universitar, UTM,
Costaș Ilie – doctor habilitat în informatică, profesor universitar, ASEM,
PENTIUC Stefan-Gheorghe, doctor inginer, profesor universitar, Universitatea "Ștefan cel Mare" din Suceava, (România),
MARUSIC Galina, doctor în informatica, conferentiar universitar, UTM.

Susţinerea va avea loc la 14.01.2022, ora 15.00, în Şedinţa Consiliului Ştiinţific Specializat D 232.02-21-44 din cadrul Universităţii Tehnice a Moldovei pe adresa: str. Studenților, 9/7, corpul de studii nr. 3, aula 3-3, Chişinău, Republica Moldova, MD-2045.

Teza de doctor şi rezumatul pot fi consultate la Biblioteca tehnico-ştiinţifică a Universităţii Tehnice a Moldovei şi pe pagina web a CNAA (www.cnaa.md/anacec.md).

Rezumatul a fost expediat la " " decembrie 2021

Secretar ştiinţific al Consiliului Ştiinţific Specializat,
FIODOROV Ion, dr., conf. univ. _____
Conducător ştiinţific,
Beşliu Victor, dr., prof. univ. _____
Autor
Marcel Danilescu _____

REPERE CONCEPTUALE ALE CERCETĂRII

Actualitatea temei

Pentru orice organizaţie, informaţia în format obișnuit sau electronic, fie că este vorba de baze de date, informaţii financiare, date contabile, profilurile angajaţilor şi multe alte documente publice sau cu diferite nivele de clasificare, reprezintă una dintre cele mai importante active.

Necesitatea de informare presupune şi o protecţie a informaţiilor, pentru a nu permite devoalarea unor informaţii sensibile, la niveluri de competenţă care nu au capacitatea de prelucrare şi păstrare a confidențialității datelor. Prin urmare, este foarte importantă politica de asigurare a confidenţialității și integrității datelor.

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

Descrierea situaţiei în domeniul de cercetare

Lucrările de cercetare, publicate până în anii 2010, privind cuantificarea încrederii și reputației unui agent sau utilizator în cadrul unei organizații, s-au oprit în punctul în care această cuantificare poate fi aplicată la nivelul sistemelor informaționale. De aici a rezultat necesitatea continuării cercetării, prin definirea cerințelor de cercetare:

- Cum se concretizează, din punctul de vedere al aplicării în sistemele informaționale, încrederea cuantificată, acordată la nivel de utilizator ?
- Cum se poate determina nivelul de acces al utilizatorului la resursele informaționale ale organizației?
- Cum se pot aplica restricțiile de acces ale utilizatorului la obiectele informaționale, prin intermediul unei interfețe grafice cu comportament dinamic?

Scopul lucrării

Ipoteza de lucru stabilită este modelarea controlului accesului la documente și a acțiunilor asupra documentelor, 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 informațional, 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 ştiinţifice

Pornind de la ipoteza de lucru enunțată, 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.

Noutatea și originalitatea științifică constă în dezvoltarea unei noi metode, pe baza relațiilor de încredere, prin care se asigură confidențialitatea și integritatea datelor și informațiilor, prin intermediul politicilor de control al accesului și acțiunilor bazate pe încredere. 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 ştiinţifică soluţionată constă în găsirea metodelor de aplicare a valorilor de încredere acordate utilizatorilor, pentru accesarea datelor și informațiilor din sistemele informatice ale organizației și crearea de procese informatice care acționează asupra acestora.

Semnificaţia teoretică. Studiile și cercetările efectuate au condus la formularea unor noi paradigme: niveluri și valori de încredere și stabilirea condițiilor de aplicare a politicilor de încredere, care vor constitui puncte de pornire pentru cercetările viitoare.

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. A fost realizată aplicația „Trust analist”, care permite crearea politicilor bazate pe încredere și implementează conceptele și modelele dezvoltate în urma cercetărilor efectuate, aplicație utilizată în activitatea diferitor organizați.

Rezultatele ştiinţifice înaintate spre susţinere:

1. Definirea valorii de încredere, a contextului de încredere, a relației de încredere și a ierarhiilor și subierarhiilor 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.

Implementarea rezultatelor ştiinţifice a fost realizată în cadrul proiectelor de cercetare-dezvoltare, în parteneriat cu Institutul de Cercetare-Dezvoltare

pentru Ecologie Acvatică, Pescuit și Acvacultură din Galați, institut ce a condus un consorțiu de cercetare din domeniul pisciculturii și industriei de prelucrare a peștelui. Proiectele s-au derulat pe parcursul a 10 ani (2009-2019).

Aprobarea rezultatelor cercetărilor. Rezultatele tezei au fost validate în cadrul lucrărilor publicate în reviste internaţionale şi naţionale:

- Revista Journal of Engineering Sciences. Vol. XXVIII, no. 2 (2021), pp. 67 - 78. ISSN 2587-3474 / ISSNe 2587-3482, Chișinău, Republica Moldova
- Revista Journal of Social Sciences Vol. III, no.3 (2020), pp.72-84, ISSN 2587-3490, eISSN 2587-3504, Chișinău, Republica Moldova
- The Journal of Accounting and Management, 2(3), 2012 pg. 47-64, Galați, România, Universitatea Danubius
- Acta Universitatis Danubius. Œconomica, 7(6), 2011, Galați, România, Universitatea Danubius
- EuroEconomica 2, 2010, pg. 113-122. Galați, România, Universitatea Danubius

De asemenea, rezultatele tezei au fost prezentate la diferite conferinţe internaţionale şi publicate în culegerile de lucrări ale acestora:

- 15th International Conference on European Integration - Realities and Perspectives, Vol 15, No1 (2020) Galați, România, Universitatea Danubius
- ITSEC-2012 International Conference on Information Technologies and Security 2012, Chișinău, Republica Moldova
- 3rd International Conference on Computer technology and Development. Chengdu, 2011 China
- Conferința Internațională "Educație și creativitate pentru o societate bazată pe cunoaștere" ediția a III-a 2009 și ediția a IV-a 2010, Universitatea "Titu Maiorescu", București, România
- The Tenth International Conference on Informatics in Economy IE 2010, București, România
- International Conference on Computer and Software Modeling, ICCSM 2010 Manila , Philippine: Institute of Electrical and Electronics Engineers

Publicaţii la tema tezei. La tema tezei au fost publicate 11 lucrări ştiinţifice: 4 articole în reviste internaţionale cotate B+ și șapte articole la conferințe internaționale dintre care două ISI Proceedings. Dintre articolele publicate, trei sunt ca singur autor:, două în reviste internaţionale cotate B+ și unul la conferință internațională.

Volumul şi structura tezei. Conţinutul de bază al tezei este expus pe 120 de pagini şi inserează 21 de figuri şi 17 tabele. Teza este compusă din introducere, patru capitole, concluzii generale și bibliografie (64 titluri).

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

CONŢINUTUL TEZEI

În **Introducere** sunt prezentate: actualitatea şi importanţa temei de cercetare, scopul şi obiectivele lucrării, este argumentată noutatea ştiinţifică şi valoarea practică a lucrării.

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-La Padula [4, 5], Biba [6], Clark-Wilson [24], RBAC [10, 11, 22, 23], ABAC [12, 14. 20, 21] și a limbajelor pentru definirea politicilor de confidențialitate: EPAL [3] și XACML [18].

În **capitolul al doilea** se face o introducere în teoria încrederii (trust theory), prin analiza și sinteza unor cercetări care au stat la baza tezei. Au fost prezentate cercetări anterioare, pentru integrarea conceptului de *încredere* în cadrul unei organizații. Ținând cont de migrația forței de muncă, de nevoia de cunoaștere a noilor membri ai unei organizații, în ultimele decenii s-au efectuat cercetări privind reputația și recomandările primite de diverși subiecți.

În lucrările analizate, s-au prezentat și s-au cuantificat diversele niveluri de încredere și modelele 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, s-au prezentat și modele distribuite de recomandare și protocoale, ce pot fi implementate în cadrul organizațiilor virtuale și nu numai. 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 [15], Abdul-Rahman și Hailes [1, 2], Mui Lik [16, 17], Pitsilis George și Marshal Lindsay [19], Indrajit Ray și Sudip Chakraborty [13], Zuo și Panda [25].

În continuare, au fost 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.

A fost abordat 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.

În final, este prezentat modul de clasificare a încrederii în cadrul unei organizații și relațiile dintre încrederea atribuită subiecților și obiectele din organizație.

Conținutul acestui capitol reprezintă fundamentul modelării, proiectării și implementării sistemelor informatice, iar politicile de securitate se aplică organizațiilor, prin asigurarea confidențialității și integrității datelor și informațiilor, din documentele care circulă în organizație. De asemenea, prin exemple, sunt prezentate câteva modalități de aplicare a politicilor de confidențialitate și integritate, prin intermediul încrederii.

În **capitolul al treilea** sunt definite elementele ce contribuie la crearea politicilor bazate pe încredere și este prezentat un model de construire a acestor politici. De asemenea, sunt definite elementele pe baza cărora s-au creat politici de control al accesului și acțiunilor bazate pe încredere. Astfel, s-a arătat că în general, încrederea acordată unei persoane [15, 7, 8] 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 și 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 organizații au nevoie de corectitudine, viteză de lucru, în dauna experienței și bunăvoinței, alte organizații 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.

Pentru a crea politici de control al accesului pentru utilizatorii unui spațiu virtual, au fost definite următoarele:

- cerințele de evaluare;
- obiectele;
- grupul de obiecte;
- ciclul de viață sau durata de existență a unui obiect;
- utilizatorii;
- grupurile 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, 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.

Grupul de obiecte reprezintă o colecție de obiecte ce aparțin unui domeniu de
activitate.

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

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.

Ciclul de viață (durata de existență) a unui obiect reprezintă totalitatea etapelor parcurse de acel obiect, de la creare până la arhivare sau ștergere.

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.

Grupul de utilizatori este format din persoane care interacționează cu un set de obiecte din cadrul unui domeniu de activitate.

Domeniul de activitate reprezintă o parte a activităților executate în cadrul organizației, grupate după caracteristici comune, cum ar fi: cunoștințe tehnice, economice sau științifice comune, interes comun, sferă de aplicare, etc.

Am numit **valoare de încredere** acordată unui proces, o valoare atribuită ce corespunde unui proces ce poate fi aplicat unui obiect .

Cerințele necesare stabilirii valorii de încredere sunt un set arbitrar de condiții pe care un utilizator trebuie să le îndeplinească pentru a i se acorda o anumită valoare de încredere în vederea executării unor acțiuni .

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 acțiuni specifice corespunzătoare **valorii de încredere** .

Pentru a crea un mecanism logic, de control al accesului la obiecte, au fost formalizate principiile expuse anterior. Pentru aceasta, s-au făcut următoarele considerații asupra elementelor cu care s-a lucrat.

- **ierarhia parțial ordonată** s-a definit ca fiind un set finit de valori *(H1 ≤ H2)* ordonate în mod crescător [3, 7, 8, 9].

- **subierarhia parțial ordonată** *(I1 ≤ I2)*, s-a definit 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 :

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

Interacțiunea dintre obiect și utilizator e denumită acțiune și se notează cu a_i. Totalitatea acțiunilor creează mulțimea de acțiuni *A*.

S-a definit 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** s-a definit ca fiind 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"). Valorile pot fi exprimate numeric sau prin literali. 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 .

Un proces *p*, al lui *x*, aplicat 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 acțiunii.

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

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 $r = 0$ [7, 8, 9].

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

În prezenta lucrare, s-a considerat **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. Astfel, rezultă următoarele:

1. Fiecare obiect are atașat un grup de valori de încredere, valori ce corespund unei ierarhii de procese, ce reprezintă ordinea în care vor fi aplicate obiectului.
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.
5. Dreptul de executare al unui proces asupra unui obiect este determinat de valoarea de încredere acordată .

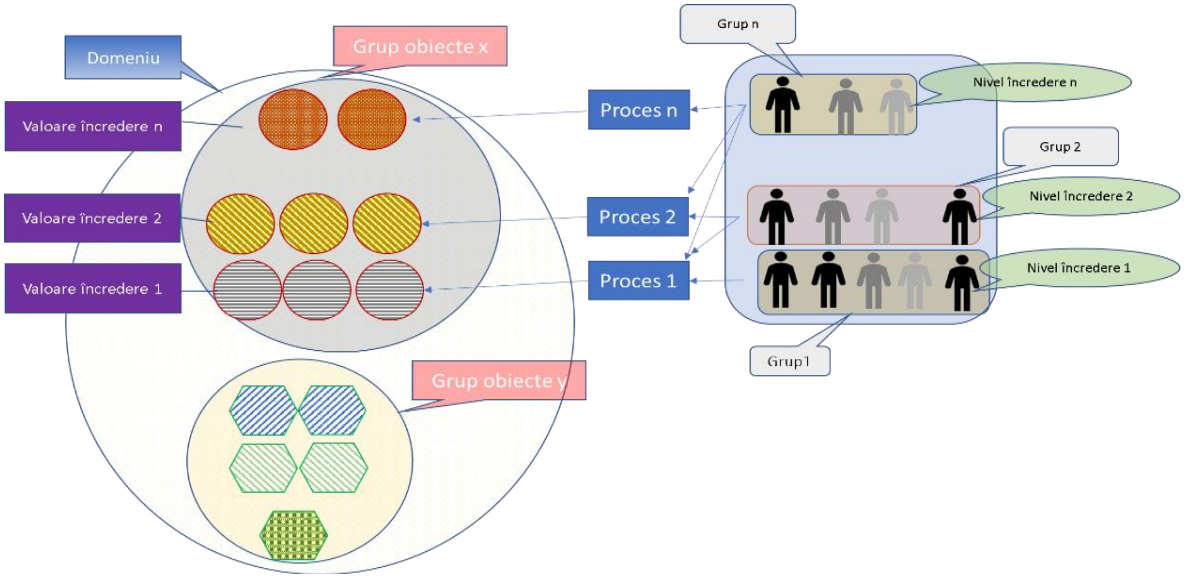

Figura 1 Relațiile de încredre între utilizatori și obiecte.

În figura 1 sunt exemplificate relațiile de încredere dintre utilizatori și obiecte.

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

S-a definit ca fiind **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 vede că se poate crea un prim set tupluri, care reprezintă legătura dintre grupuri de obiecte, grupuri de utilizatori și acțiuni, bazate pe nivelul de încredere, (GO, D, G, R, C) pe care îl numim 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.

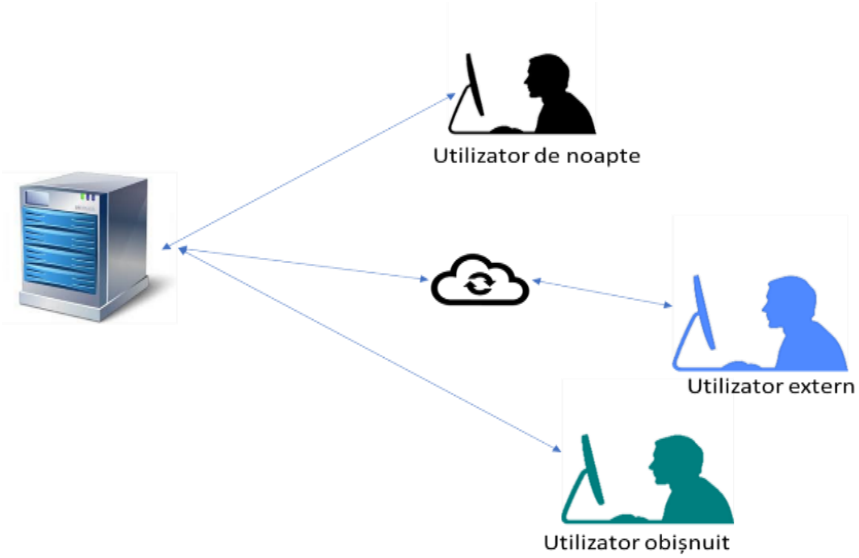

Figura 2 Diverse exemple de contex de lucru.

În figura 2 sunt prezentate posibile contexte de lucru ale utilizatorilor.

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 utlizator 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.

Pentru simplificarea acțiunilor permise unui utilizator asupra unui obiect într-un context dat, se poate 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 fi situații când, drepturi ale unor grupuri de utilizatori, s-ar putea să nu implice și existența unor acțiuni corespunzătoare, atribuite unor utilizatori din grup. Atunci se vor institui niște restricții

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.

Pentru a desemna o restricție privind o acțiune, se notează cu -P_k o restricție detaliată și cu -R_u ansamblul de politici restrictive. Astfel, se obține 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 [2, 4].

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) .
- **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) .

În continuare, au fost modelate fluxurile de lucru, ca suport pentru implementarea politicilor bazate pe încredere. Crearea fluxului de lucru este foarte importantă, în vederea simplificării implementării politicilor bazate pe încredere.

Unui obiect, pe parcursul duratei de viață, îi sunt aplicate o serie de procese ordonate, conform planificării create anterior. Fiecărui proces (p), îi corespund o serie de acțiuni (A), evenimente (E) și 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 permite posibilitatea de a realiza o ierarhie de procese, ce conțin, la rândul lor, ierarhii de acțiuni (A_k), ierarhii de evenimente (E_k) și secvențe de flux (F_k).

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

Proiectarea și implementarea politicilor bazate pe încredere presupune determinarea acțiunilor, evenimentelor și 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.

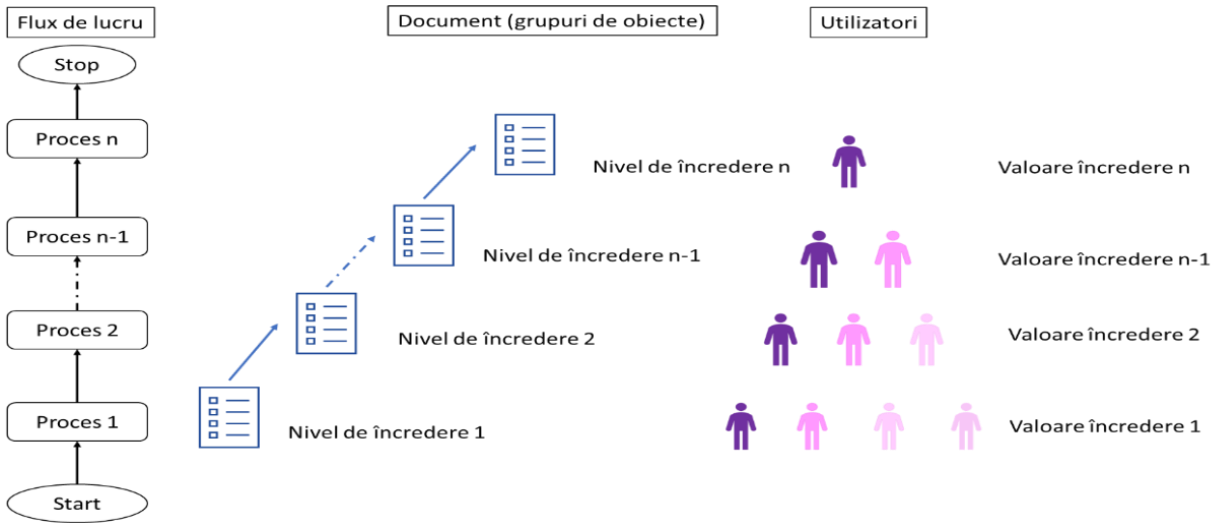

Figura 3 Relația dintre fluxuri de lucru (procese) , obiecte, utilizatori.

Pe parcursul duratei de viață a unui document, ce poate fi considerat ca un grup de obiecte (date și informații ce au o anumită semantică), nivelul de încredere se modifică, în general, prin creșterea acestuia, pe parcursul fluxului de prelucrare. Figura 3 prezintă o ierarhie de procese aplicată unui document.

Au fost formalizate condițiile generale pentru a aplica o politică de încredere :

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 $\forall p_k(O_i)$,

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

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

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

(3.2.1.1)

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;

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

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

O_i = Obiectul i;

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

p_k = procesul k suferit de O_i prin intermediul unui utilizator U_k;

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

R_u = nivelul de încredere pentru utilizatorul 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, s-a concluzionat că orice obiect are atașată o ierarhie de procese 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 care 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 punctul de vedere al complexității, politicile se clasifică în:

- politici de control simple,
- politici de control derivate.

S-a definit 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. 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.

S-a definit o **politică de control derivată** bazată pe încredere, o politică de tip general, căreia i s-au aplicat restricții și delegări. 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 aplicarea politicii de încredere, s-au desprins următoarele concluzii:

- unui obiect îi este aplicat un set de procese, ordonate pe baza unei ierarhii parțiale.
- fiecare proces este executat la un moment t_i unde $t_{i-1} < t_i < t_{i=1} \Rightarrow$ ierarhia acțiunilor este dependentă de timp.
- obiectul, după ce i s-a aplicat 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 asupra unui obiect, în mod ordonat, ierarhic, pe parcursul unui flux de lucru, aplicând procesele predeterminate.

S-a definit **fluxul de lucru,** ca fiind totalitatea proceselor aplicate unui 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.

S-a definit **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.

A fost descrisă o politică de control al accesului și acțiunilor bazată pe încredere prin următoarea matrice de tupluri:

$$M(O_i) = \left\| \begin{matrix} t1, U_x1, p_{k1}, re_v1, de_v1, & C_x1 \\ \dots & \dots \\ tn, U_xn, p_{kn}, re_vn, de_vn, & C_xn \end{matrix} \right\| \Leftrightarrow R_g(G_m) \geq V(D_i)$$

- t_i = momentul în care are loc procesul, $i \in [1,n)$.
- C_{xi} = contextul de lucru de la momentul ti.
- O_i = obiectul asupra căruia se aplică procesul.
- D_i = domeniul căruia îi aparține obiectul.
- U_{xi} = utilizatorul ce are acces la domeniu, ca aparține unei ierarhii parțiale și este membru al grupului G_m
- p_{ki} = procesul ce se aplică obiectului, la momentul t_i și aparține unei ierarhii parțiale de procese ce se aplică obiectului
- re_{vi} = restricția ce se aplică utilizatorului U_{xi} la momentul t_i pentru procesul P_{ki}
- de_{vi} = delegarea ce se aplică utilizatorului U_{xi} la momentul t_i pentru procesul P_{ki}

În continuare, s-a prezentat modelarea politicilor Biba de asigurare a integrității, prin intermediul politicilor de control al accesului și acțiunilor bazate pe încredere.

Pentru aceasta au fost prezentate:

- modelarea proprietății de integritate simplă,
- proprietatea de integritate stea ,
- invocarea proprietății.

Cerințele de integritate Biba, permit a fi respectate pentru orice utilizator ce accesează un obiect la un moment dat *t*, următoarele:

- *Starea de integritate simplă*:

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

Din condiția de mai sus, pentru $\forall U_x \Rightarrow \exists A_k(O_i)$ dacă $R_u(U_k) = R_a(A_k)$

Unde:

$U_x = s$;

$Gm = S$

$R_u(U_k) = i(s)$
$R_a(A_k) = i(o)$
$O_i = o$
$GO = O$
A_k = *acțiune*

- *Proprietatea de integritate stea * :*

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

Condiția de mai sus impune ca $\exists A_k(O_i)$ pentru U_x *dacă* $R_u(U_k)=R_a(A_k)$

- *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.

În continuare a fost prezentată importanța fluxului de lucru, prin modelarea unei aplicații de acordare a unui concediu de odihnă, în vederea creării politicilor de control al accesului sub forma:

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

cât și a politicilor de restricții și delegări sub forma:

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

În **capitolul al patrulea** a fost abordat controlul accesului și al acțiunilor utilizatorilor unui sistem informațional, bazat pe încredere. Au fost prezentate trei exemple de modelare a accesului și acțiunilor utilizatorilor asupra documentelor, 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. Exemplele au prezentat modelarea controlului accesului și acțiunilor prin intermediul interfeței grafice a utilizatorilor (GUI).

În primul exemplu s-a prezentat o aplicație mai complexă pentru o clinică medicală (figura 4), ce ține cont de legislația privind protecția datelor (GDPR) și drepturile de accesare ale utilizatorilor, a datelor și informațiilor despre pacienți.

Pe parcursul lucrării, s-au prezentat fluxul de lucru general și fluxurile de lucru pe fiecare punct de lucru din cadrul clinicii, cu cerințele lor de securitate.

S-au determinat documentele ce grupează obiectele (datele și informațiile din document) cu care interacționează utilizatorii sistemului informatic.

De asemenea, s-au stabilit utilizatorii, contextul de lucru și procesele pe care trebuie să le aplice.

Utilizand limbajul *xml*, s-a arătat cum pot fi implementate politicile de control al accesului și acțiunilor utilizatorilor, utilizând obiectele de interfață (GUI) ale limbajelor de programare și cum se realizează controlul lor, prin intermediul proprietăților, cum ar fi:

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

care ne permit crearea conținutului dinamic.

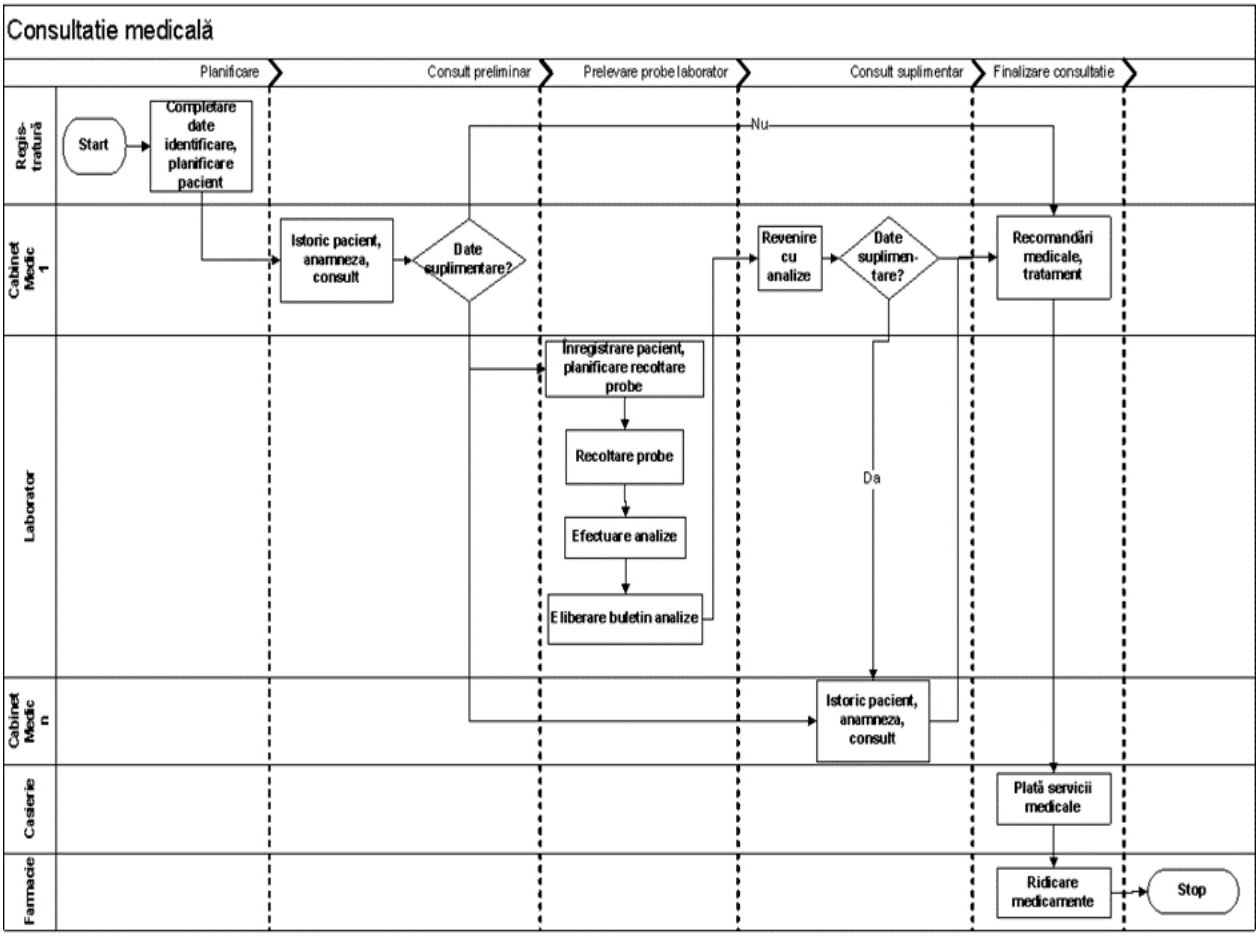

Figura 4 Fluxul de lucru din cadrul clinicii.

Pentru modelul de mai sus, în cadrul unei proceduri „LOAD” a interfeței grafice, s-a arătat cum grupurile de elemente pot fi 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.

Modelul de aplicație creat, este serverless, bazat pe mesaje.

În cel de-al doilea exemplu (figura 5), s-a prezentat o aplicație de acordare a unui concediu medical, pentru o rețea de întreprindere.

De asemenea, s-a făcut analiza sistemului informatic și s-a determinat fluxul informațional.

La fel ca în exemplul anterior, s-au stabilit documentele ce grupează obiectele cu care interacționează un utilizator.

S-au făcut optimizările de flux necesare, s-au stabilit utilizatorii, lista de delegări cât și restricțiile pe cazuri. S-au stabilit politicile de control al accesului asupra obiectelor.

S-a prezentat apoi modelul de utilizare a limbajului *xml*, în vederea implementării controlului accesului și acțiunilor, prin intermediul interfețelor grafice ale aplicației.

În cel de-al treilea exemplu, s-a demonstrat cum se creează un raport dinamic, cu ajutorul *xml*, într-o organizație ce are o politică internă de clasificare

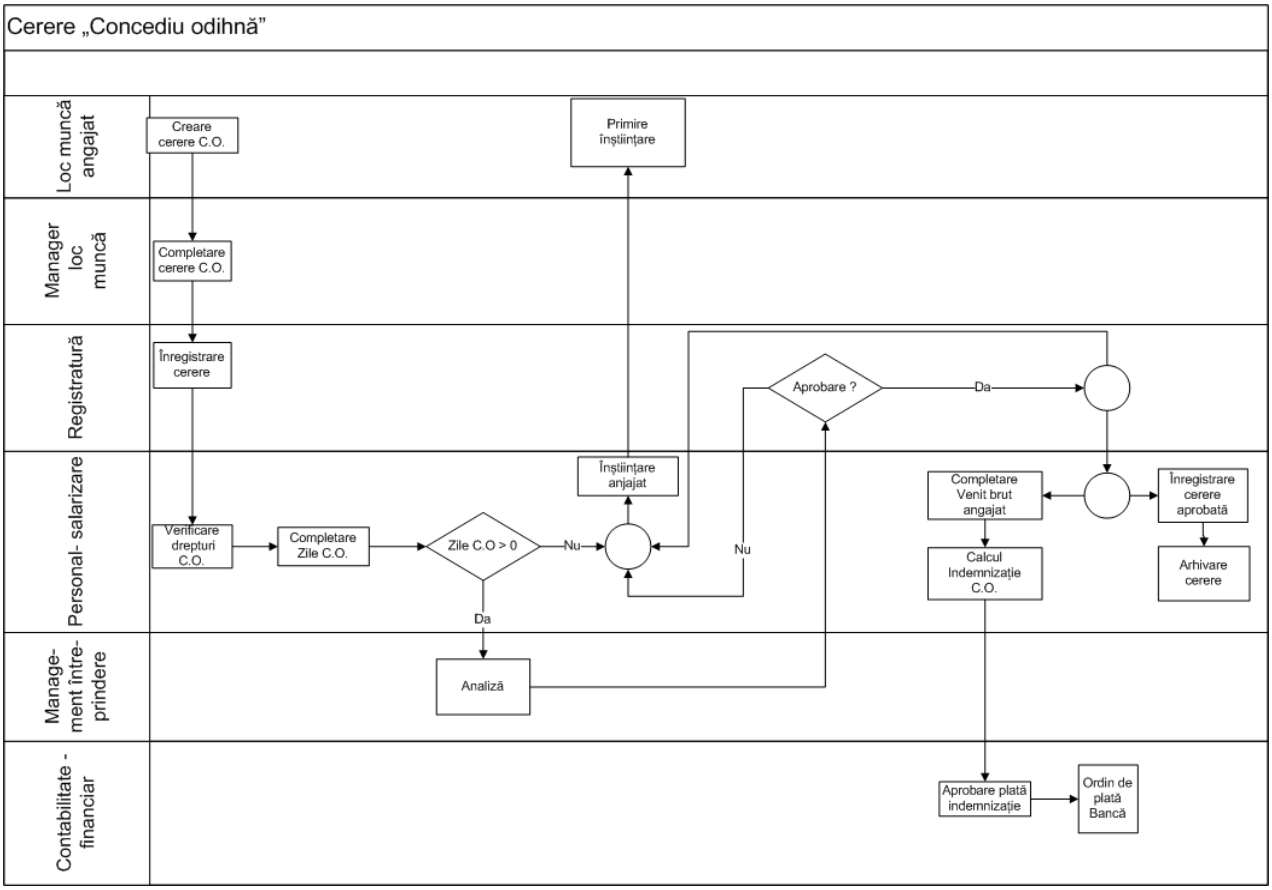

Figura 5 Fluxul informational pentru o aplicație de concediu de odihnă.

a 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, am stabilit următoarele:

- documentul este format din secțiuni (părți) de document, ce pot fi: text, imagini, tabele, grafice, slide-uri, etc., ce sunt creația unui colectiv format din membri ai domeniilor organizației, ce au acces la informațiile transpuse;
- secțiunile au fost considerate, 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 aplicarea politicii de încredere, pentru oricare obiect O_i, care are un nivel de încredere minim necesar pentru a fi accesat de un utilizator, există un utilizator ce are o valoare de încredere ce îi permite aplicarea de procese.

A fost 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:noNamespa ceSchemaLocation="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>
```

Dacă *D* este mulțimea domeniilor de activitate ale organizației
$D=\{D_1, D_2, \ldots D_i, \ldots D_n\}$
GM= mulțimea de grupuri de utilizatori ce aparțin organizației,
$GM=\{Gm_1, Gm_2 \ldots Gm_i .. Gm_n\}$
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*, acesta trebuie să aibă trust_value >= trust_level al obiectului O_i. În plus, la procesele permise a fi aplicate obiectului *Oi*, acestea trebuie să fie diferite de ∅. Prin urmare, dacă $Rp(O_i) <= Ru(U_{ki})$, atunci obiectul O_i poate fi accesat de către utilizatorul U_k.

În acest capitol, prin exemplele create, s-a demonstrat flexibilitatea politicilor de control al accesului și acțiunilor bazate pe încredere, în implementarea și utilizarea lor. Se concluzionează că spectrul de implementare și utilizare este mult mai larg și ceea ce s-a prezentat în capitolul curent este o bază de pornire în experimentarea aplicării acestor politici.

CONCLUZII GENERALE ŞI 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 al 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, pag. 60-71).
2. Pentru prima dată în cercetarea informatică, s-au stabilit elementele necesare formalizării condițiilor de aplicare a politicilor de încredere, pentru accesarea și interacționarea cu obiectele sistemului informatic. (Cap. 3, pag. 73-78)
3. A fost propus un concept complex al modelului de control al accesului și acțiunilor în sistemele informaționale, mai extins decât cele existente anterior (inclusiv, propuse de către autor în lucrări anterioare), 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 unui model teoretic complex, ce stă la baza aplicării politicilor de control al accesului și acțiunilor utilizatorilor, cât și prin atingerea obiectivelor declarate la începutul lucrării

Valoarea aplicativă a modelului TBAAC a fost demonstrată prin aplicarea în modelarea politicilor Biba, MAC și DAC (Cap. 3, 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, 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 demonstrat aplicabilitatea 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, pag. 84-93) în vederea demonstrării construirii politicilor. Obiectul construit utilizând formatul *xml*, conține 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, pag. 106-110) a demonstrat aplicabilitatea politicilor într-o organizație în care politicile se aplică la nivel de utilizatori.
- În al treilea exemplu (Cap. 4, pag. 110-112), este prezentată implementarea politicilor în cadrul unei organizații care utilizează informații 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, atât de condițiile 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 lucrării a fost realizată prin parteneriat cu Institutul de Cercetare - Dezvoltare pentru Ecologie Acvatică, Pescuit și Acavacultură în cadrul proiectelor dezvoltate în comun într-o perioadă de zece ani.

Pentru realizarea acestor politici a fost proiectată și realizată aplicația „Trust analist”, aplicație ce permite crearea politicilor bazate pe încredere și implementează conceptele și modelele dezvoltate în urma cercetărilor efectuate.

Aplicația este utilizată în activitatea de implementare a politicilor de securitate în cadrul organizației susnumite și a altor entități.

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 tuplurilor de date, cât și a proiecțiilor tabelelor;
- Cercetări privind utilizarea framework-urilor de implementare a politicilor pentru diverse tipuri de aplicații (standalone, client-server și web);
- Cercetări privind crearea unui limbaj pentru impunere a politicilor de control bazate pe încredere;
- Crearea de modele de implementare în cadrul diverselor aplicații de tip ERP;
- Cercetarea posibilității aplicării TBAAC în domeniul senzorilor și IoT.

BIBLIOGRAFIE

1. 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 .
2. 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
3. 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/
4. 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
5. 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
6. 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
7. **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
8. **DANILESCU Marcel**, BESLIU Victor, Creating Trust Based Access Policies to Control User Actions on Documents, In: *Information Technologies and Security2012", Intern.Conf. (2012; Chisinau). Proceedings of ITSEC-2012 International Conference on Information Technologies and Security 2012*, 15-16 Oct. 2012, Ed.Veacheslav Perju–Chisinau NCAA, 2013–388 p., 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

9. **DANILESCU Marcel**, DANILESCU Laura, Control Access To Information By Applying Trust Policies. *Conferința Internațională „Educație și creativitate pentru o societate bazată pe cunoaștere" ediția a IV-a*, 2010,pp. 49-54, Universitatea „Titu Maiorescu", Bucuresti, România. ISBN 978-606-8002-47-7.
10. 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 .
11. FERRAIOLO David F., KUHN Richard, CHANDRAMOULI Ramaswamy, *Role-Based Access* Control (ed. Second edition).: ARTECH HOUSE, INC., 2007, Norwood, Massachusets, U.S.A. ISBN-13: 978-1596931138 , ISBN-10: 1596931132 .
12. 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 .
13. INDRAJIT Ray, SUDIP Chakraborty, A Vector Model of Trust for Developing Trustworthy Systems. In: *Lecture Notes in Computer Science Ser., Computer Security –ESORICS 2004*. Springer Verlag, pp. 260-275. Berlin, Heidelberg, Germany. ISBN 978-3-540-30108-0 https://doi.org/10.1007/978-3-540-30108-0_16 .
14. 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 .
15. 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 .
16. 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

17. 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 .
18. *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.
19. 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 .
20. 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 .
21. 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 .
22. 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 .
23. 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
24. 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.

25. 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

LISTA LUCRĂRILOR PUBLICATE LA TEMA TEZEI

1. **DANILESCU Marcel**, Modeling Access Control And User Actions Using Trust - Based Access Control Policies. In: *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
2. **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), Universitatea Danubius, Galați, România, 2012, pp. 47-64. Print ISSN: 2284 – 9459, On-line ISSN: 2392 – 8778. Disponibil : http://journals.univ-danubius.ro/index.php/ jam/ article/view/1592
3. **DANILESCU Marcel**. Comparative study of access control methods in enterprise information systems, based on RBAC, ABAC, and TBAC policies,. In: *Danubius International Conferences, 15th International Conference on European Integration - Realities and Perspectives*, Vol 15, No1 (2020) Universitatea Danubius, Galați, România, Print ISSN: 2067 - 9211, Online ISSN: 2069 – 9344. disponibil : http://proceedings.univ-danubius.ro/index.php/eirp.
4. **DANILESCU Marcel**, BESLIU Victor. Creating Trust Based Access Policies to Control User Actions on Documents. In: *Information Technologies and Security2012, Intern.Conf. (2012; Chisinau). Proceedings of ITSEC-2012 International Conference on Information Technologies and Security*, 2012, 15-16 Oct. 2012, Chisinau / Ed.Veacheslav Perju–Chisinau: NCAA, 2013. –388p. ISBN 978-9975-4172-3-5 Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/Information%20Technologies%20and%20Security%202012.pdf
5. **DANILESCU Marcel**, DANILESCU Laura. Control Access To Information By Applying Trust Policies. In: *Conferința Internațională "Educație și creativitate pentru o societate bazată pe cunoaștere"* ediția a IV-a 2010, pp. 49-54. Universitatea "Titu Maiorescu", Bucuresti. ISBN 978-606-8002-47-7.
6. ADOMNICAI Cosmin, **DANILESCU Marcel** (2011). 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. Disponibil: http://dx.doi.org/10.1115/1.859919.paper183
7. DANILESCU Laura, **DANILESCU Marcel**. Xml Based Techniques For Data Privacy In: E-Business. In: *Conferința Internațională "Educație și creativitate pentru o societate bazată pe cunoaștere"* ediția a III-a, 2009 pp. 15-18. Universitatea "Titu Maiorescu", Bucuresti .ISBN 078-606-8002-36-1.
8. DANILESCU Laura, **DANILESCU Marcel.** Algorithm for defining trust hierarchies to control access to information. In: *International Conference on*

Informatics in Economy. Bucuresti: The Tenth International Conference on Informatics in Economy IE 2010. 2011,A.S.E. (Ed.) Bucuresti ISSN 2247-1470.
9. DANILESCU Laura, **DANILESCU Marcel**. Organization's data access control policies based on trust. In: *EuroEconomica*, 2, 2010, pp. 113-122. Universitatea Danubius, Galați, România. Print ISSN: 1582-8859, Online ISSN: 2065-3883.
10. DANILESCU Laura, **DANILESCU Marcel**. Control Access To Information By Applying Policies Based On Trust Hierarchies. In: *International Conference on Computer and Software Modeling, ICCSM 2010* (pp. 285-290). Institute of Electrical and Electronics Engineers, Inc., Manila , Philippine.
11. Danilescu Laura, **Danilescu Marcel**. "*Trust hierarchy trees applied in team management and data access*" – revista "Acta Universitatis Danubius. Œconomica", CNCSIS B+, Vol 7, No 6 (2011), pag. 141-144, ISSN 2065-0175, http://journals.univ-danubius.ro/index.php/oeconomica/ article/view/1383.

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: -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 12 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.).

DANILESCU MARCEL

CONTROLUL ACCESULUI ȘI ACȚIUNILOR ÎN SISTEMELE INFORMAȚIONALE

232.02 – TEHNOLOGII , PRODUSE ŞI SISTEME INFORMAŢIONALE

Rezumatul tezei de doctor în informatică

Aprobat spre tipar:	Formatul hârtiei 60x84 1/16
Hârtie ofset. Tipar RISO	Tiraj ex 40
Coli de tipar:	Comanda nr.

Editura "Zigotto", Galați