

CONTRIBUȚII PRIVIND ARHITECTURA ȘI FIABILITATEA SISTEMELOR INFORMATICE DISTRIBUITE ORIENTATE PE SERVICII WEB

- REZUMAT -

Coordonator științific, Prof.univ.dr.ing. NICOLAE ROBU

Doctorand, ing. CEZAR TOADER

Această teză abordează, mai întâi, problematica organizării resurselor unei aplicații Web conform principiilor REST și continuă cu problema integrării în sistemele noi, moderne, a resurselor existente anterior. Se propune și se analizează o variantă de implementare a unei arhitecturi orientate pe resurse, denumită aici *Arhitectură RESTful Multilayer*. Aceasta respectă principiile esențiale: principiul adresabilității resurselor și principiul interfeței uniforme pentru accesul la resurse.

Organizarea aplicațiilor distribuite a fost analizată în strânsă legătură cu conceptul de resurse algoritmice. Aici au fost incluse și serviciile Web. Astfel s-a făcut trecerea spre conceptul de sistem distribuit orientat pe servicii Web.

S-au analizat, mai întâi, probleme de fiabilitate ale sistemelor distribuite. S-a efectuat o analiză a conceptelor actuale legate de disponibilitate, siguranță, toleranță la defecte și fiabilitate, ca un concept integrator. Studiul problemelor de fiabilitate a sistemelor distribuite, fiind orientat către arhitecturi cu servicii Web, a continuat cu analiza replicării optimiste. S-au prezentat caracteristicile și elementele replicării optimiste, comparativ cu replicarea pesimistă.

S-a propus și s-a analizat un model de sistem distribuit în care un proces situat pe o anumită gazdă are rolul de a coordona procese situate pe alte gazde. Astfel s-a conturat modelul de sistem distribuit cu procese de management și de execuție separate.

Acest model a fost dezvoltat, în continuare, prin specificarea rolurilor proceselor implicate și anume: rolul de executant al unor procese de replicare și, respectiv, rolul de manager al acestor procese de replicare. Astfel s-a modelat un sistem tolerant la defecte ce folosește o tehnică de replicare în care intervine un proces de management al replicării și mai multe procese executant.

Într-un capitol al tezei se definesc modurile de funcționare ale acestui sistem de replicare cu separarea managementului de execuție, precum și protocoalele de funcționare ale componentelor sistemului.

După tratarea problemelor specifice modelării sistemului de replicare cu separarea managementului de execuție, într-un alt capitol al tezei, s-a arătat un mod de planificare și realizare a unui sistem informatic orientat pe servicii Web, care, pentru a fi tolerant la defecte, folosește tehnica de replicare manageriată, descrisă anterior.

Aici se prezintă și abordările experimentale, sistemele hardware și software folosite și, mai mult, se evidențiază corelația dintre întârzierea sistemului în formularea unui răspuns la cererile clienților și procesele de replicare. În această teză se definește un indicator de performanță a funcționării sistemelor tolerante la defecte, bazate pe tehnica de replicare cu procese de execuție la distanță. Acest parametru a fost denumit *întârziere relativă*. Lucrarea prezintă valorile experimentale specifice sistemelor folosite și, pentru generalizare, propune folosirea valorilor inițiale ale acestui parametru ca valori de referință pentru a monitoriza, în

timp, eventuala degradare a performanțelor sistemelor care folosesc replicarea proceselor pe gazde aflate la distanță.

În cadrul conceptului de *fiabilitate* a sistemelor, care este un concept mai larg, apare inclus și conceptul de *securitate*. În această teză s-a abordat problema securizării comunicațiilor între procesul manager al replicării și procesele de execuție. Comunicațiile dintre aceste procese legitime în cadrul sistemului cu replicare trebuie securizate pentru a împiedica eventualele atacuri din partea unor procese externe care vizează accesul la date sensibile (date de autentificare) sau date specifice fazelor de lucru ale sistemului cu replicare manageriată.

În această teză s-a prezentat o tehnică de securizare a mesajelor transmise între procesele manager și executant folosind un *lacăt informatic*. S-au formulat protocoalele pentru crearea mesajelor securizate, respectiv, pentru decriptarea mesajelor securizate. Pașii necesari sunt descriși pe larg, cu detalii, apoi sunt prezentați pe scurt în schemele protocoalelor menționate. În final, s-a efectuat o analiză care arată că atacurile venite din partea unor procese nelegitime nu vor avea succes și nu vor conduce la dezvăluirea datelor sensibile din mesajele transmise pe rețea între procesele legitime.

TEMATICA ABORDATĂ

- Arhitecturi ale aplicațiilor Web, probleme de adresabilitate a resurselor Web și operații asupra acestora;
- Servicii Web, arhitecturi orientate pe servicii, resurse algoritmice și arhitecturi stratificate, integrarea aplicațiilor Web non-RESTful în arhitecturi RESTful;
- Disponibilitatea, siguranța și fiabilitatea serviciilor Web;
- Tehnici tradiționale de replicare comparativ cu replicarea optimistă;
- Modelarea sistemelor distribuite cu management centralizat și execuție separată pe mai multe procese, comunicația între procese, ordinea cauzală a mesajelor, problema acordului distribuit;
- Modelarea sistemelor cu replicare coordonată centralizat, planificarea fazelor de execuție și stabilirea protocoalelor;
- Arhitectura sistemelor fiabile, tehnici de replicare, procese de execuție și control.
- Securizarea comunicațiilor între componentele sistemelor distribuite, în special ale sistemelor cu replicare.

OBIECTIVELE PROPUSE

- Studiul tendințelor actuale în organizarea resurselor aplicațiilor Web, clarificarea arhitecturilor orientate pe resurse;
- Elaborarea unei arhitecturi RESTful stratificate capabilă să integreze și aplicații Web non-RESTful;
- Studiul problemelor legate de disponibilitatea, siguranța și fiabilitatea sistemelor distribuite;
- Elaborarea unui model de sistem distribuit cu procese de execuție coordonate separat de un subsistem de management;
- Elaborarea unei arhitecturi de sistem distribuit cu replicare manageriată și precizarea modurilor de operare, a fazelor de execuție și a protocoalelor.
- Elaborarea unui protocol de securizare a mesajelor în sistemele cu replicare.

ORGANIZAREA TEZEI

În Capitolul 1, sunt prezentate cadrul general în care se încadrează teza, tematicile abordate, obiectivele principale și modul de organizare a tezei.

În Capitolul 2, intitulat *Arhitecturi, resurse și servicii în Web-ul programabil*, se analizează probleme actuale specifice dezvoltării aplicațiilor Web și tehnologiei identificatorilor de resurse, se analizează operațiile efectuate asupra resurselor în cadrul aplicațiilor Web și se definesc trei tipuri de arhitecturi întâlnite în aplicațiile Web actuale. Scopul clarificării acestor arhitecturi este de a aduce Web-ului programabil un plus de claritate prin creșterea gradului de uniformitate în modul de apelare a resurselor, prin obținerea unor avantaje maxime pe baza capacităților protocolului HTTP, și, în final, prin crearea posibilității de integrare a aplicațiilor mai vechi existente în cadrul companiilor în noile arhitecturi ale aplicațiilor Web.

În acest capitol se prezintă, în continuare, conceptul de serviciu Web, caracteristicile acestor servicii, impactul lor asupra dezvoltării aplicațiilor distribuite și o clasificare a stărilor și serviciilor. Se continuă cu prezentarea unei modalități de formare a resurselor de tip serviciu Web, care, astfel, devin componente *stateful* în aplicații distribuite. Acest tip de resurse vor fi folosite în cadrul tezei, într-un capitol ulterior. Capitolul continuă cu prezentarea conceptului de resurse algoritmice și a arhitecturilor RESTful stratificate. În acest capitol autorul propune o arhitectură orientată pe resurse numită *Arhitectură RESTful Multilayer*.

Autorul organizează resursele aplicațiilor Web pe trei niveluri, clarifică rolul entităților software de pe fiecare nivel și arată modul cum interacționează entitățile software aflate pe niveluri diferite. Această arhitectură stratificată respectă două principii: *principiul adresabilității resurselor* și, *principiul interfeței uniforme pentru accesul la resurse*.

Capitolul 3 este intitulat *Fiabilitatea serviciilor Web*. În acest capitol se trece de la problemele privind organizarea aplicațiilor distribuite, care au fost tratate în capitolul anterior, la probleme de fiabilitate a sistemelor distribuite. Se prezintă, mai întâi, o analiză a conceptelor actuale legate de disponibilitate, siguranță, toleranță la defecte și fiabilitate, ca un concept integrator. Se continuă cu analiza replicării optimiste, tehnologie folosită în această teză într-un capitol ulterior. Se prezintă caracteristicile și elementele replicării *optimiste*, comparativ cu cele ale replicării *pesimiste*.

În Capitolul 4, intitulat *Modelarea unui sistem distribuit cu management centralizat*, se prezintă pe etape dezvoltarea unui model de sistem distribuit în care elementele abstracte primordiale sunt *procesul* și *conexiunea (legătura) între procese*. Se tratează problema comunicației între procese în cadrul sistemului distribuit, conceptul de *mesaj între procese*, și se prezintă *problema acordului distribuit*. În continuare se trece la abstractizarea elementelor din cadrul unui proces, respectiv, niveluri, componente și evenimente. Se prezintă importanța conceptului de *timp logic* în cadrul unui sistem distribuit și, pe baza acestuia, se definește conceptul abstract de *ordine cauzală a mesajelor*. Toate aceste concepte sunt necesare pentru definirea, în cadrul acestui capitol, a unui model de sistem distribuit în care unele procese au *rol de management* al operațiilor desfășurate de alte procese care au doar *rol de execuție*. După prezentarea proceselor componente ale sistemului, în acest capitol se abstractizează *schimbul de mesaje între procesele* sistemului distribuit. În acest capitol se propune și se analizează un model abstract de sistem distribuit în care sunt modelate procese executant controlate de un proces manager, care rulează la distanță, pe o altă gazdă, față de procesele executant. Modelul prezentat în acest capitol este la baza dezvoltării, într-un capitol ulterior, a unui sistem distribuit tolerant la defecte, care folosește replicarea operațiilor.

Capitolul 5 este intitulat *Model de replicare cu separarea managementului de execuție*. Pornind de la modelul abstract de sistem distribuit prezentat anterior se propune în

acest capitol un model de replicare a operațiilor și datelor pe structura unui sistem distribuit în care există mai multe procese de execuție. După prezentarea unei liste de obiective pentru sistemul tolerant la defecte, se propune *separarea operațiilor de management de operațiile efective de execuție și stocare de date* în cadrul sistemului distribuit.

În acest capitol se propune utilizarea unui proces central, special destinat pentru operații de coordonare și control a altor procese destinate operațiilor de execuție. Într-o primă etapă, acest sistem distribuit este analizat din punctul de vedere al stărilor și, respectiv, al modurilor de operare. În a doua etapă, se prezintă fazele de execuție și protocoalele pentru componentele esențiale ale sistemului cu replicare, respectiv, componenta de management și componentele de execuție. Aceste faze de execuție sunt analizate diferențiat pe modurile de execuție ale sistemului, luat ca întreg, moduri prezentate în acest capitol.

În Capitolul 6, intitulat *Arhitectura unui sistem fiabil cu replicare manageriată*, se prezintă un mod de implementare a modelului de replicare prezentat în capitolul anterior și se arată în detaliu ipotezele de lucru, modul de operare al acestui sistem cu replicare coordonată de un proces separat, protocoalele de funcționare, modul de resincronizare a replicilor sistemului și alte detalii de implementare.

Arhitectura propusă este compusă, în esență, din componente cu următoarele roluri: înregistrarea cererilor clienților, execuția operațiilor cerute de client, coordonare și control, înregistrarea stării serviciilor Web cu rol de execuție și altele. Pe baza informațiilor primite de la subsistemele de înregistrare, managerul serviciilor Web este capabil să decidă în ce stare este fiecare serviciu Web și când trebuie făcută resincronizarea sistemului. Pentru aplicația client acest sistem apare ca un software unitar, capabil să rezolve intern defectele de sistem apărute și să dea un răspuns corespunzător la cererea făcută, chiar dacă uneori apare o întârziere datorată procesului de resincronizare a unor servicii replică.

Sunt prezentate în acest capitol aspecte ale implementării și detalii despre rezultatele experimentale. S-a propus *un nou parametru al sistemelor distribuite tolerante la defecte* care să exprime influența fazei de replicare a serviciilor Web asupra timpului de răspuns, numit *Relative Delay*. Această mărime relativă permite evaluarea modificărilor performanței sistemului față de valori de referință. Abordările experimentale au arătat o influență a fazei de replicare asupra performanței globale a sistemului, dar valorile întârzierilor sistemului pot fi menținute la valori acceptabile. Monitorizarea evoluției în timp a valorilor acestui parametru permite aprecierea scăderilor de performanță a sistemului față de o stare inițială și deschide noi posibilități de control și optimizare.

În acest capitol este abordată și problema securității sistemului distribuit, ca o componentă importantă a conceptului de *fiabilitate*. Pentru arhitectura de sistem cu replicare manageriată se studiază problema difuzării mesajelor de către componenta de management către serviciile pe care le coordonează. În scopul protejării sistemului de atacuri informatice se analizează problema securizării mesajelor difuzate în cadrul acestui sistem cu replicare. Se propune în acest capitol un protocol pentru crearea de mesaje securizate folosind o tehnică de protejare a informației sensibile cu un *lacăt informatic*, iar algoritmul folosit este bazat pe polinoame de interpolare Lagrange.

Capitolul 7 prezintă *Concluzii și contribuții personale* în cadrul acestei teze.

CONCLUZII ȘI CONTRIBUȚII

În această teză s-au formulat următoarele concluzii și contribuții:

- S-a efectuat o analiză a evoluției modului de adresare a resurselor într-o aplicație Web și o clasificare a arhitecturilor pe baza stilului de adresare a resurselor cu prezentarea elementelor specifice și a avantajelor [Toader2008a], [Toader2009a].

- S-a propus un mod de proiectare a ierarhiei resurselor algoritmice ale unei aplicații Web pentru a implementa principiile arhitecturale REST, ceea ce conduce, mai departe, la o structurare mai bună a resurselor, la creșterea gradului de uniformitate a modului de adresare a resurselor și la utilizarea cu avantaje maxime a capabilităților protocolului HTTP [Toader2008b].
- S-a propus o modalitate de adaptare a ierarhiei virtuale a resurselor, utilizată la nivelul superior, cel al aplicației complexe bazată pe o multitudine de resurse, cu ierarhia reală a resurselor de pe nivelurile inferioare, fie resurse nou create, fie cele moștenite din sistemele existente anterior, pe principiul dezvoltării sistemelor complexe cu păstrarea compatibilității cu sistemele existente [Toader2009b].
- S-a propus și s-a definit *Arhitectura RESTful Multilayer*, orientată pe resurse, în care fiecare strat are rolul său specific în organizarea ierarhică și adresabilitatea resurselor utilizate într-o aplicație Web, toate acestea având la bază principiul interfețelor uniforme pentru accesul la resurse [Toader2009].
- S-a prezentat un mod de implementare a clienților RESTful care să utilizeze capabilitățile protocolului HTTP și să beneficieze de organizarea resurselor unei aplicații complexe cu arhitectură *RESTful Multilayer* [Toader2009a].
- S-a abordat problema fiabilității serviciilor Web în contextul utilizării lor pentru dezvoltarea unor aplicații bazate pe principiile arhitecturilor orientate pe servicii (*SOA – Service Oriented Architectures*).
- S-au analizat și evidențiat conceptele de *disponibilitate*, *siguranță* și *fiabilitate* și s-au prezentat detalii despre taxonomia termenilor folosiți în domeniul fiabilității sistemelor: *serviciu corect*, *eroare*, *eșec al sistemului*, *defecte*, *toleranță la defecte*.
- S-a prezentat tehnica de *replicare* folosită cu scopul de a realiza sisteme tolerante la defecte și s-au analizat tehnicile tradiționale de replicare cu caracteristicile lor. S-a analizat conceptul de *replicare optimistă* și s-au prezentat caracteristicile sale.
- S-au definit elementele esențiale ale unui model de sistem distribuit care conține, în esență sa, procese și conexiuni între procese și, în care s-au formalizat comunicațiile între procese pe baza conceptului de *eveniment*. În acest context s-a formulat un model de organizare a unui sistem distribuit care va constitui, ulterior în această teză, baza unui sistem cu replicare.
- S-au formulat o serie de *obiective ale sistemului cu replicare*, care au influențat ulterior toată dezvoltarea acestuia, în ceea ce privește asigurarea fiabilității. În sistemul propus *toleranța la defecte* este asigurată, în esență, de replicarea datelor pe mai multe noduri de rețea. La nivelul sistemului distribuit au fost luate în considerare atât căderile nodurilor rețelei, cât și întreruperea legăturilor dintre noduri. S-au prezentat modurile de operare ale sistemului propus, precum și tranzițiile între acestea.
- În dezvoltarea sistemului tolerant la defecte, s-a propus separarea *componentelor de management* (care formează un subsistem de management) și a *componentelor cu rol de execuție* (care formează un subsistem de execuție). Avantajele sunt semnificative în cazul localizării acestora componente pe sisteme hardware separate.
- S-au analizat în detaliu rolurile componentelor de management și a celor de execuție și s-a arătat necesitatea folosirii în cadrul sistemului distribuit a unor componente complexe formate din *servicii Web stateless* și *resurse stateful*.
- S-au evidențiat *operațiile necesare în cadrul unui sistem cu replicare manageriată* pentru desfășurarea în bune condiții a replicării datelor, dar mai ales pentru

- Pentru sistemul cu replicare propus în această teză s-au prezentat în detaliu protocoalele și fazele de execuție, respectiv: *protocolul componentei de execuție* cu *fazele de execuție* corespunzătoare și *protocolul componentei de management* cu *fazele de execuție ale componentei de management*, diferențiat pe *moduri de operare ale sistemului*.
- S-a propus o *arhitectură de sistem distribuit, tolerant la defecte*. Au fost definite componentele sistemului și s-a precizat rolul fiecărei componente și interacțiunile dintre ele. Sistemul transpune în practică un model abstract de sistem definit anterior, cu replicare coordonată de o componentă de management separată.
- S-a abordat problema securității sistemului distribuit, ca o componentă importantă a conceptului de *fiabilitate*. Pentru arhitectura de sistem cu replicare manageriată s-a studiat problema difuzării mesajelor de către componenta de management către serviciile pe care le coordonează. În scopul protejării sistemului de atacuri informatice a fost analizată *problema securizării mesajelor difuzate* în cadrul unui sistem tolerant la defecte, care folosește replicarea operațiilor.
- S-a propus un *protocol pentru securizarea mesajelor* folosind o tehnică de protejare a informației sensibile cu un *lacăt informatic*, iar pentru implementarea algoritmului de protejare s-au folosit polinoamele de interpolare Lagrange.
- S-a propus un *nou parametru al sistemelor distribuite tolerante la defecte* care să exprime influența fazei de replicare a serviciilor Web asupra timpului de răspuns, numit *Relative Delay*. Această mărime relativă permite evaluarea modificărilor performanței sistemului față de valori de referință. Abordările experimentale au arătat o influență a fazei de replicare asupra performanței globale a sistemului, dar valorile întâzierilor sistemului pot fi menținute la valori acceptabile. Monitorizarea evoluției în timp a valorilor acestui parametru permite aprecierea scăderilor de performanță a sistemului față de o stare inițială și deschide noi posibilități de control și optimizare [Toader2010], [Toader2011].

BIBLIOGRAFIE (extras)

- [Toader2005] – Toader, C., *Studiu comparativ privind stadiul actual al serviciilor de rețea în sistemele de operare. Securizarea autentificării și traficului în rețea*, Raport de cercetare pentru doctorat, Universitatea “Politehnica” din Timișoara, 2005.
- [Toader2006] – Toader, C., Management of Web applications performance, In: *International Conference on Sustainable Development Strategies*, Baia Mare, Romania, 2006.
- [Toader2007] – Toader, C., Petrovan, A., Costea, C., Business Models and Secure Web Learning on Public Key Infrastructures, In: *Proceedings of International Multidisciplinary Conference*, North University of Baia Mare, Romania, 2007.
- [Toader2008a] – Toader, C., Impact of modern WEB technologies on e-learning platforms, In: *Creative Mathematics and Informatics*, nr.18, ISSN 1584-286X; 1843-441X, 2009, Web: <http://creative-mathematics.ubm.ro/>, (revistă indexată BDI, CNCSIS, B+).
- [Toader2008b] – Toader, C., Actual aspects concerning the architecture of Web-based Learning Systems, In: *Proceedings of International Conference on Sustainable Development Strategies*, North University of Baia Mare, Romania, 2008.

- [Toader2009] – Toader, C., Multilayer Resource-Oriented Architecture Supporting Restful And Non-Restful Resources, In: *Proceedings of the 20th International DAAAM Symposium*, Vol.20, pp.467-468, ISBN: 978-3-901509-70-4, Vienna University of Technology, 2009 (ISI Web of Knowledge).
- [Toader2009a] – Toader, C., *Studiu privind tehnologiile actuale de generare a paginilor Web. Creșterea gradului de interactivitate al aplicațiilor de tip Web-based Learning*, Raport de cercetare pentru doctorat, Universitatea “Politehnica” din Timișoara, 2009.
- [Toader2009b] – Toader, C., *Studiu privind posibilități de realizare a aplicațiilor distribuite pentru instruire asistată de calculator. Definierea și implementarea arhitecturii RESTful Multilayer pentru aplicații Web-based Learning*, Raport de cercetare pentru doctorat, Universitatea “Politehnica” din Timișoara, 2009.
- [Toader2009c] – Toader, C., RESTful Multilayer Architectures for Web-based Learning Systems, In: *Creative Mathematics and Informatics*, nr.18, ISSN 1584-286X; 1843-441X, 2009 (revistă indexată BDI, CNCSIS, B+) <http://creative-mathematics.ubm.ro/> .
- [Toader2010] – Toader, C., Increasing Reliability of Web Services, In: *Journal of Control Engineering and Applied Informatics*, Vol.12, No.4, pp.30-35, ISSN 1454-8658, Dec.2010 (ISI Web of Knowledge) <http://ceai.srait.ro/index.php/ceai/issue/view/192> .
- [Toader2011] – Toader, C., Reliability and Fault-Tolerance in Distributed Systems, In: *Proceedings of International Multidisciplinary Conference, IMC 2011*, 9th Edition, University of Baia Mare, Romania, and University College of Nyiregyhaza, Hungary, pp.257-262, ISBN 978-615-5097-18-8, May 2011.