

# ARHITECTURI PENTRU APLICAȚIILE MOBILE ȘI DISTRIBUITE

**Alin Zamfiroiu**

zamfiroiu@ici.ro

**Emanuil Rednic**

emanuil.rednic@gmail.com

Academia de Studii Economice, București

**Rezumat:** Aplicațiile mobile reprezintă o provocare pentru lumea dezvoltatorilor de software. Evoluția tehnologică s-a mutat dintr-o zonă a aplicațiilor desktop către o zonă a aplicațiilor distribuite și în special rulabile pe dispozitive mobile pentru o mai mare disponibilitate. În lucrarea de față sunt prezentate arhitecturi folosite pentru realizarea aplicațiilor mobile distribuite și pentru modul de conectare al acestora la internet. Sunt prezentate arhitecturi de Cloud, de rețele intranet și principiile avute în vedere în construirea unui intranet. Sunt analizate entitățile utilizate de către un sistem informatic cadastral precum și standardul CADASTRU 2014.

**Cuvinte cheie:** Aplicație Mobilă, Aplicație Distribuită, Arhitectură, Sistem Informatic, CADASTRU 2014.

**Abstract:** Mobile applications is a challenge for all software developers. Technological development has moved from desktop applications area to an area of distributed applications especially on mobile devices rulabile for a higher availability. This paper presents the architecture used for distributed mobile applications and their internet connection architecture. Cloud architectures are presented for intranets and principles considered in building an intranet. Are analyzed the entities used by a cadastral informatic system and the CADASTRE 2014 standard.

**Key words:** Mobile Application, Distributed Application, Architecture, Informatic System, CADASTRE 2014.

## 1. Arhitecturi mobile

Aplicația mobilă reprezintă un ansamblu de instrucțiuni codate, folosit de un dispozitiv mobil pentru rezolvarea unei probleme.

În [1] aplicația mobilă este definită ca una care rulează pe dispozitive ce sunt folosite oriunde se deplasează utilizatorul lor.

Datorită evoluției rapide a tehnologiei și a nevoilor oamenilor de a avea cât mai aproape toate aplicațiile necesare, dezvoltarea aplicațiilor destinate dispozitivelor mobile a luat amploare. Aplicațiile mobile reprezintă o nouă categorie de produse software spre deosebire de cele obișnuite pentru calculatoare desktop sau aplicațiile web, prin mărimea lor și necesarul realizării ca și aplicație orientată spre cetățean.

Aplicațiile mobile depind foarte mult de caracteristicile hardware ale dispozitivului, de platforma dispozitivului și a sistemului de operare implementat pe dispozitivul mobil pe care rulează aplicația mobilă. Diversitatea prezentă în cadrul dispozitivelor mobile există și în cadrul aplicațiilor mobile

Atunci când se dorește dezvoltarea unei aplicații mobile, primul pas este stabilirea tipologiei aplicației. Soluția software poate să fie una locală care rulează pe dispozitivul mobil sau una care rulează pe un server și care furnizează servicii prin intermediul browser-ului sau al unei arhitecturi client-server ce nu folosește protocoale Web.

Prin natura lor aplicațiile mobile sunt mici, portabile și au o calitate personală. Problemele precum interfața, mărimea display-ului, modul de introducere a datelor, pierderile de conexiune wireless sau securitatea trebuie avute în vedere încă din timpul dezvoltării aplicației mobile. Programatorii de aplicații desktop trebuie să aibă foarte mare grijă la programarea aplicațiilor mobile cum gestionează resursele dispozitivului și cum gestionează conexiunea wireless. Dezvoltatorii care sunt conștienți de diferențele dintre calculatoarele personale și dispozitivele mobile cu privire la resursele de memorie, interfața minimă sau puterea redusă de calcul dezvoltă aplicații mobile mult mai eficiente. În dezvoltarea unei aplicații, următoarele aspecte trebuie luate în considerare:

- înțelegerea utilizatorului este esențială deoarece presupune cunoașterea așteptărilor avute de către acesta de la aplicațiile dezvoltate și implementarea celor mai folosite module și a interfețelor ușor de folosit;
- construirea unei baze de date mobile presupune stocarea informațiilor în cadrul dispozitivelor mobile prin baze de date adaptate acestor dispozitive;
- proiectarea unei aplicații logice care să răspundă așteptărilor utilizatorilor și să nu prezinte module neconcordante cu problema rezolvată;
- testarea aplicației pe un dispozitiv real pentru verificarea comportamentului în mediul real și nu doar într-un emulator;
- verificarea calității serviciilor efectuate de către aplicația mobilă pe dispozitiv.

De asemenea programatorii trebuie să aibă grijă la gestionarea conexiunii wireless. Modelele de conexiune la internet implementate în cadrul aplicațiilor sunt:

- conectare permanentă, presupune ca fluxul de date să fie deschis, consumul de baterie fiind însă mai mare;
- conectat ocazional, presupune deschiderea fluxului la intervale de timp, doar pentru actualizarea informațiilor;
- deconectat ocazional, presupune închiderea fluxului în anumite momente când nu este necesară conexiunea la server.

În [2] este prezentată structura aplicațiilor mobile dezvoltate în cod nativ.

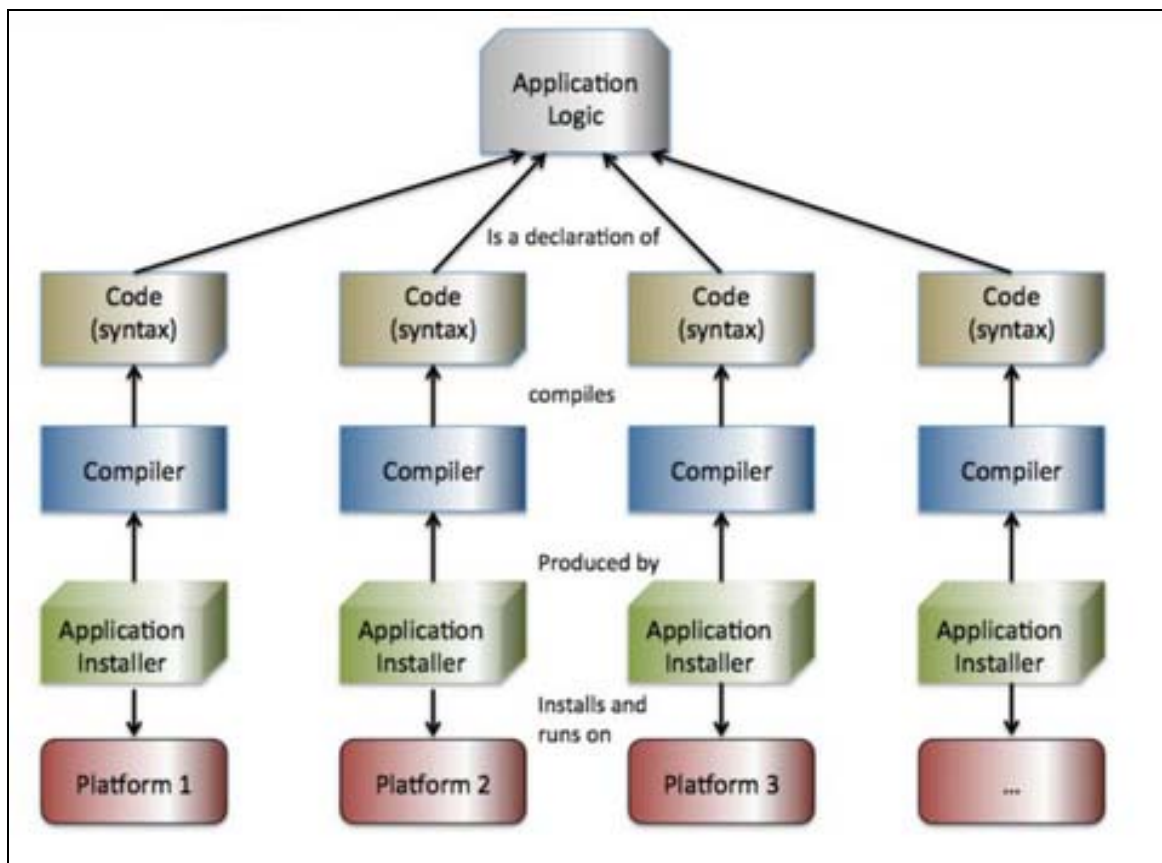
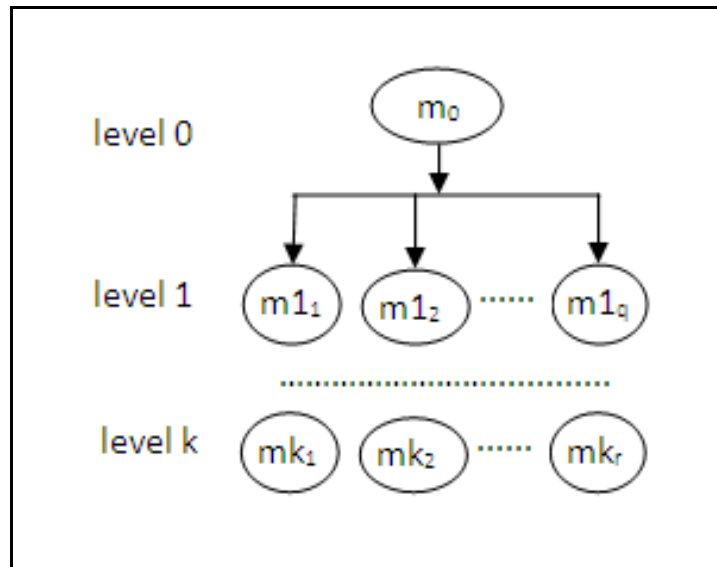


Figura 1. Structura aplicațiilor mobile în cod nativ [2].

Pentru o bună regenerabilitate a aplicațiilor mobile în [3] este propusă o arhitectură ierarhică a aplicațiilor mobile bazată pe module, figura 2.



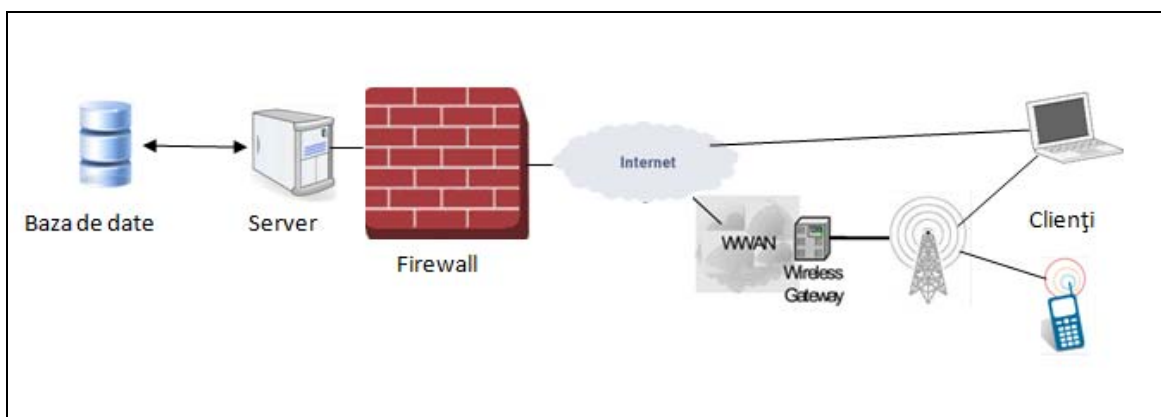
**Figura 2. Structura ierarhică a aplicațiilor**

Conform acestei arhitecturi aplicațiile sunt scalabile, noile module sunt mai ușor atașabile aplicației deja existente. Pentru utilizatorii care nu doresc toate modulele din cadrul aplicației, pot fi eliminate cu ușurință modulele nedorite de către aceștia și astfel aplicația să devină exact cea pe care și-o dorește fiecare utilizator.

În [4] aplicațiile mobile sunt împărțite în următoarele categorii:

- aplicații de informare generală;
- aplicații pentru verificarea identității virtuale;
- aplicații de comunicare;
- aplicații economice;
- jocuri.

Aplicațiile din aceste categorii presupun conectarea la internet. În [5] este prezentată arhitectura generală a rețelei de internet ce permite conectarea la rețea a aplicațiilor mobile și a aplicațiilor clasice de pe laptop-uri, figura 3.

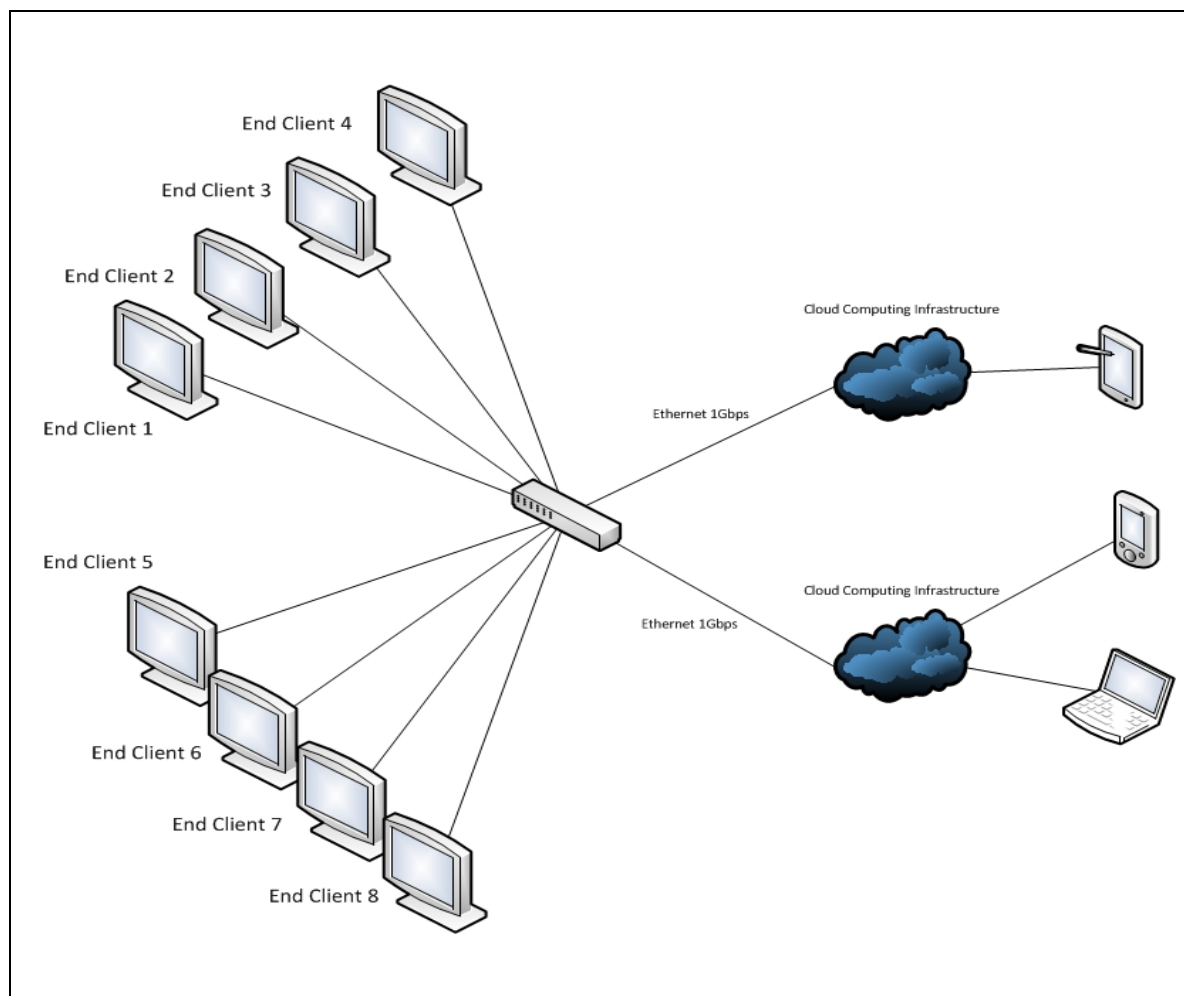


**Figura 3. Arhitectura generală a aplicațiilor mobile cu conectare la internet**

Aceste aplicații prezintă un mare avantaj din punct de vedere al procesării, deoarece procesarea nu se realizează pe dispozitivul mobil, ci pe server, puterea de procesare a serverului fiind mult mai puternică decât a unui dispozitiv mobil. Dispozitiv mobile care este folosit doar pentru prezentarea rezultatelor obținute de procesarea serverului.

## 2. Arhitecturi distribuite

Modalitatea de construire a unui intranet s-a modificat foarte mult, chiar dacă cele mai recente abordări sunt legate de arhitectura Cloud, figura 4.

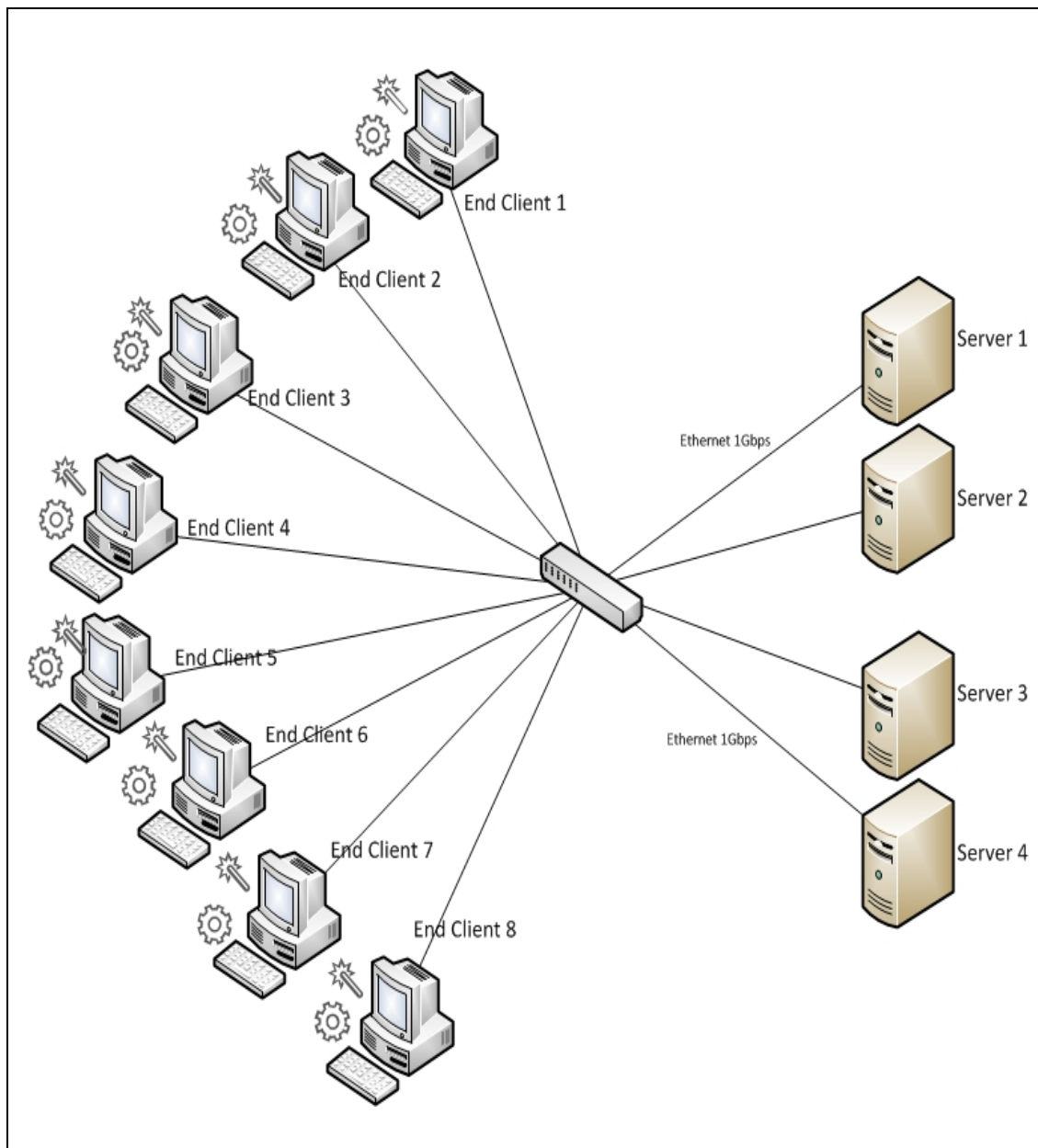


**Figura 4. Arhitectura Cloud intranet**

În construirea unui intranet, cel mai important lucru este cel legat de accesibilitatea utilizatorilor la intranet, dat și de profilul eterogen al utilizatorilor, respectiv al dispozitivelor cu care se conectează la intranet. Dacă profilul contemporan este construirea arhitecturilor mobile, astfel încât orice dispozitiv de tip smartphone, indiferent de brand, să se poată conecta la intranet, cele două abordări vin una în completarea celeilalte. De asemenea o arhitectură de tip Cloud, aduce modalități noi de securitate a datelor, a accesului, precum autorizării, prin virtualizarea stațiilor de lucru, într-un mod mult mai dinamic, față de clasicele organizări de tip intranet.

Presiunea foarte mare a fost dată în primul rând de eterogenitatea clienților finali, care se conectează la intranet. Mai mult, aplicațiile care rulează pe respectivele echipamente, au făcut să influențeze aceste noi tendințe. Dacă într-un intranet clasic avem un număr finit de aplicații atent administrate care rulează, într-o arhitectură cloud, aplicațiile sunt eterogene, aplicații care nu țin de o anumită platformă, de către un anumit furnizor, de către o anumită clasă de programe sau de un anumit tip: multimedia, gps, ce prelucrează date de tip alfanumeric, etc.

Dacă o arhitectură clasică de tip intranet, așa cum este prezentată în figura 5, era una destul de rigidă din punct de vedere al extensibilității și flexibilității hardware, software, o arhitectură cloud permite o specializare și o îmbunătățire continuă.



**Figura 5. Intranet Clasic**

Modalitatea de evaluare, sistemul de metrice propus în evaluarea cât mai elocventă a unei arhitecturi intranet, prin indicii următori:

SV – vulnerabilitatea sistemului: *mare, medie, scăzută*;

NS – numărul de servere;

NC – numărul de clienți;

NCS – numărul de aplicații software pe client;

TISC – timp total de instalare aplicații software pe client;

DC – dinamica angajaților în respectiva companie/intranet; un angajat poate lucra la una sau mai multe stații, respectiv la o stație pot lucra mai mulți angajați;

ML – mobilitatea conexiunii: *mare, medie, scăzută, zero*;

SP – portabilitatea produselor software program, măsurată la fel ca ML;

respectiv

IL – nivelul de interoperabilitate, măsurată la fel din punct de vedere al ML și SP.

Exemplu cum este evaluat o arhitectură intranet este prezentat în tabelul 1.

**Tabel 1. Evaluare Intranet**

Indice	SV	NS	NC	NCS	TISC	DC	ML	SP	IL
Valoare	Medie-Mare	4	8	10	10	+5, în ultimele 6 luni	scăzută	scăzută	scăzută

Problematika evaluării se pune prin prisma extinderii sistemului de metrice de evaluare a unui intranet, dacă respectivul intranet ar avea subcomponente de arhitecturi de tip intranet [6].

### 3. Sisteme informatice distribuite

Pentru ca un sistem informatic să utilizeze una din arhitecturile prezentate în această lucrare, trebuie ca respectivul sistem să fie unul preponderent distribuit. De exemplu, pentru un sistem informatic cadastral, încă din faza de proiectare, trebuie conceput pentru a respecta cadrul legal existent în acest domeniu precum și standardul CADASTRU 2014 [7]. Utilizarea produsului software duce la creșterea numărului înregistrărilor care au anumite atribute comune, restul fiind diferite: cheia primară multiplă. Este necesar schimbarea caracteristicilor naturale, pentru a păstra astfel toate înregistrările pentru a avea la un moment dat dinamica unei anumite parcele privită prin prisma: schimbării proprietarilor, redimensionării parcelei. Înfăptuirea acestui istoric este foarte importantă pentru soluționarea tuturor problemelor care apar privind proprietatea, precum prin îndeplinirea normei de a purta istoricul legal, normă ce aparține standardului CADASTRU 2014.

Privind prin prisma entităților care sunt utilizate de către aplicație:

- proprietarii sunt înregistrați prin intermediul primei declarații de avere, iar pentru următoarele declarații nu mai este nevoie decât să se precizeze dacă au apărut anumite modificări: vânzare, respectiv cumpărare parcele, schimbarea destinației agricole, modificarea suprafeței arabile datorită creșterii suprafeței construite: se cunoaște faptul că impozitul agricol variază în funcție de caracteristicile enumerate;
- orice modificare apărută asupra unui teren, precum reparcelarea, schimbarea proprietarului, se face printr-o nouă operație de introducere teren, în care se vor preciza modificările făcute;
- factorul multimedia de asemenea trebuie să îndeplinească cerința aceasta; un teren este parcat în  $n$  subparcele, cu  $n$  numere topografice, se vor face  $n$  schițe care sunt stocate în această tabelă multimedia.
- toate cererile pentru certificate de producător sunt înregistrate, cu toate că un proprietar face o astfel de cerere în fiecare an, diferența între înregistrările din această tabelă sunt cele de ordin calendaristic; păstrarea tuturor acestor cereri duce la creșterea, respectiv supravegherea producătorilor agricoli și eliminarea oricărei informații false din sistemul cadastral;
- entitățile care nu respectă acest lucru sunt cele care se ocupă cu mentenanța aplicației, cele de tip nonfunciare: tabela utilizatori, tabela supraveghere, care monitorizează toate operațiile întreprinse de utilizatorii acestei aplicații asupra obiectelor sale referite din baza de date, cum sunt tabele, viziuni, funcții, proceduri; operațiile DML sunt efectuate transparent de către administratorul de baze de date și trec neobservate în gestiunea funciară; aceste entități au rolul și de a preîntâmpina unele operații care periclitează buna funcționare a produsului software;
- tabelele auxiliare, cele tampon folosite în DML nu intră în discuție pentru că ele au o existență volatilă, ele fiind de asemenea utilizate de administratorul DBA[8].

După modul de descriere al arhitecturilor de tip intranet, sistemele informatice păstrează acest paralelism și din punct de vedere al arhitecturilor software folosite pentru descrierea sistemelor informatice. Astfel pentru un sistem informatic de tip cadastral, arhitecturile folosite influențează modalitatea de dezvoltare implementare a respectivului sistem informatic, pe componentele sale. Astfel, pentru componenta ce se ocupă de securitatea sistemului din punct de vedere al accesului și autorizării utilizatorilor de sistem, aceasta este la rândul ei o sub-arhitectură distribuită, ce este ușor de construit pe o arhitectură de tip cloud. De exemplu, dacă această componentă este construită, din punct de vedere software cu ajutorul suitei de produse software program Oracle, respectiv Oracle Identity and Access Management Suite Plus, acestea oferind, de asemenea, facilități avansate de virtualizare a identității, stocare și servicii de sincronizare pentru sisteme performante, asigurarea securității pentru aplicații, date și servicii “cloud-based”. Este singura soluție integrată care oferă capacități complete de tip serviciu de director. Printr-un set de funcționalități ce include autentificarea unică: single sign-on, administrarea centralizată a privilegiilor de acces, autentificare multifactor, protejarea informației în format digital, securizarea serviciilor web, transferul tokenurilor de securitate în interiorul Registrului Agricol, federalizarea, respectiv, distribuirea, identităților și a sesiunilor de utilizare, precum și administrarea centralizată a privilegiilor utilizatorilor, Oracle Identity and Access Management Suite Plus furnizează o arhitectură unică, modulară ce oferă utilizatorilor finali, în cazul de față proprietarii de terenuri, flexibilitatea de a utiliza fie o soluție completă, fie de a se concentra pe implementarea unor componente individuale, pentru integrarea cu ușurință a serviciilor de securitate de la alți furnizori externi sistemului cadastral.

Oracle Identity and Access Management Suite Plus este un pachet care include:

- Access Manager;
- Identity Federation;
- Identity Manager;
- Security Token Service;
- Oracle Single SignOn, OSSO;

Directory Services Plus, cu subcomponentele sale, respectiv Oracle Directory Server Enterprise Edition – soluție cu scalabilitate ridicată ce se adresează mediilor eterogene; Oracle Internet Directory – soluție cu scalabilitate și redundanță ridicată ce folosește baza de date Oracle pentru stocarea informației; Oracle Virtual Directory – soluție de unificare a datelor de identitate ale utilizatorilor din mai multe surse, în timp real, fără copii, sincronizare [9].

Datorită faptului că organizațiile sunt în continuă transformare din nevoia de a furniza metode de securizare avansate pe tot fluxul informațional, cu structura modulară și bazate pe standard privind managementul identității, se îndreaptă spre externalizarea serviciilor, integrarea cu sistemele externe. Oracle Identity and Access Management Suite rezolvă aceste provocări cu o soluție completă, ce include următoarele funcționalități:

- autentificare, autorizare și auditul accesului la resursele web;
- autentificare unică pentru aplicațiile web;
- acces federalizat;
- autorizare la nivel de acces în aplicație;
- propagarea sigură a identității între aplicații prin intermediul secure token services;
- administrarea centralizată a drepturilor de acces ale utilizatorilor la toate aplicațiile sistemului informatic cadastral.

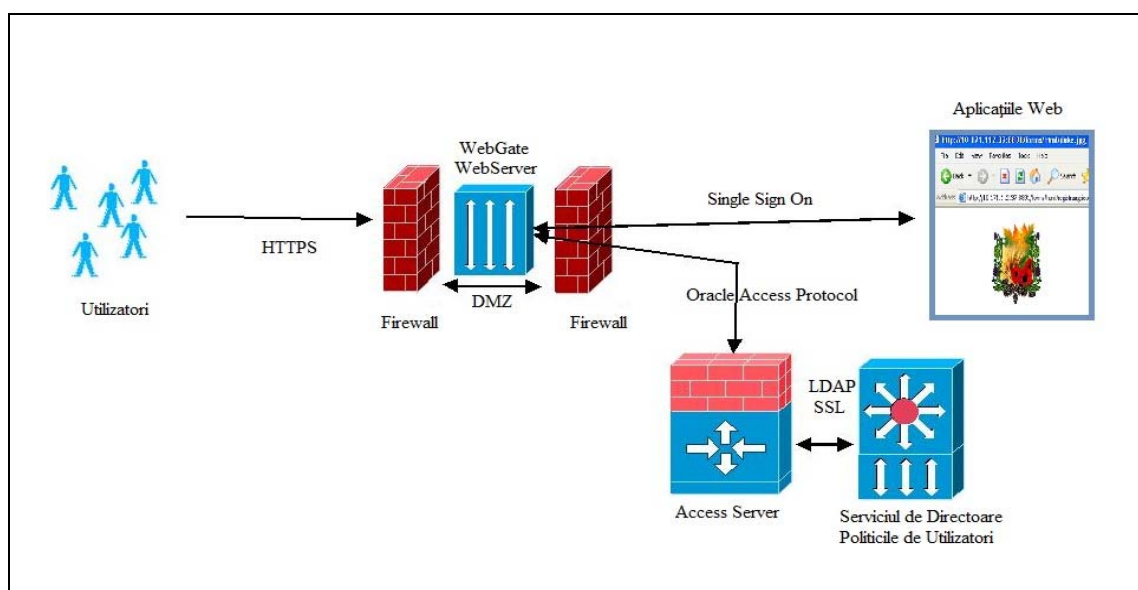
Oracle Access Manager este o soluție de tip enterprise pentru controlul centralizat al accesului la aplicații critice ce oferă într-o componentă integrată funcționalități de autentificare, autorizare, web SSO, administrarea politicilor și regulilor de acces, administrarea agenților, controlul sesiunilor utilizatorilor, monitorizarea sistemului, raportare și auditare. Stocarea profilelor de

utilizatori se face folosind un serviciu de director LDAP extern, iar integrarea cu serverul de aplicații Oracle Weblogic Server este disponibilă prin simple configurări.

Oracle Directory Server Enterprise Edition este soluția de tip director ideală pentru sistemele informatice eterogene. Oracle Directory Server Enterprise Edition oferă servicii de tip director folosind o bază de date inclusă, directory proxy, sincronizare cu Microsoft Active Directory. Oferă de asemenea integrarea cu orice serviciu de director existent, precum și consola web pentru administrare.

Oracle Directory Server Enterprise Edition oferă scalabilitate, securitate, precum și balansarea încărcării prin intermediul componentei directory proxy, suportând creșterea atât pe orizontală cât și pe verticală; scalabilitatea performanței este liniară față de creșterea capacității de procesare [10].

Datorită arhitecturii sale, Oracle Internet Directory beneficiază de opțiunile de scalabilitate, redundanță, Oracle RAC, și securitate: Advanced Security, Database Vault ce sunt folosite prin intermediul bazei de date Oracle. Pentru securizarea datelor Oracle Internet Directory folosește filtre și instrucțiuni de control la nivelul atributelor. Modul în care se realizează accesul este prezentat în figura 6.



**Figura 6. Access în Sistemul de Management al Identității**

Componenta de securitate privind managementul identității este la rândul ei o arhitectură distribuită privind accesul și autorizarea la nivelul resurselor partajate pe web. Orice proces din cadrul acestei componente se inițializează astfel atunci când un utilizator final, respectiv un proprietar de terenuri, încearcă să acceseze o resursă protejată, WebGate și Serverul de Acces efectuează următoarea secvență de pași :

- WebGate care este încărcat în zona DMZ, *Demilitarized Zone*, interceptează cererile utilizatorilor și verifică împreună cu Serverul de Acces dacă resursa accesată este protejată [11];
- dacă resursa este protejată atunci WebGate cere credențialele de acces ale utilizatorului și le transferă Serverului de Acces pentru validare;
- serverul de acces validează credențialele primite în funcție de informațiile preluate din serviciul de director;
- rezultatul acestei validări este trimis înapoi către WebGate; dacă autentificarea a avut succes atunci WebGate setează un cookie în browserul utilizatorului și verifică împreună cu Serverul de Acces dacă respectivul utilizator are permisiunile necesare de a accesa respectiva resursă;
- serverul de acces preia politicile directorului și verifică dacă utilizatorul are acces la



respectiva resursă protejată; rezultatul este trimis înapoi către component WebGate;

- dacă utilizatorul este autorizat atunci i se acordă accesul la resursa securizată.

O altă componentă folosită este WebPass, definit ca un plug-in de web server ce permite schimbul de informații între web server și Serverul de Identități folosind Oracle Identity Protocol, fostul Netpoint - COREid Identity Protocol. WebPass reprezintă nivelul de prezentare al Sistemului de Identități. Implicit WebPass își redă conținutul în format HTML astfel încât să fie accesat prin intermediul unui browser [12].

Serverul de Identități, Identity Server, administrează informațiile privind identitatea utilizatorilor, grupurilor, organizațiilor. Serverul de Identități efectuează trei funcții principale:

- citește și scrie în serviciul de directoare, folosind protocolul de comunicare LDAP, prin intermediul conexiunii de rețea;
- stochează informații despre utilizator în cadrul serviciului de directoare și menține directorul actualizat;
- procesează toate cererile referitoare la identitățile utilizatorilor, grupurilor, organizațiilor.

Indiferent de componentele sale, un sistem informatic distribuit trebuie să fie deschis din punct de vedere software și hardware, respectiv orice îmbunătățire a lui să fie făcută cu minim de efort atât din partea administratorilor, din partea utilizatorilor finali, precum orice aplicație software să ruleze, fără incidente pe respectiva platformă.

## 4. Concluzii

Prin utilizarea arhitecturilor hardware și software prezentate în această lucrare, orice sistem informatic este scalabil, orice altă componentă software se poate adăuga sistemului. De asemenea, sunt suportate căutări după chei multiple, la nivel de baze de date distribuite, dacă respectivele informații se găsesc dispersat în mediul distribuit de date, facilități ce duc la creșterea sistemului prin abordarea soluției de high availability.

Datorită faptului că un sistem informatic este scalabil, noile direcții de cercetare în domeniul securității informatice, se vor plia ușor, din punct de vedere software, în arhitectura lui. Pentru că suportul principal al sistemelor informatice e dat de volumul documentelor procesate, utilizarea și integrarea semnăturii olografe este necesară. Recunoașterea, compararea, alterarea și stocarea semnăturii olografe la nivel de baze de date multimedia, se va realiza prin prisma componentei multimedia a unui sistem informatic, acolo unde este cazul, de aceea toate operațiile ce se efectuează asupra resurselor multimedia se vor aplica și asupra semnăturilor olografe. Semnătura olografă se va integra la nivelul procesului de înregistrare în sistem, atât operatorii, personalul din domeniul cadastral, precum și proprietarii de terenuri, vor urma procesul clasic de autentificare, după care se va face o verificare la nivelul semnăturii olografe stocate la nivelul bazei de date, comparându-se validitatea utilizatorului, dacă este autorizat sau nu, pentru accesul la sistem.

Securitatea la nivel de sistem informatic, din punct de vedere multimedia, este extensibilă prin folosirea mecanismelor de AFIS, Automated Fingerprint Identification System, autentificarea și autorizarea urmând a fi realizate și prin intermediul amprentării digitale, noul modul ocupându-se de Identificare Biometrică. Modulul multimedia va putea integra informația suplimentară ce va fi stocată în baza de date, cum ar fi scanarea amprentelor digitale. Sistemul informatic va da posibilitatea prelucrării informațiilor suplimentare, care apar pe suprafața scanată, gen: cicatrice, tatuaje, semne din naștere, punându-se problema eliminării lor prin intermediul proceselor de prelucrare multimedia. Amprenta digitală, stocată, este ușor de preluat iar mai apoi de utilizat în procesul de securizare al documentelor prin intermediul watermarking-ului de tip imagine, clasică semnătură putând fi înlocuită prin intermediul amprentării digitale.

## BIBLIOGRAFIE

1. **AL-SAYYED, R.M.H.; MANASEER, S.; RABABEH, O.:** Mobile Information System, How to Build with Case Study, International Journal of Interactive Mobile Technologies, vol. 4, nr. 4. 2010, pp. 12-17.
2. <http://ctrl-d.ro/development/>
3. **IVAN, I.; BOJA, C.; ZAMFIROIU, A.:** Self- Healing for Mobile Applications, Journal Of Mobile, Embedded And Distributed Systems - JMEDS, vol. 4, nr. 2, 2012, pg. 96-106, ISSN: 2067 – 4074 (online)
4. **IVAN, I.; MILODIN, D.; ZAMFIROIU, A.:** Studiarea tipurilor de aplicații mobile și a calității acestora. Revista Română de Informatică și Automatică, vol. 21, nr. 2, 2011.
5. **DOSPINESCU, O.:** Aplicații mobile - arhitecturi generale, Analele științifice ale Universității "Alexandru Ioan Cuza" din Iași, 2004/2005: [http://anale.feaa.uaic.ro/anale/resurse/35\\_Dospinescu\\_O-Aplicatii\\_mobile-Arhitecturi\\_generale.pdf](http://anale.feaa.uaic.ro/anale/resurse/35_Dospinescu_O-Aplicatii_mobile-Arhitecturi_generale.pdf)
6. **IVAN, I.; POCATILU, P.; AMITROAIE, M.:** Metrici ale societății informaționale, Informatică Economică vol. 5, nr. 4 (20), 2001, pg. 33-40, ISSN 1453-1305
7. [http://www.esri.com/industries/cadastre/pdf/nc\\_2014.pdf](http://www.esri.com/industries/cadastre/pdf/nc_2014.pdf)
8. Oracle Identity And Management – all in one, ORACLE, U.S.A. 2007
9. Oracle Identity Manager Develop Identity Provisioning, ORACLE, U.S.A. 2006
10. Oracle Database 11g Implement Database Vault, ORACLE, U.S.A. 2010
11. Oracle Application Server 10g Administration I, ORACLE, U.S.A. 2004
12. **REDNIC, E.; VELICANU, M.:** Identity Management in University System, Informatică Economică vol. 12, nr 2, 2008, pag. 71-74, ISSN 1453-1305.