Probleme și provocări în arhitecturile de tip cloud

Issues and Challenges in Cloud Computing Architectures

Bogdan ISAC
Faculty of ETTI, University POLITEHNICA of Bucharest, Romania
bogdan_isac@yahoo.com

Abstract

Cloud computing is a concept that include a set of software services at the network level (usually using Internet) consisting of remote data storage and online applications on remote virtual servers. Cloud architecture experienced a spectacular development in recent years given the advantages it offers: increased storage capacity and computing power with minimum investment. A very important problem faced by cloud computing is the data security and privacy. This paper presents the main cloud computing service delivery models and the types of risks that may arise.

Index terms: cloud computing, infrastructure, risk, network, storage

1. Arhitectura de tip cloud

De-a lungul timpului, Internet-ul a fost reprezentat pe scheme de rețea printr-un simbol de tip nor ("*cloud*") până în 2008, când au început să apară o serie de servicii care permiteau accesarea resurselor pe cloud-ul Internet-ului. În conceptul de cloud computing au fost comasate activități ca folosirea site-urilor de socializare și alte forme de comunicare între clienți în Internet; recent, acest termen a început să facă referire la accesarea online a aplicațiilor, a datelor și a puterii de procesare a acestora. Cloud-ul reprezintă o modalitate de a crește capacitatea de stocare pentru date sau de a mări capabilitățile resurselor locale, fără însă a necesita investirea într-o nouă infrastructură IT.

În ultimii ani, arhitecturile de tip cloud au avansat de la conceptul de afacere promițătoare la unul din cele mai de succes segmente ale infrastructurii IT. Însă cu cât mai multe persoane, companii sau zone geografice sunt migrate către cloud, din ce în ce mai multă îngrijorare apare în legătură cu cât de sigur este acest mediu. Așadar, datorită siguranței datelor, această dezvoltare a conceptului de cloud a fost mult încetinită, securitatea datelor fiind principala problemă a arhitecturilor de tip cloud.

Pe de o parte, securitatea ar putea fi îmbunătățită prin centralizarea datelor și creșterea resurselor orientate pe partea de securitate. Pe de altă parte, îngrijorarea pierderii controlului asupra unor date importante încă rămâne. Dacă un provider nu își face bine treaba în a securiza propriile medii de acces, clienții pot fi în pericol. Este dificil să se măsoare calitatea abordării securității de către provideri, deoarece

majoritatea acestora nu își expun configurațiile infrastructurii către clienți.

Este posibil ca servicii care implică denumirea de cloud computing să fie deja familiare, de exemplu câteva servicii e-mail sau spații de stocare Web-based, instrumente de editare online etc. Conceptul de cloud computing este folosit și pentru Web commerce (aplicații pentru vânzări online). Majoritatea aplicațiilor Web sunt migrate către cloud și multe dintre site-urile existente integrează deja servicii de tip cloud.

Un mod de definire a conceptului de "cloud computing"ar fi: "oferirea resurselor întâlnite la un calculator, mai degrabă ca servicii decât ca produs (software, informații, date), disponibile oricărui client, calculator sau alt echipament. Conceptul oferă procesare, software, acces la date, servicii de stocare care nu necesită ca utilizatorul să aibă cunoștințe legate de amplasarea fizică și configurarea sistemelor care furnizează produsele".

2. Provocări (performanțe și limitări)

Cloud computing-ul oferă o șansă pentru un spațiu de stocare on-line de încredere, de multe ori foarte folositor celor care se conectează de pe dispozitive mobile (laptop, smartphone, tabletă), din rețele publice (Internet cafe, rețele wireless) sau celor fără spații de stocare suficiente.

Mare parte din procesarea care în mod normal se face pe browserul Web este transferată către cloud (în infrastructura cloud-ului, spre exemplu serverele). Așadar, cloud computing ajută foarte mult și echipamentele care nu sunt foarte performante din punct de vedere tehnic, cu putere mică de procesare sau capacitate modestă pentru stocarea datelor.

Pentru că procesarea și stocarea datelor au fost mutate către partea de infrastructură, cloud computing a condus indirect la creșterea pieței tabletelor, laptopurilor, echipamentelor portabile, ceea ce în continuare a determinat scăderea semnificativă a prețurilor acestora.

Utilizatorii aplicațiilor de tip cloud computing cunosc frustrarea și neplăcerea cauzate de folosirea acestor aplicații cu conexiuni la Internet de viteză mică. Problemele care apar sunt incapabilitatea de logare sau de menținere continuă a conexiunii cu poșta electronică online, documente la distanță care nu se încarcă, plăți care nu au fost efectuate. Acestea sunt rezultatul conexiunilor de viteză mică și de slabă calitate, care îl determină pe utilizator să lucreze cu aplicațiile la nivel local.

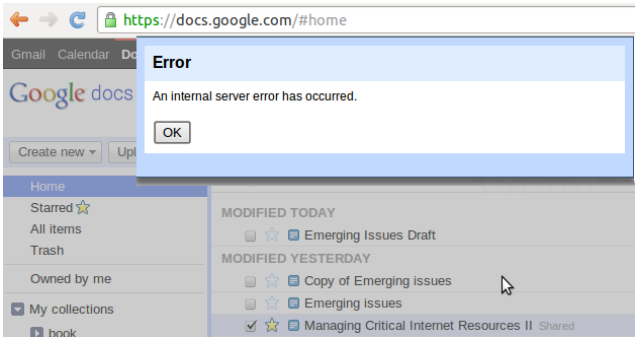

Fig. 1. Depășire de bandă alocată pentru Google Docs la conexiune ADSL de 1024kb/s

Cloud computing-ul nu necesită numai o conexiune de viteză mare, dar și o conexiune de calitate superioară, care să rămână mereu activă. În timp ce multe site-uri rulează și pe conexiuni broadband de viteză mică, aplicațiile cloud nu sunt de obicei disponibile pe astfel de conexiuni.

Pe lângă conexiune, este important și QoS (Quality of Service): indicatori care scot în evidență de câte ori și cât timp a picat conexiunea, timpul de răspuns la ping, întârzierea cu care se procesează datele (*latency*) și pierderile de date.

Așadar, datorită acestor cerințe (conexiuni rapide și de calitate), cloud computing-ul poate avea costuri ridicate în implementare.

Acceptarea conceptului de cloud computing este asociată numeroaselor provocări de care trebuie să treacă, deoarece utilizatorii încă privesc cu scepticism în special securitatea datelor stocate în cloud.

Pe baza unui studiu făcut în anul 2008 de către IDC (figura 2), cele mai mari provocări de care trebuie să treacă cloud computing-ul sunt:

a. **securitatea**: este evident că problema securității este cea mai importantă în acceptarea migrării către cloud. Fără niciun dubiu, mutarea datelor, rularea softurilor pe hard-disk-urile altor persoane pare descurajatoare pentru mulți. Foarte cunoscutele probleme de securitate cum ar fi pierderea datelor, phishing-ul, botnet-ul (controlul de la distanță al unei suite de dispozitive) sunt amenințări serioase la adresa softurilor și a datelor companiilor. De exemplu, hackerii pot utiliza cloud-ul pentru a controla la distanță sistemele de calcul ale clienților, pentru că infrastructura din cloud le permite mult mai ușor pornirea unui atac.

b. **costurile migrării**: utilizatorii din cloud trebuie să fie atenți la costurile comunicațiilor și ale integrării. Deși migrarea către cloud nu constituie o investiție majoră (deoarece nu necesită investiție în infrastructură), mutarea datelor în interiorul sau în exteriorul cloud-ului poate avea costuri destul de ridicate.

c. **încărcarea**: flexibilitatea resurselor a făcut ca analiza costurilor să fie mult mai ridicată decât în cazul unui *data center* obișnuit. Mai mult, implementarea virtualizării a condus la înlocuirea serverelor dedicate. Pentru providerii de aplicații software din cloud, costurile dezvoltării aplicațiilor pot fi destul de mari. Acestea includ reproiectarea și redezvoltarea aplicațiilor concepute inițial, costuri pentru noi caracteristici care să permită particularizări intensive, performanțe și îmbunătățiri ale securității pentru mai multe conectări ale aceluiași user și posibilitatea de a rezista complexității schimbărilor precedente.

d. **SLA** (Service Agreement Level): utilizatorii nu mai au control asupra infrastructurii și resurselor echipamentelor, deci ei nu trebuie să asigure calitatea, disponibilitatea, încrederea și performanțele acestor resurse după ce clienții au fost migrați către cloud. Cu alte cuvinte, este foarte important ca utilizatorii să fie siguri de serviciile oferite. În mod uzual acestea sunt agreate prin intermediul SLA-urilor negociate între vânzător și utilizator. Prima problemă este definirea specificațiilor astfel încât ambele părți să fie acoperite, clienții să fie satisfăcuți, iar serviciile oferite să fie conform așteptărilor. Fiecare parte a cloud-ului (infrastructura, software-ul, platforma) trebuie să aibă specificații și, implicit, SLA-uri diferite.

e. **migrarea**: pe baza unui studiu efectuat, cele 7 tipuri de aplicații care trebuie să fie migrate sunt: aplicații pentru management IT (26,2%), aplicații de colaborare (25,4%), aplicații personale (25%), aplicații business (23,4%), dezvoltare de aplicații (16,8%), capacitate de procesare (15,6%), capacitate de stocare (15,5%). Acest experiment scoate în evidență faptul că încă există temeri ale companiilor legate de mutarea datelor în cloud. În prezent, cel mai simplu este să fie mutate aplicațiile de management IT și aplicațiile personale, însă majoritatea companiilor nu doresc mutarea platformelor în cloud.

Fig. 2. Studiu de caz asupra problemelor frecvente la cloud computing. Sursa: IDC Enterprise Panel, august 2008

3. Probleme de securitate în cloud

În modelul de dezvoltare a cloud-ului, partea de rețea, platformele, stocarea și infrastructura software sunt oferite ca servicii care pot fi integrate din ce în ce mai mult în interiorul cloud-ului (figura 3).

Modelele de dezvoltare pentru cloud sunt:

a. Cloud Privat

Acesta este un termen nou pe care unii vendori au început recent să îl folosească pentru a descrie produse care folosesc rețele private. Este configurat în data center-ul intern al unei companii. Resursele scalabile și aplicațiile virtuale oferite de vendor sunt grupate împreună și disponibile pentru partajare și folosire de către utilizatori. Diferă de cloud-ul public, unde resursele și aplicațiile sunt gestionate de companie, asemenea Intranet-ului. Utilizarea acestui tip de cloud este mult mai sigură - doar utilizatorii din companie și alte persoane desemnate pot avea acces aici.

b. Cloud Public

Acest termen descrie cloud-ul tradițional, unde resursele sunt oferite prin intermediul Internet-ului sau prin intermediul unor aplicații Web, de către un provider din exterior care partajează aceste resurse. Acest model se bazează pe principiul "plată pentru utilizare", similar modelului de facturare pe bază de abonament, care este destul de flexibil. Acest tip de cloud este mai puțin sigur decât modelul anterior deoarece aplicațiile și datele accesate în cloud-ul public sunt predispuse atacurilor.

c. Cloud Hibrid

Acesta este un cloud privat legat prin unul sau mai multe servicii de cloud-uri externe, centralizate, adoptate ca într-o singură entitate și protejate de o rețea securizată. De obicei cloud-ul hibrid oferă soluții IT virtuale prin intermediul unui mix de cloud-uri publice și private. Oferă un control mai strict asupra datelor și aplicațiilor și permite diferitelor părți să acceseze informația în Internet. Are de asemenea o arhitectură care permite interfațarea cu alte sisteme.

Pe baza modelelor de dezvoltare a cloud-urilor, următoarele probleme de securitate se referă la diferitele tipuri de furnizare a serviciilor pentru cloud.

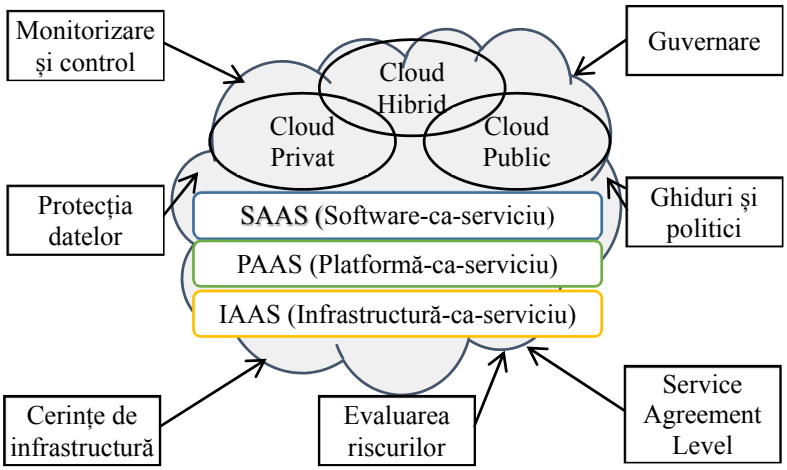

Fig. 3. Model de dezvoltare a cloud-ului

Cele trei modele principale de furnizare a serviciilor sunt: Infrastructura-ca-serviciu (Infrastructure-as-a-Service, IaaS), Platforma -ca-serviciu (Platform-as-a-Service, PaaS) și Software-ca-serviciu (Software-as-a-Service, SaaS).

a. IaaS - este un nivel al cloud-ului unde resursele dedicate sunt partajate numai clienților care beneficiază de serviciul pay-per-use. Acest serviciu minimizează nevoia de investiție în hardware, dispozitive de rețea și putere de procesare. De asemenea, are o funcționalitate mult mai flexibilă și o latură financiară care poate varia mult mai ușor decât în cazul data center-urilor sau serviciilor de colocare, deoarece resursele de calcul pot fi mult mai repede adăugate sau eliminate. IaaS și alte servicii asociate au permis companiilor start-up și altor afaceri să se concentreze pe competențele necesare dezvoltării, înlăturând grijile legate de partea de IT. Cu toate acestea, securitatea este la un nivel mai scăzut oferind doar firewall perimetric, load balancing, iar aplicațiile care se vor migra în interiorul cloud-ului vor avea nevoie de o securizare mai sporită.

b. PaaS - reprezintă un set de servicii și instrumente de dezvoltare găzduite pe serverele providerului. Este nivelul de deasupra IaaS în stivă și încorporează tot ceea ce înseamnă sistem de operare, middleware etc. Acest lucru oferă un set de medii de dezvoltare integrate unde dezvoltatorii de aplicații pot lucra fără a cunoaște ce se află în spatele acestor sisteme. PaaS oferă dezvoltatorilor un serviciu care asigură un management complet al ciclului de viață pentru dezvoltare, de la planificare, design, construcția aplicațiilor, la dezvoltare, testare și mentenanță. Totul este luat din vizorul developerilor. PaaS funcționează după același principiu ca și IaaS, dar oferă un nivel mai ridicat de funcționalitate optimă. Clienții care utilizează acest serviciu își transferă mai multe costuri de la investiții capitale la costuri operaționale, dar trebuie să fie atenți la posibilele limitări pe care le pot întâmpina din cauza acestor niveluri. Utilizarea mașinilor virtuale este asemenea unui catalizator în nivelul PaaS în cloud computing. Acestea necesită să fie protejate împotriva atacurilor malware tip malware de cloud. Așadar menținerea integrității aplicațiilor și aplicarea verificărilor suplimentare la autentificări în timpul transferului de date de-a lungul canalelor rețelei este fundamentală.

c. SaaS - este un model de distribuție a softurilor unde aplicațiile sunt găzduite de un vendor sau furnizor de servicii și sunt disponibile clienților prin intermediul rețelei, de obicei Internet-ul. Acest serviciu devine din ce în ce mai răspândit de vreme ce tehnologiile care suportă serviciile Web și arhitecturile orientate pe obiect devin tot mai

populare. SaaS este de asemenea asociată conceptului de pay-as-you-go (plată pe măsură ce avansezi). Între timp conexiunile de bandă largă s-au răspândit tot mai mult în lume. SaaS este de cele mai multe ori implementată pentru a asigura funcționalitatea softurilor către client la un cost scăzut, dar în același timp permițându-le clienților să beneficieze de licențiere, sisteme de operare interne fără necesitatea instalării, managementului, suportului și a costului inițial ridicat. Arhitectura aplicațiilor care au la bază serviciul SaaS are un design specific pentru a suporta mai multe autentificări simultane. Aplicațiile SaaS sunt accesate prin intermediul browserelor Web pe Internet, de aceea securitatea browserului este prioritară. Se folosesc astfel sisteme de securitate WS (Web Services), criptare XML (Extensible Markup Language), SSL (Secure Socket Layer).

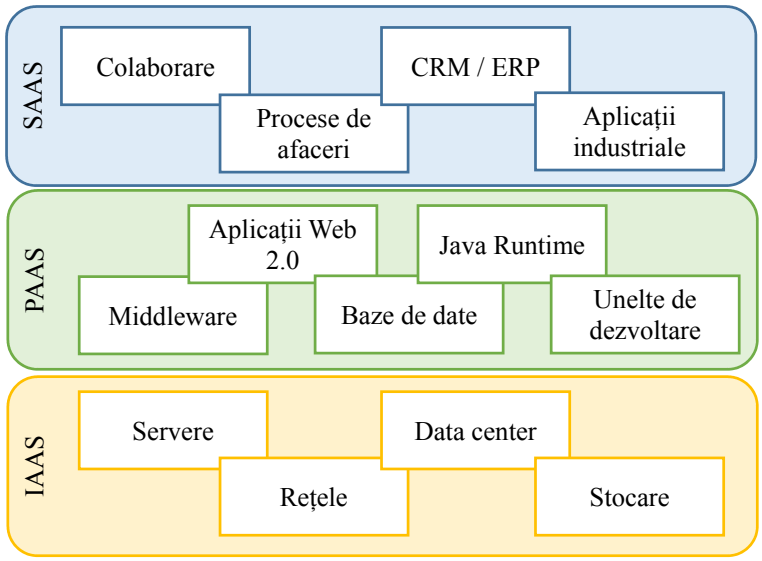

Fig. 4. Modele principale de furnizare a serviciilor: IAAS, PAAS, SAAS

Combinând așadar aceste trei tipuri de cloud cu modelele de furnizare, obținem o ilustrare holistică asemenea celei din figura de mai sus, înconjurată de echipamente de conexiune legate de teme ale securității informației.

Virtualizarea resurselor fizice, a infrastructurii, a platformelor middleware și a aplicațiilor sunt oferite ca servicii în cloud. Atât furnizorii, cât și clienții, trebuie să mențină securitatea cloud-ului pe toate interfețele.

4. Modele de riscuri

Riscul este posibilitatea ca un eveniment să apară și să afecteze îndeplinirea unui obiectiv. Tipurile de riscuri (la nivel de securitate, integritate, disponibilitate, performanță) sunt aceleași în sistemele cloud ca și în sistemele non-cloud. Profilul de risc al unei companii și riscurile se vor modifica în momentul adoptării acestui model de tehnologie.

Câteva modele de riscuri asumate sunt:

- Efectul disruptiv (impactul pe care îl are adoptarea unei noi tehnologii asupra unui business): Prin scăderea nivelului de acceptare a unor noi competitori, cloud computing ar putea să aibă impact negativ asupra unor modele de business, ducând poate și la eliminarea lor completă în viitor. De exemplu streaming-ul media pe Internet a fost o soluție care a dus la scăderea masivă a

vânzărilor de suporturi optice (CD-uri sau DVD-uri). Competitorii existenți care acceptă ideea de cloud vor trebui să vină cu idei noi și inovații pentru piețele lor de desfacere cât mai rapid.

- Apartenența aceluiași ecosistem de risc ca și CSP-ul (Cloud Services Provider) / vendorul și ceilalți clienți: Când o companie adoptă această soluție tehnologică, se creează noi dependențe cu CSP-ul în materie de probleme legale, riscuri, escaladarea incidentelor, soluționarea acestora și alte câteva arii de interes. Acțiunile CSP-ului și ale celorlalți clienți pot afecta compania.

- Lipsa transparenței: Este foarte puțin probabil ca un CSP să divulge informații despre procesele, operațiunile, controlul și metodologiile folosite. De exemplu, clienții dintr-un cloud nu au cunoștințe despre unde se află mediile de stocare, algoritmii folosiți pentru alocarea resurselor de procesare, felul în care sunt securizate componentele arhitecturii cloud-ului etc.

- Probleme de performanță și siguranță: Defecțiunile sistemelor sunt evenimente riscante care pot apărea în orice mediu, dar reprezintă o mare provocare dacă apar în cadrul unui cloud. Deși acordurile pentru *service level* pot fi structurate să îndeplinească diverse condiții, soluțiile vendorului nu sunt întotdeauna în situația de a îndeplini aceste acorduri dacă apar probleme neașteptate.

- Probleme de securitate și conformitate: În funcție de procesele suportate de cloud computing, problemele de securitate și retenție pot fi ridicate respectând anumite legi și reglementări de conformitate cum ar fi Sarbanes-Oxley Act of 2002 (SOX), Health Insurance Portability and Accountability Act of 1996 (HIPAA) și alte legi similare. În cloud, datele sunt stocate pe echipamente hard în exteriorul companiilor și fără a avea controlul direct al acestora. În funcție de tehnologia folosită (SaaS, PaaS, IaaS), clienții cloud-ului pot fi puși în situația de a nu reuși să obțină log-uri ale incidentelor de conectivitate (acestea fiind în posesia vendorului).

- Ținte ale atacurilor cibernetice: Consolidarea mai multor companii care să activeze într-o infrastructură susținută de un vendor reprezintă o țintă de mai mare interes pentru atacuri. În consecință, riscurile unei astfel de soluții tehnologice sunt mai mari decât în cadrul unei companii cu infrastructură proprie.

- Riscul scurgerilor de informații: Un mediu cloud cu mai mulți clienți în care utilizatorii sau aplicațiile partajează resurse prezintă un risc ridicat al scurgerilor de informații (risc care nu există în cadrul serverelor dedicate, la care resursele sunt folosite de un singur client).

- Schimbări în organizare: Dacă soluția cloud computing este adoptată până la un anumit punct, o companie nu mai are nevoie de foarte mult personal în cadrul departamentului IT, ceea ce duce la o restructurare a acestui departament.

5. Concluzii

S-a menționat de-a lungul timpului că tehnologia cloud are un potențial ridicat de a aduce schimbări masive în cadrul organizațiilor, asemenea Internet-ului în secolul 20. În următorii ani tehnologia cloud își va pune amprenta asupra liniei istorice a evoluției domeniului rețelelor de calculatoare, Internet și în general al tehnologiei informației.

Adoptarea și acceptarea soluției cloud este în concordanță cu popularitatea și acceptarea altor trenduri din trecut (rețelele de socializare sau virtualizarea), la care oamenii și oportunitățile trec neobservate, dar sunt îndreptățite să faciliteze comunicațiile și stocarea informațiilor. În ziua de azi, cu atâtea soluții cloud disponibile, succesorii generațiilor trecute de calculatoare au la dispoziție o opțiune mult mai ieftină, prin care nu trebuie să cunoască informații tehnice despre hardware sau despre locul unde se află aceste resurse de calcul.

Câteva aspecte ale tehnologiei cloud pot să

ridice provocări majore la adresa managementului riscului la nivelul unei companii. Uşurinţa cu care este implementată această tehnologie poate fi incredibilă în momentul în care se face o analiză a riscurilor la care este supusă o companie din cadrul unui cloud. Doar o gândire naivă ar putea ocoli aceste riscuri: activităţi infracţionale, erori umane, accidente neprevăzute - care pot apărea în orice companie.

Aplicarea soluţiilor cloud fără a avea grija şi controlul necesare, din cauza nerăbdării, sunt posibile cauze ale unor probleme ulterioare. Utilizarea propice, cu atenţie, precauţie şi control permanent, poate aduce o multitudine de beneficii. Prin conştientizarea acestor riscuri şi a altor probleme apărute la cloud computing, directorii companiilor îşi pot atinge obiectivele în cadrul acestui mediu dinamic care evoluează pe zi ce trece şi care probabil va deveni cel mai important model de procesare al viitorului.

Bibliografie

[1]. F. Gens, "New IDC IT Cloud Services Survey: Top Benefits and Challenges," IDC eXchange, 2009.

[2]. J. B. Gartner: "Seven Cloud-Computing Security Risks," *Infoworld*, 2008, [Online]. Available: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853

[3]. ENISA, "Cloud Computing: Benefits, Risks and Recommendations for Information Security," 2009, [Online]. Available: http:/www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[4]. M. P. Wilson *et al.*, "Joint Physical Layer coding and network coding for bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5641-5654, 2010.

[5]. M. Klems *et al.*, "What's Inside the Cloud? An Architectural Map of the Cloud Landscape," *IEEE Xplore*, vol. 12, pp. 23-31, Jun. 2009, [Online]. Available: http://www.di.ufpe.br/~redis/intranet/bibliography/middleware/lenk-what-2009.pdf

[6]. C. Weinhardt *et al.*, "Business Models in the Service World," *IT Professional*, vol. 11, pp. 28-33, 2009, [Online]. Available: http://www.im.uni-karlsruhe.de/Upload/Publications/2f5d87da-1af5-4d44-b422-9b7e5802b5a5.pdf

[7]. Cloud Computing Use Case Discussion Group (2012, Sep. 20), [Online]. Available: http://opencloudmanifesto.org/Cloud_Computing_Use_Cases_Whitepaper3_0.pdf

[8]. S. Ramgovind *et al.*, "The Management of Security in Cloud Computing," in *Proc. 2010 IEEE Int. Conf. Cloud Computing*, 2010, [Online]. Available: http://uir.unisa.ac.za/bitstream/handle/10500/3883/ramgovind.pdf?sequence=1

[9]. Cloud Security Alliance (2013, Feb. 08), [Online]. Available: http://www.cloudsecurityalliance.org