Universitatea “Alexandru Ioan Cuza”
Facultatea de Informatică

Conf. Dr. Lenuța Alboaie
adria@info.uaic.ro

Cuprins

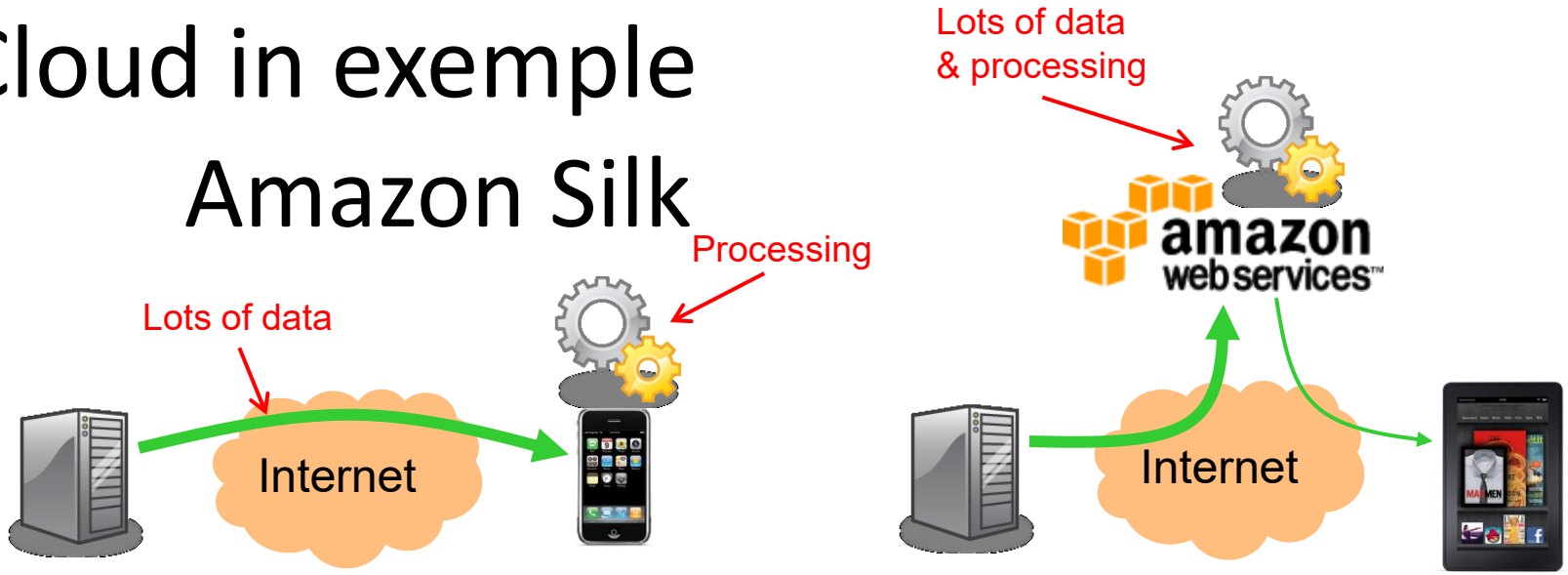
- Cloud in exemple
- Aspecte de securitate in cloud-uri publice
- Cloud-uri private
- Cloud – viziune asupra viitorului

Cloud in exemple

- Motivul principal al utilizarii: costuri scazute datorate elasticitatii
  - *Commodity machines* – usor de adaugat, inlocuit, extins
  - Resurse la cerere – se plateste cat si cand ai nevoie
- Tipuri de servicii:
- ***Software as a Service (SaaS)*: *cloud-hosted apps***
  - e.g. Hotmail, GMail, Google Docs, Office Web, …
- ***Platform as a Service (PaaS)***: nivel de programare si servicii in cloud
  - e.g. Hadoop, MS Azure….?…
- ***Infrastructure as a Service (IaaS)***: masini, retele, disk-uri virtuale
  - E.g. Amazon EC2, …

Cloud in exemple

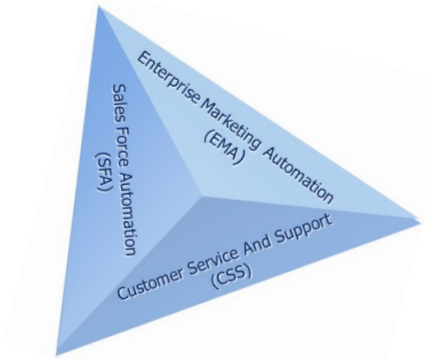
Amazon Silk



- Ideea: Utilizarea Cloud pentru a face browserele mai rapide
  - Randarea paginilor este impartita intre dispozitivul utilizator si cloud
  - Platforma de Cloud executa 'heavy lifting' (randare, executia scriptului, ...)
  - Dispozitivul arata rezultatele , deci nu are nevoie de latime de banda mare sau de putere de procesare

Cloud in exemple

- ***Software as a Service (SaaS)***
- ***E.g.*** **Salesforce.com** (similar: NetSuite; Quicken's Web apps; TurboTax Web; etc.)
  - Prima platforma SaaS de succes, in 1999 ce promova termenul de cloud
  - "Customer Relationship Management"
    - Instrumente pentru oamenii de vanzari pentru a gasi clienti
    - Ofera o imagine asupra statutului clientului



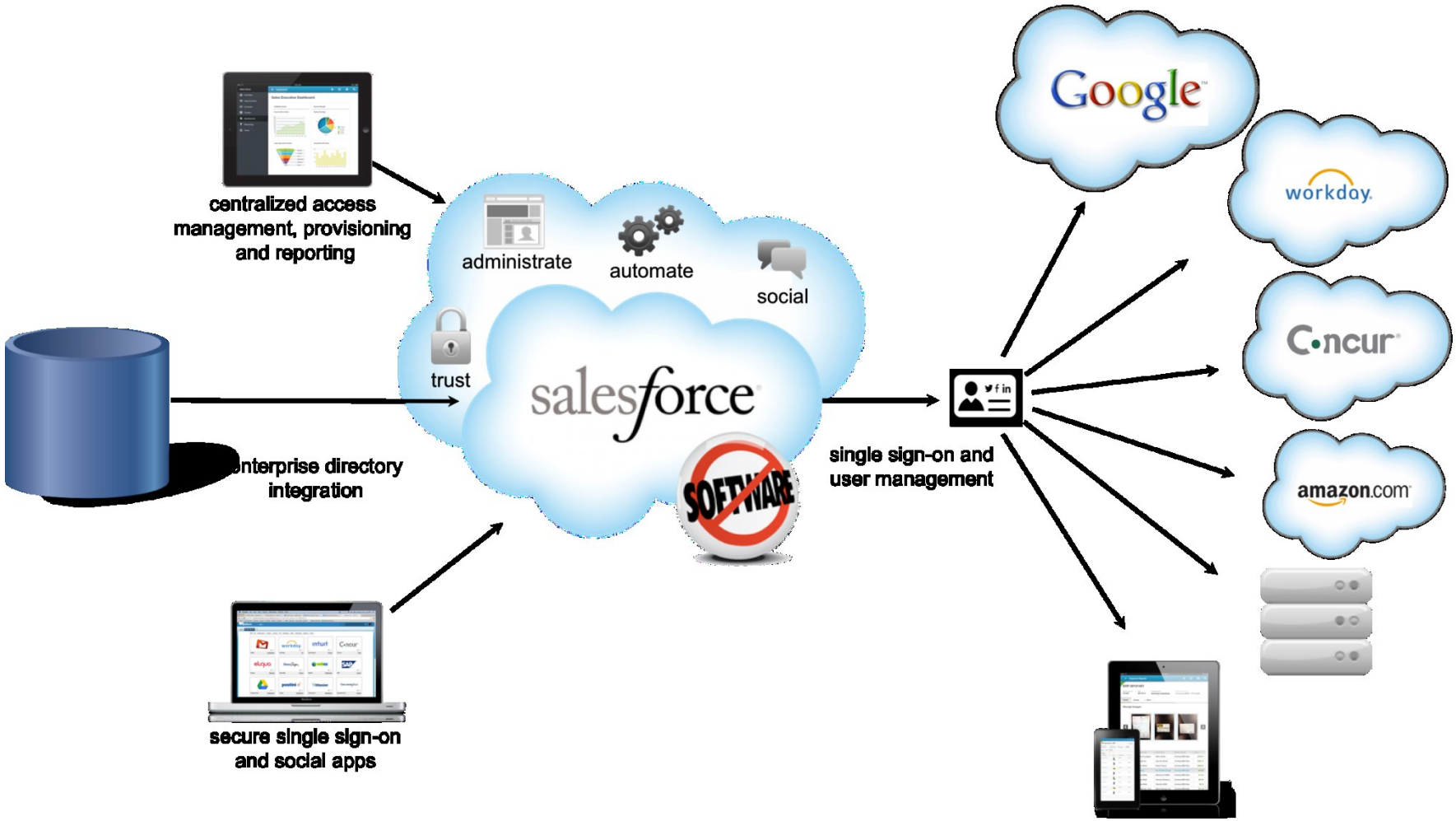
Timeline:

- Primul CRM oferit ca SAAS (Software as a service)
- 2005: ofera Force.com ca platforma pentru aplicatii
- 2010: a fost lansat Chatter (~ Facebook pentru afaceri),
  - A fost achizitionat Heroku
- 2011: achizitionarea platformei de monitorizare social media Radian 6; mai mult de 90,000 de clienti (Dell, AMD, SunTrust, Spring, Computer Associates, Kaiser Permanente,…)

Cloud in exemple

- ***Software as a Service (SaaS)***
- ***E.g.*** **Salesforce.com** - arhitectura
  - In 2009:
    - 1000 mirrored machines pentru 55K clienti enterprise si 1.5 M subscribers
    - 10 baze de date Oracle in 50 de servere
      - Mecanisme de indexare complexe
    - Interfata Ajax Web + servicii de comunicare variate
    - Numeroase plugin-uri via PaaS force.com (30M linii de cod din surse externe)
    - Multi-tenant: fiecare centru de date contine servere care sunt partajate intre clienti

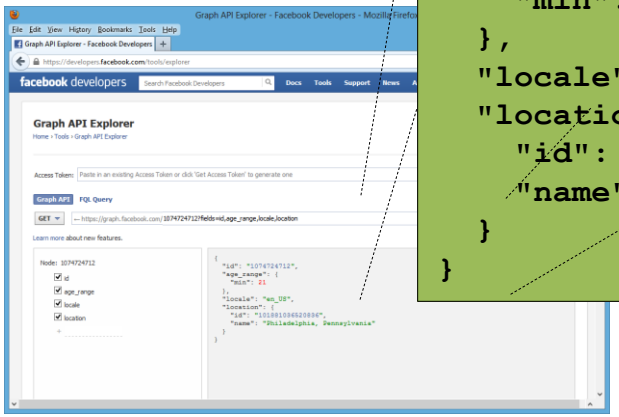
Cloud in exemple



Cloud in exemple

- *Platform as a Service (PaaS)*
- *E.g.* **Facebook** – furnizeaza capabilitati PaaS
  - Servicii Web – API-uri remote – care permit accesarea de date din retele sociale
  - Multe sisteme ruleaza aplicatiile in Amazon EC2, si folosesc interfata Facebook (in trecut Graph API, …)

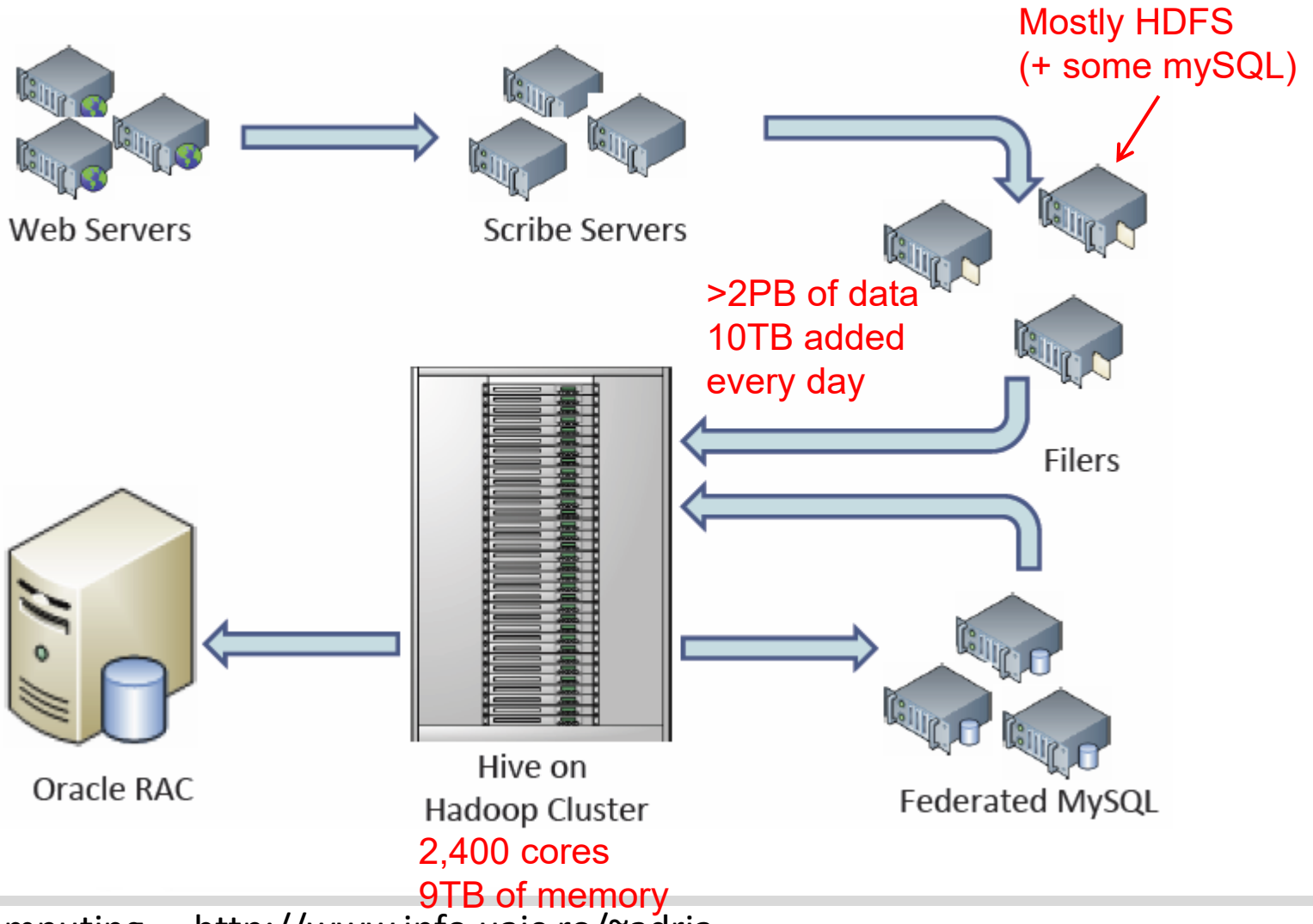
https://graph.facebook.com/(identifier)?fields=(fieldList)




```
{
  "id": "1074724712",
  "age_range": {
    "min": 21
  },
  "locale": "en_US",
  "location": {
    "id": "101881036520836",
    "name": "Philadelphia, Pennsylvania"
  }
}
```

  - Foloseste servicii PaaS pentru cloud-ul sau privat (e.g. analiza log-urilor, realizarea de sugestii, identificarea ad-urilor potrivite, etc)

Data Warehousing - Facebook



Cloud in exemple

- ***Platform as a Service (PaaS)***
- ***E.g.*** **Facebook**
- Scribe – inregistreaza datele care vor fi analizate de Hadoop
- Hadoop (MapReduce) *batch processing engine* pentru analiza datelor
- In 2009: cel de-al doilea cluster Hadoop din lume, 2400 cores, > 2PB data cu > 10TB adaugate in fiecare zi
  - Hive – SQL peste Hadoop, folosit pentru a scrie interogari de analiza a datelor
  - Federated MySQL, Oracle – multi-machine DBMSs de stocare a rezultatelor interogarilor

Cloud in exemple

- ***Infrastructure as a Service (IaaS)***
- **E.g. Netflix utilizand AWS**
- *Streaming movie retrieval and playback*
  - Fisiere media stocate in S3
  - Translatarea resurselor pe diferite dispozitive (iPad, etc) – se foloseste EC2
  - Amazon Web Services – gazduieste partea de cautare si de afisare a listei de filme
  - Folosind MapReduce se face analiza diverselor metrici de business
- **Lectii invatate de Netflix:**
  - ***Dorothy, you're not in Kansas anymore***
    - ***Be prepared to unlearn a lot of what you know***
    - ***Example: Assumptions about network capacity***
  - ***Best way to avoid failure: Fail constantly***
    - ***Design for failure independence;***
  - ***Learn with real scale, not toy models***
    - ***Only full-scale traffic shows where the real bottlenecks are***

Cloud Public|Securitate

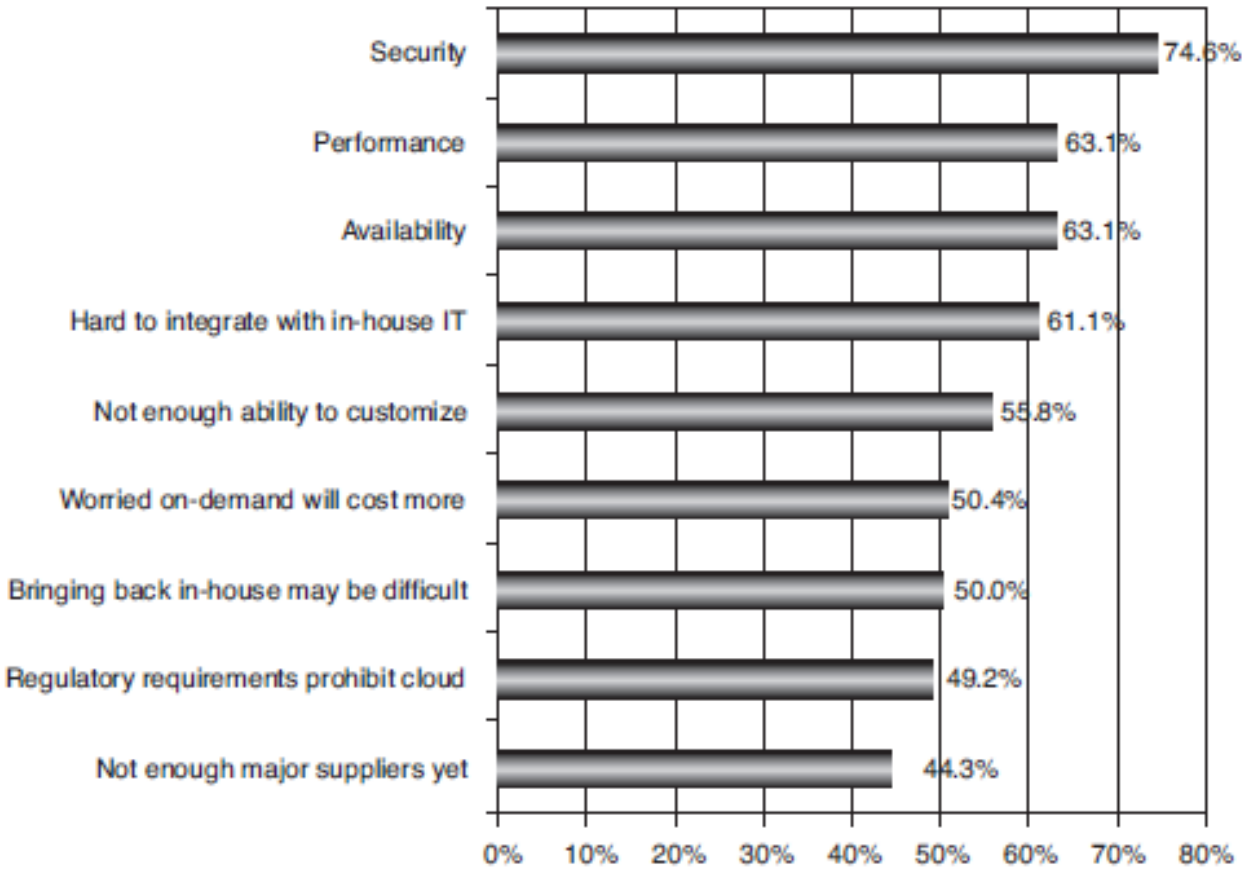


Figure 4.1 Results of IDC's 2009 annual survey of enterprise IT executives regarding concerns about adopting cloud computing for their core applications. Security has remained the top concern for the past three years.

- *"But how can anyone trust the cloud?"*
  - *This puts the fate of your company in the hands of third parties!"*

Cloud Public|Securitate

- Securitate la nivel fizic
  - Bazata pe experienta obtinuta din proiectarea si intretinerea de-a lungul timpului a centrelor de date de mari dimensiuni
  - *Security by obscurity*

    Accesul fizic este controlat: se face apel la personal specializat, supraveghere video, sisteme de detectie a potentialilor intrusi etc.

Cloud Public|Securitate

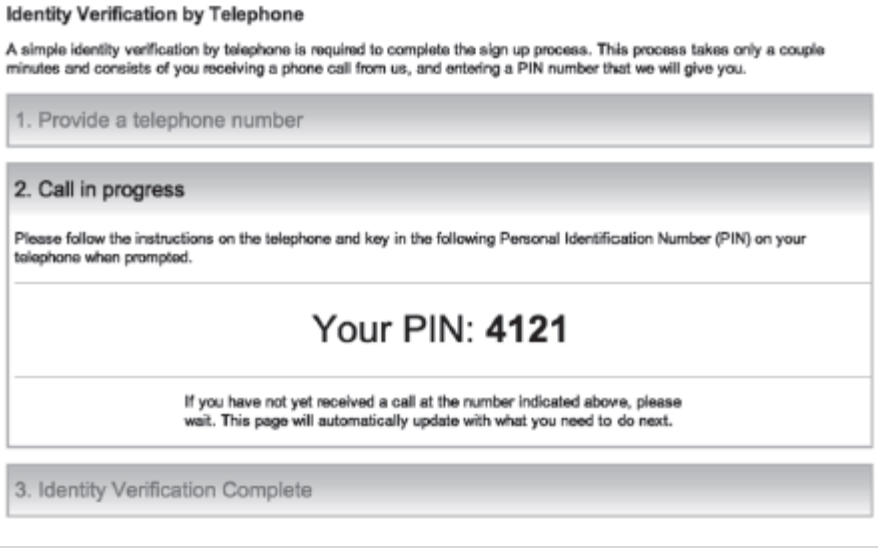
- Securitate la nivel fizic
  - Personalul autorizat foloseste metode multiple de securitate pentru accesarea resurselor
  - Certificarea *SAS 70 Type II (Statement on Auditing Standards No. 70)*
    - Similara American Institute of Certified Public Accountants (AICPA)
    - specifica metodele adecvate ce trebuie utilizate pentru controlul intern
- Exemplu: Gramm-Leach-Bliley Act (GLBA) - Financial Services Modernization Act of 1999, SOX audit (Sarbanes-Oxley) , HIPAA (Health Insurance Portability and Accountability Act) cer in mod obligatoriu SAS 70

Cloud Public|Securitate

- Controlul accesului
  - *Cine poate accesa cloud-ul?*
  - Use-case: AWS – foloseste metoda de control a accesului de la logare
    - Prima informatie secreta partajata: cardul de credit☺
    - *Billing validation*
      - Metoda folosita pentru a se asigura ca utilizatorul este detinatorul legitim a unui card ce poate fi utilizat intr-o tranzactie
      - Obs. Adresa nu este trecuta pe cardul de credit => adresa trecuta corect este un secret partajat care asigura un prim nivel de autorizare pentru acces la serviciile cloud

Cloud Public|Securitate

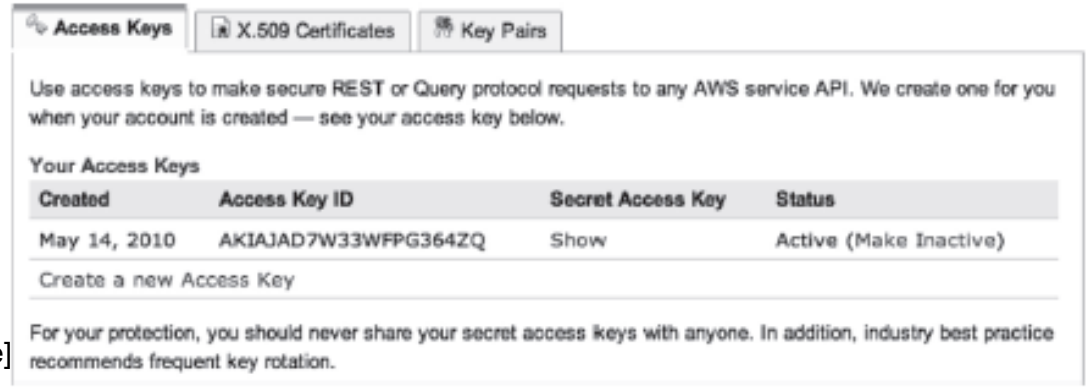
- Controlul accesului
  - *Verificarea identitatii via telefon* in stil *out-of-band*
    - *Out-of-band* <- neutilizarea unei aceeasi interfete (e.g. browser) folosit pentru autentificare; se face apel la un dispozitiv fizic pe care utilizatorul il detine fizic
    - Secretul partajat este un numar de telefon
    - => se verifica faptul ca esti cine spui ca esti
    - Exemplu AWS:



[Jothy Rosenberg, et. al.
The Cloud at your Service]

Cloud Public|Securitate

- Controlul accesului
  - *Credentialele de sign-in*
    - Se recomanda utilizarea RSA SecurID
    - *Multifactor authentication* este recomandata in raport cu *single-factor* (e.g. se utilizeaza doar parola).
  - *Access key*
    - *Utilizarea unui API* necesita obligatoriu o cheie de acces, care este oferita la inceput utilizatorului

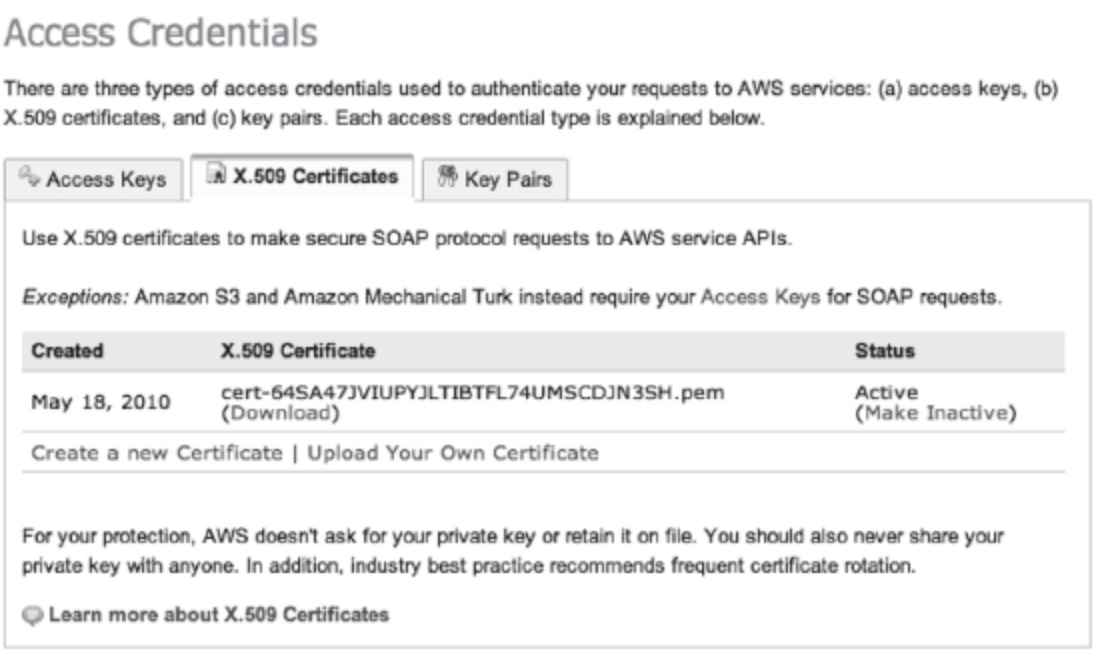


[Jothy Rosenberg, et. al. The Cloud at your Service]

Cloud Public|Securitate

- Controlul accesului
  - *Certificate X.509*
    - Sunt bazate pe *public key cryptography*
    - Sunt generate de furnizorul de cloud => pentru un moment cheia privata este detinuta de catre acesta

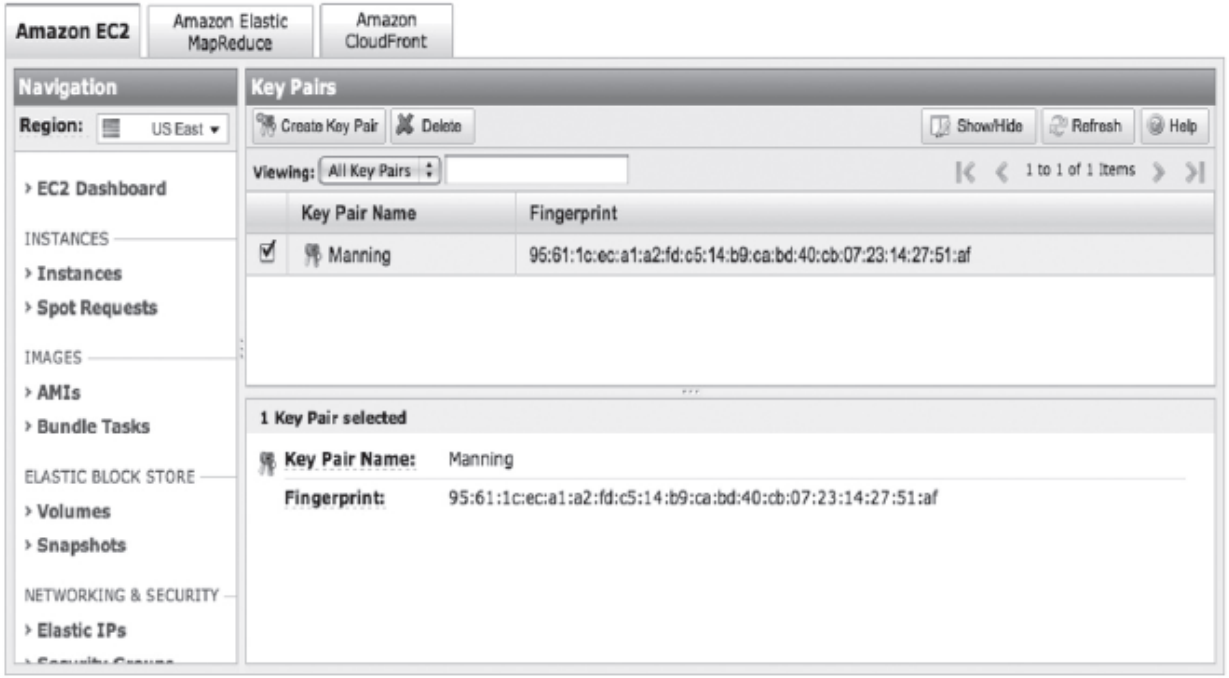
- Utilizare: se creaza o semnatura digitala pe baza cheii private si se include in cerere impreuna cu certificatul; cand furnizorul primeste cererea, foloseste cheia publica din certificat pentru decriptarea semnaturii si confirma identitatea celui care a facut cererea; furnizorul verifica de asemenea ca certificatul furnizat se potriveste cu cel din fisier



[Jothy Rosenberg, et. al.
The Cloud at your Service]

Cloud Public|Securitate

- Controlul accesului
- E.g. modalitatea de accesare a instantelor in cloud se face pe baza *Key pairs*
- Pentru fiecare serviciu se utilizeaza *key pairs* diferite



The ways key pairs are generated and managed through AWS's Management Console. The public key is retained at AWS, whereas the private key isn't. You can download it to your machine for secret storage.

[Jothy Rosenberg, et. al. The Cloud at your Service]

Cloud Public|Securitate

- Securitatea datelor si a retelei
  - *“cloud is more secure than most data centers”*
    - Centralizarea datelor in cloud versus date aflate in mod distribuit pe laptopurile diferitilor utilizatori din organizatie
    - Pentru date centralizate se realizeaza mult mai usor monitorizarea accesului si a utilizarii
    - Un atac reusit la nivel de cloud poate duce la pagube cu impact crescut, dar furnizorii de cloud pot oferi un timp de raspuns mai scazut si de cele mai multe ori mai specializat
    - Furnizorii de cloud realizeaza verificari permanente asupra datelor (e.g. Amazon S3 realizeaza MD5 hash pentru toate obiectele stocate in S3)

  => mentinerea propriilor centre de date este mai costisitoare si de multe ori mai putin sigura decat daca s-ar face apel la un furnizor de cloud

Cloud Public|Securitate

- Securitatea la nivelul sistemului de operare
  - Securitatea la nivel de sistem intr-un cloud public este furnizata la mai multe nivele: sistem de operare la nivelul host-ului, sistem de operare gazda sau sistemul de operare a instantei virtuale
    - => scopul: instantele masinilor virtuale sunt in siguranta in cloud si data continuta nu poate fi interceptata de sisteme neautorizate sau utilizatori neautorizati;
  - Exemplu: in Amazon, pentru a mentine securitatea hosturilor OS, se cere administratorilor AWS utilizarea cheilor SSH criptografice proprii pentru accesarea host-urilor *bastion (host*-uri proiectate si configurate sa protejeze infrastructura Amazon, si sunt inaccesibile utilizatorilor cloud-ului).

Cloud Public|Securitate

- Securitatea la nivelul retelei
  - Cloud-urile publice folosesc firewall-uri; acestea sunt configurate implicit in *deny mode* si utilizatorul trebuie sa isi deschida explicit porturile pentru a permite trafic; modificarile cer obligatoriu certificatele X.509
  - Exemplu: Amazon incurajeaza clientii cloud sa aplice ***filtre per-instanta*** => restrictionarea traficului de intrare si iesire per instanta
  - Atacuri de tip DDOS, sunt atenuate prin tehnici de tipul cook-uri SYN si limitarea conexiunii; mai mult furnizorii au la dispozitie o latime de banda care depaseste nevoia uzuala => impedica saturatia latimii de banda de un potential atac extern
  - Atacurile de tip Smurf nu sunt posibile in conditiile in care nu se permite trimiterea de date cu IP sau MAC sursa care nu apartin emitatorului

Cloud Public|Securitate

- *Co-mingling security*
  - Exemplu: In Amazon, nu este posibil ca o instanta virtuala care ruleaza intr-un mod promiscu sa primeasca sau sa capteze traficul destinat altei instante in cloud (desi clientii pot plasa diferite interfete intr-un mod promiscu, hypervizorul nu va furniza traficul care nu le este adresat; acest lucru este valabil inclusiv pentru doua instante detinute de acelasi client, si chiar daca sunt gazduite pe acelasi host)
- Securitatea datelor stocate
  - ACL controleaza permisiunile de scriere/stergere
  - ?data poate fi interceptata in comunicarea nod in cloud – nod in Internet?
    - API-urile de stocare sunt accesibile via endpoint-uri encriptate SSL => transferul datelor in ambele directii de comunicare (internet sau instante din cloud)

Cloud Public|Securitate

- Responsabilitatile si rolul detinatorului aplicatiei
  - Utilizatorii sunt responsabili pentru SO-ul gazda care ruleaza in mediul virtualizat (au drepturi de root si control administrativ complet asupra conturilor, serviciilor si aplicatiilor) => parolele, cheile secrete trebuie tinute in siguranta
    - Atacurile de tipul *social engineering* ramine o veriga foarte slaba la nivelul securitatii
  - Administratorii cloud-ului nu au acces la instantele clientului si nu se pot loga pe SO-ul gazda
    - Recomandari:
      - dezactivarea accesului bazat pe parola si utilizarea token-urilor sau autentificare bazata pe chei pentru a obtine access la conturi obisnuite

Cloud Public|Securitate

- Use case: *Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds*
  - Pasul 1 - *placement*: cercetarea arata ca este posibil sa iti dai seama asupra structurii cloudului, sa identifici unde este gazduita masina target, si sa ceri alocarea de masini virtuale pana cand una este *co-resident* cu cea vizata
    - Empirical mapping iti asingura o rata de succes de 40%
  - Pasul 2 - *extraction*: se poate construi un canal de atac (*side-channels*) intre VM-urile si se pot extrage informatii
    - E.g. CPU data cash

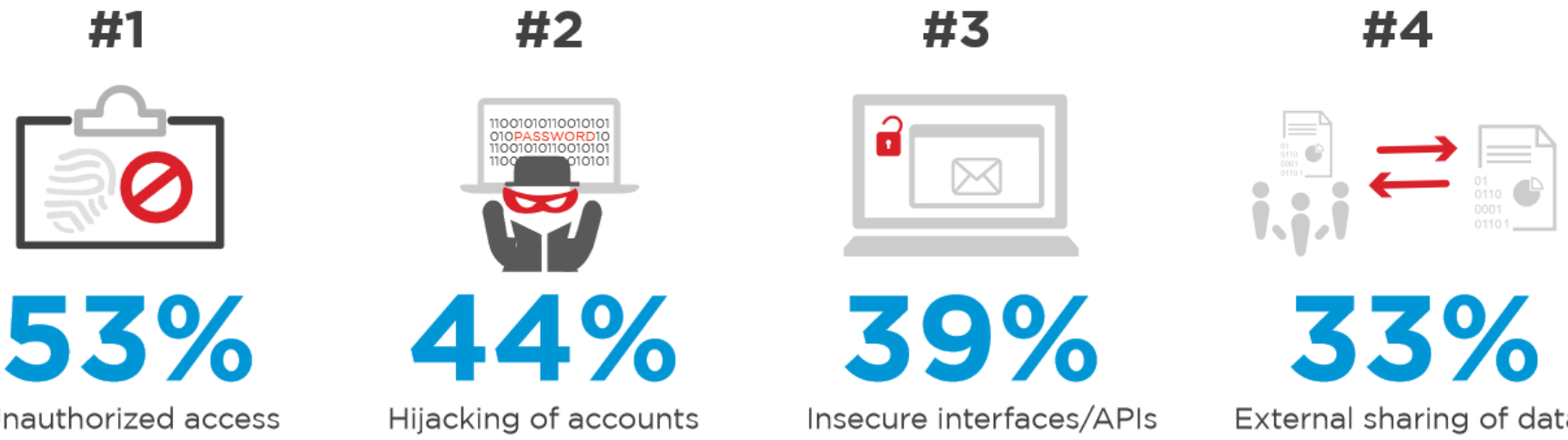
  Studiul a fost realizat asupra Amazon EC2.

  http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf#page=13&zoom=auto,-15,600
- Use Case: *Man in the Cloud Attack*
  https://www.imperva.com/docs/HII_Man_In_The_Cloud_Attacks.pdf

Cloud Public|Securitate

Probleme de securitate in cloud?

Unauthorized access through misuse of employee credentials and improper access controls is the single biggest threat (53%) to cloud security. This is followed by hijacking of accounts (44%) and insecure interfaces / APIs (39%). 33% of organizations say external sharing of sensitive information is the biggest security threat. Identity management and access control is an emerging and increasing threat concern for enterprises scaling and on-boarding to the cloud. The good news is that all these risks can be addressed by using security controls including multi-factor authentication, Identity and Access Management (IAM), Cloud Access Security Brokers (CASB), IP range restrictions and access auditing.



https://pages.cloudpassage.com/rs/857-FXQ-213/images/cloud-security-survey-report-2016.pdf

Cloud Public|Securitate

Probleme de securitate in cloud?....supozitii…

- ***One – the statistics on industries impacted by data security breaches are based on the industry of the data owner, not the industry of the service provider****. Clouds are run by service providers; they are not the data owners.*
- ***Two – the data security breach notification laws are structured such that service providers, including cloud service providers, must notify their customers and are not required to directly notify affected individuals or regulators.*** *The notice that cloud service providers give their customers may never become public.*
- ***Three – cloud service providers may be incentivized not to report data security breaches due to the potentially catastrophic impact on their business model****. That's speculation, of course, but should not go unnoted.*
- ***Four – and this one would be really mind-blowing – maybe data security breaches in the cloud just are not happening?*** *Again, speculation, but think about it.*

[http://www.cloudsecurityresource.com/topics/cloud-security/articles/421623-case-the-mysteriously-missing-security-breach-the-cloud.htm]

Cloud Privat

- Gartner Group: “predict that private cloud spending will soon exceed public cloud spending”
- Private Cloud (Internal Cloud sau Corporate Cloud) – “*A computing architecture that provides hosted services to a specific group of people behind a firewall. A private cloud uses virtualization, automation, and distributed computing to provide on-demand elastic computing capacity to internal users.*”
- *Obs.* Atribute ca: *pooled resources, metered billing* sunt mai putin aplicabile la cloud-ul privat
- Principalele consideratii privind cloud-ul privat:

Consideration	Rationale
Security	Applications that require direct control and custody over data for security or privacy reasons
Availability	Applications that require certain access to a defined set of computing resources that can’t be guaranteed in a shared resource pool environment
User community	Organization with a large number of users, perhaps geographically distributed, who need access to utility computing resources
Economies of scale	Existing data center and hardware resources that can be used, and the ability to purchase capital equipment at favorable pricing levels

[Jothy Rosenberg, et. al. The Cloud at your Service]

Cloud Privat

- Principalele consideratii privind cloud-ul privat:
  - **Securitatea**
    - Principala distinctie care face cloud-ul privat mai sigur, o constituie separarea resurselor fizice si logice mult mai bine ceea ce elimina indoielile in randul utilizatorilor
  - **Disponibilitatea**
    - Obs. Cloud-ul nu este o sursa infinita de resurse, a se vedea Amazon 2009 – si cele 500 XL de instante sau Rackspace – 2009 a impus folosirea a maxim 50 de instante/per user
  - **Comunitatea de utilizatori**
    - Pentru cereri medii de resurse de calcul, avand o politica buna la nivelul virtualizarii infrastructura existenta poate face fata cererilor; pentru organizatiile mari infrastructura de tip cloud este de dorit
  - **Perspectiva economica**
    - In situatii conventionale, organizatiile au nevoie de un numar mai mare de tehnicieni si ingineri pentru un data center mic -> migrarea catre cloud poate aduce economii

Cloud Privat

- Probleme in crerea unui cloud privat
  - Cloud-urile private sunt la scala mica
  - Aplicatiile *legacy* se porteaza greu intr-un cloud
  - *On-premises* nu implica neaprat si *more secure*
  - "*do what you do best*"
    - Optimizarea pe baza performantelor *real-time* in urma a milioane de tranzactii – "*private clouds will always be many steps behind the public clouds*"
- Dezvoltarea de solutii arondate cloud-ului privat – optiuni:

Provider type	Example vendors	Description
Open source	Eucalyptus, OpenNebula	Free software for creating a private cloud implementation, primarily on UNIX-based systems
Proprietary software	VMware, Enomaly, Appistry	Proprietary private cloud solutions open with a specific strength in a core cloud technology, such as virtualization, storage, or management
Hosted offering	Savvis, OpSource, SunGard	Dedicated hardware hosted in a cloud model for a single customer, built using either open source or a proprietary solution
System integrator	Appirio, Accenture, Infosys	Specialty providers or practice areas in large firms dedicated to architecture, design, and deployment of private clouds

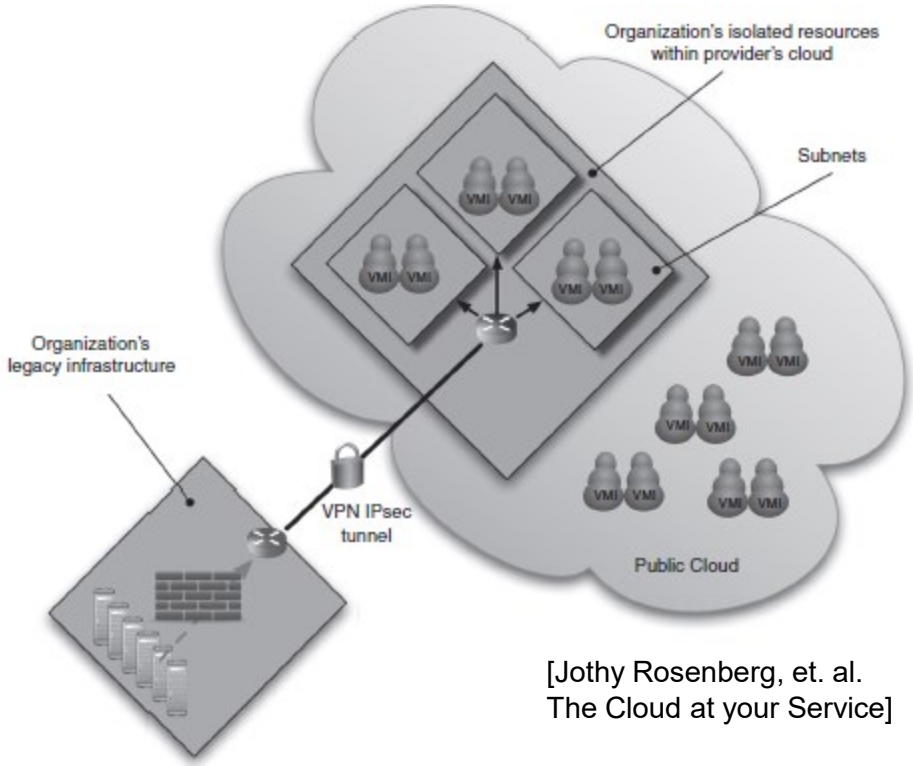
[Jothy Rosenberg, et. al. The Cloud at your Service]

Cloud Privat

- Dezvoltarea unui cloud privat – optiuni:
  - ***Private clouds/ open source***
    - Furnizorii de cloud implementeaza solutia in combinatie cu soft open source si soft *homegrown*
    - E.g. OpenStack, OpenShift, Eucaliptus, OpenNebula, ….
    - => poate fi utilizat pentru crearea de cloud hibrid
  - ***Solutii software in cloud proprietare***
    - Appistry , ParaScale(concentrat pe aspecte legate de stocarea in cloud), EMC, Oracle, IBM, Unisys (ofera intreaga stiva cloud)
  - **De la cloud public la cloud privat**
    - Hardware Amazon Virtual Private Cloud (VPC) permite conectarea de resurse la cloud-ul public prin firewall via IPsec VPN

Cloud Privat

- *Cloud privat Virtual (VPC)*
  - Amazonul este primul furnizor al acestui tip de model de cloud hibrid
  - Ideea: conectarea centrului de date privat cu Amazon Ec2
    - Instantele EC2 sunt utilizate in VPC pentru a adauga suport atunci cand traficul depaseste capacitatea resurselor *on-premise*
  - *Back-end*-ul aplicatiei, serverele de baze de date, serverele de autentificare ramin in centru de date privat
  - Amazon VPC permite conectarea infrastructurii cu noduri AWS izolate printr-un VPN
  - Google ofera *Secure Data connector* care conecteaza infrastructura on-premise cu platforma GAE



[Jothy Rosenberg, et. al. The Cloud at your Service]

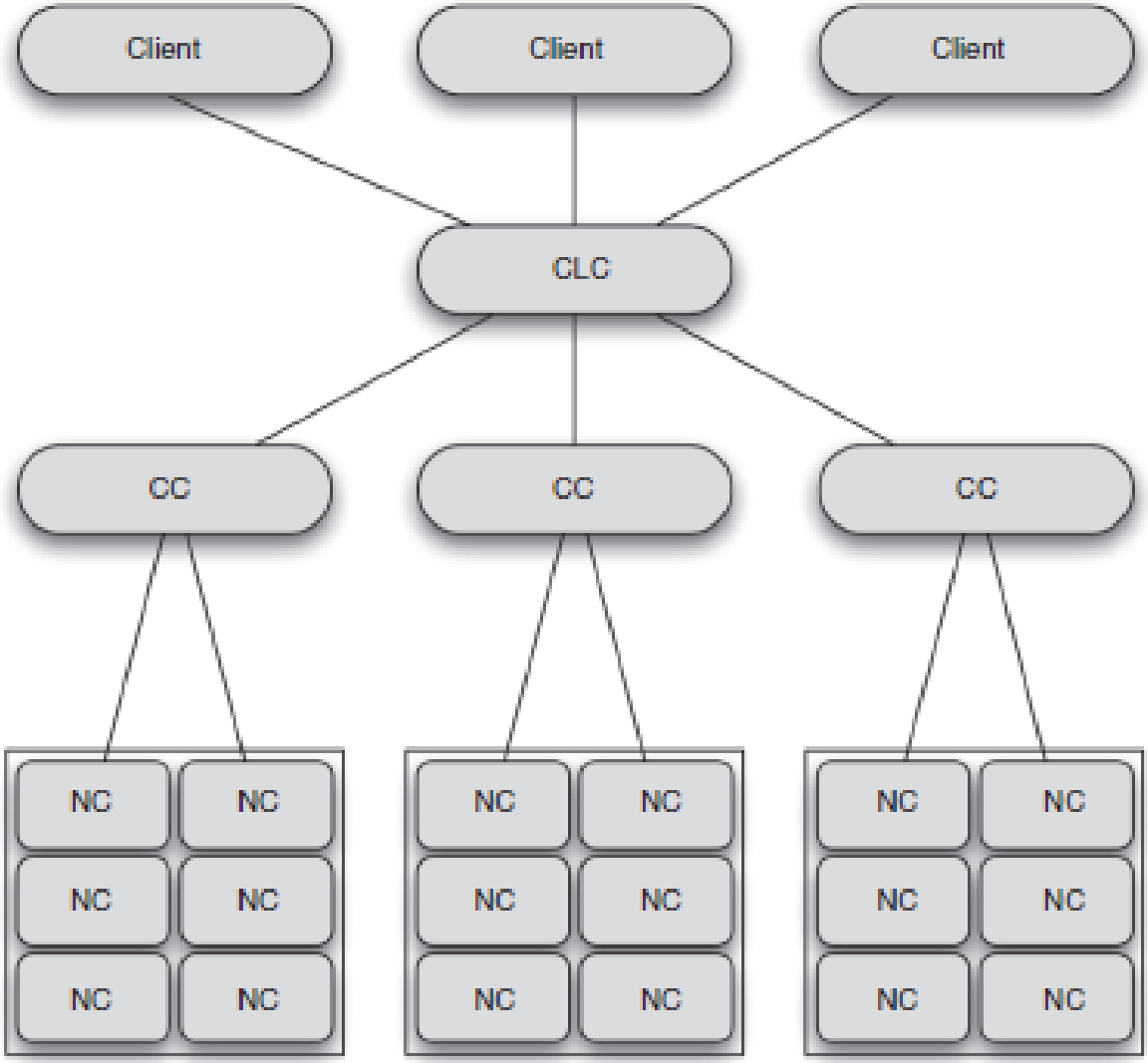
Cloud Privat

- *Cloud privat Virtual (VPC)*
  - Scenarii de utilizare
    - Expandarea aplicatiilor corporatiilor in cloud
      - Sisteme de email, sisteme financiare, aplicatiile CRM
    - Scalare elastica a site-ului web in cloud
    - Recuperarea in caz de dazastru
      - Pentru un simplu datacenter, recuperarea inseamna folosirea unei alt data-center din alta locatie => proces costisitor
      - Folosind VPC, periodic datele critice se pot salva in noduri de stocare in cloud

Cloud Privat

- *Use case:* Implementarea unui cloud open-source privat
  - Multe solutii de cloud privat au a dispozitie distributii Linux (Ubuntu Server – are optiunea UEC (Ubuntu Enterprise Cloud) => instalarea Eucalyptus)
  - Eucalyptos – avand ca start un proiect academic
  - Eucalyptus componente:
    - NC (Node Controller) – se gaseste pe fiecare computer pe care se doreste gazduirea de instante si face managementul acestora
    - CC (Cluster Controller) – este responsabil pentru managementul NC-urilor
    - CLC (Cloud Controller) face managementul unuia sau a mai multor CC
      - Este punctul central de management a intregului sistem
      - Tine evidenta utilizatorilor sistemului (administratorul se conecteaza la CLC pentru adaugarea utilizatorilor, alocarea instantelor, etc)
    - Componentele Eucalyptus comunica intre ele, dar doar CLC este expus cu o adresa publica

Cloud Privat



[Jothy Rosenberg, et. al.
The Cloud at your Service]

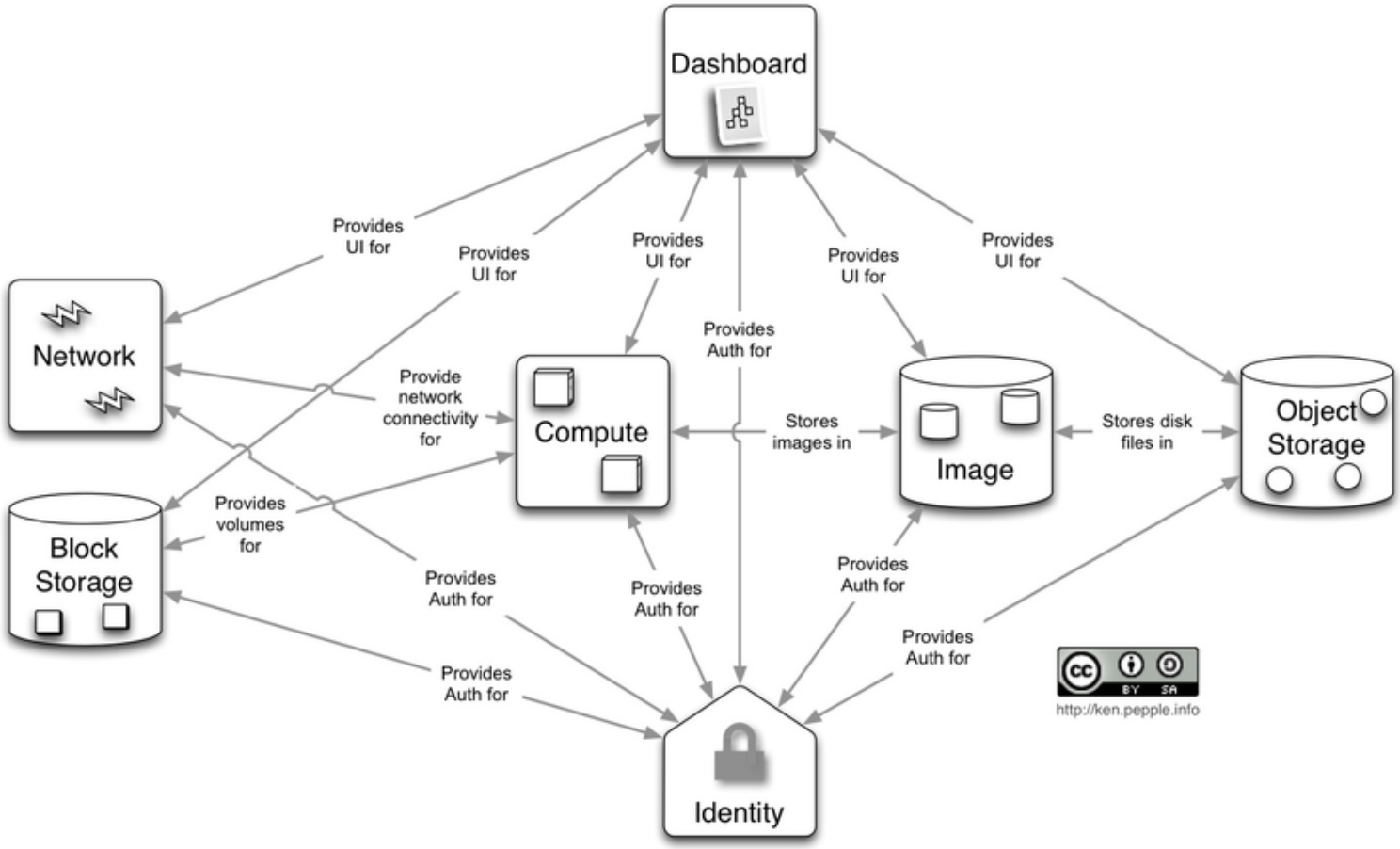
Cloud Privat

- *Use case:* Implementarea unui cloud open-source privat
  - Cel mai mic sistem de tip cloud: un nod cu rol de CC si CLC si un nod NC
  - Tehnologia de virtualizare implicit folosita este Xen (dar se poate folosi VMWare, VirtualBox)
    - OBS. Xen are avantajul interoperabilitatii si migrarii spre cloud-ul Amazon
  - Implementare:
    - Interfata CLC expusa clientilor este bazata pe SOAP, si este conform documentatiei WSDL de la Amazon
    - Interfetele de administrare folosite de Amazon in EC2 nu sunt disponibile public, si Eucalyptus implementeaza propriile interfete
    - In Cloud-ul Amazon, pentru registrare ai nevoie de aprobarea pe baza unui card de credit; in Eucalyptus se face o cerere printr-o interfata Web si se primeste accesul din partea administratorului
    - In cloud-ul privat administatorul poate porni sau termina o instanta, poate adauga imagini ale diskului etc.

Cloud Privat

Open Stack

- http://docs.openstack.org



[http://docs.openstack.org/trunk/openstack-compute/admin/content/conceptual-architecture.html]

Cloud Privat

Open Stack

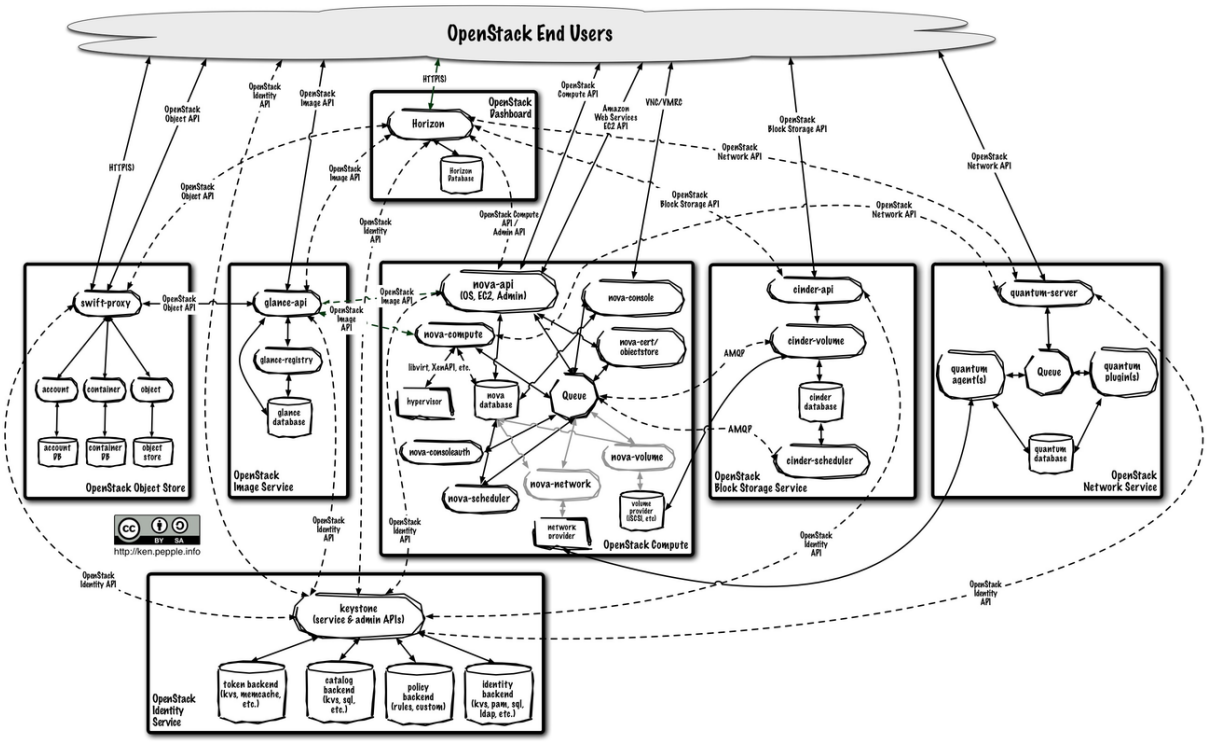
- Dashboard (“Horizon”) – front-end pentru alte servicii OpenStack
- Compute (“Nova”) – stocheaza si recuperaza disk-urile virtuale (“images”) si metadate asociate in Image
  - Rackspace si HP furnizeaza servicii comerciale bazate pe Nova
  - Este folosit ca nuclu al infrastructurii in Mercado Libre sau NASA (sursa de origine)
- Network (“Quantum”) – furnizeaza retea virtuala pentru Compute
- Block Storage (“Cinder”) furnizeaza mecanism de stocare persistent pentru Compute
- Image (“Glance”) – permite stocarea imaginilor diskurilor virtuale in Object Store
- Object Store (“Swift”) – permite stocarea si regasirea de fisiere
- Identity (“Keystone”) – asigura autentificarea tuturor serviciilor

[http://docs.openstack.org/trunk/openstack-compute/admin/content/conceptual-architecture.html]

Cloud Privat

Open Stack - arhitectura

- Utilizatorii finali pot interactiona prin intermediul unei interfete web (Horizon) sau un API
- Serviciile individuale interactioneaza intre ele prin API-uri publice (exceptie fac doar anumite comenzi de administrare)



[http://docs.openstack.org/trunk/openstack-compute/admin/content/conceptual-architecture.html]

Cloud Privat

- In realitate:
  - Sprint detine un cloud privat pentru aplicatii de detectarea a fraudelor
    - Sprint este o companie furnizoare de comunicatii wireless (are in jur de 50 de milioane de utilizatori) si este obligata sa faca procesarea datelor din acest sistem distribuit in timp real
    - Aplicatiile pentru detectarea fraudelor fac managementul la informatii private (credit card, localizarea geografica in timp real,…)
    - S-ar fi putut dezvolta un sistem in vechea traditie, folosindu-se servere de inalta performanta dar s-a facut apel la *commodity servers*
    - Softul folosit pentru managementul serverelor este de la Appistry
  - Bechtel PSN (Project Services Network)
    - Bechtel companie de constructii cu peste 40 de mii de anagajati
    - Analiza a costurilor:
      - amazon cere clientilor 0.15$/GB/luna versus Bechel plateste 3.75$/GB/luna;
      - Google mentine 20 de mii de servere cu un singur administrator, Bechel are 1 la 100 de servere)

Cloud Privat

- In realitate:
  - Bechtel PSN (Project Services Network)
    - Analiza a costurilor:
      - Salesforce.com are o versiune de aplicatie care serveste 1 milion de utilizatori (upgrade-ul se face de 4 ori pe an cu o perioada foarte mica de intrerupere) versus Bechtel care foloseste 230 de aplicatii cu pana la 5 versiuni pentru 40 de mii de angajati)
    - Solutia: standardizarea infrastructurii IT intr-un cloud privat => economii de 25-30% din toate costurile IT
  - Cloud privat guvernamental
    - Pentru date neconfidentiale se face apel la cloud-uri publice
    - Pentru datele confidentiale se creaza cloud-uri private (e.g. RACE (Rapid Access Computing Environement))

Cloud| Viziune asupra viitorului

- O imagine in trecut:

William Gibson (*The Economist, December 4, 2003), "The future is already* here—only, it's not evenly distributed."

1943	IBM's T. J. Watson predicted, "I think there is a world market for maybe five computers."
late 1970s	"The mainframe will always be the prevalent computing platform. The minicomputer is a toy."
early 1980s	"The PC will never be successful. People do not need their own personal computers."
mid-1980s	"The minicomputer will prevail. PC and networked computers are merely toys."
early 1990s	"The Internet has no real future as a computing platform. Too unreliable. Too hard to use. Could never support millions."
mid-1990s	"Electronic commerce is a joke. The Web is just a way to provide marketing information."
late 1990s	"There is no business model giving software away for free. The concept of collecting 'eyeballs' will never make money."

[Jothy Rosenberg, et. al. The Cloud at your Service]

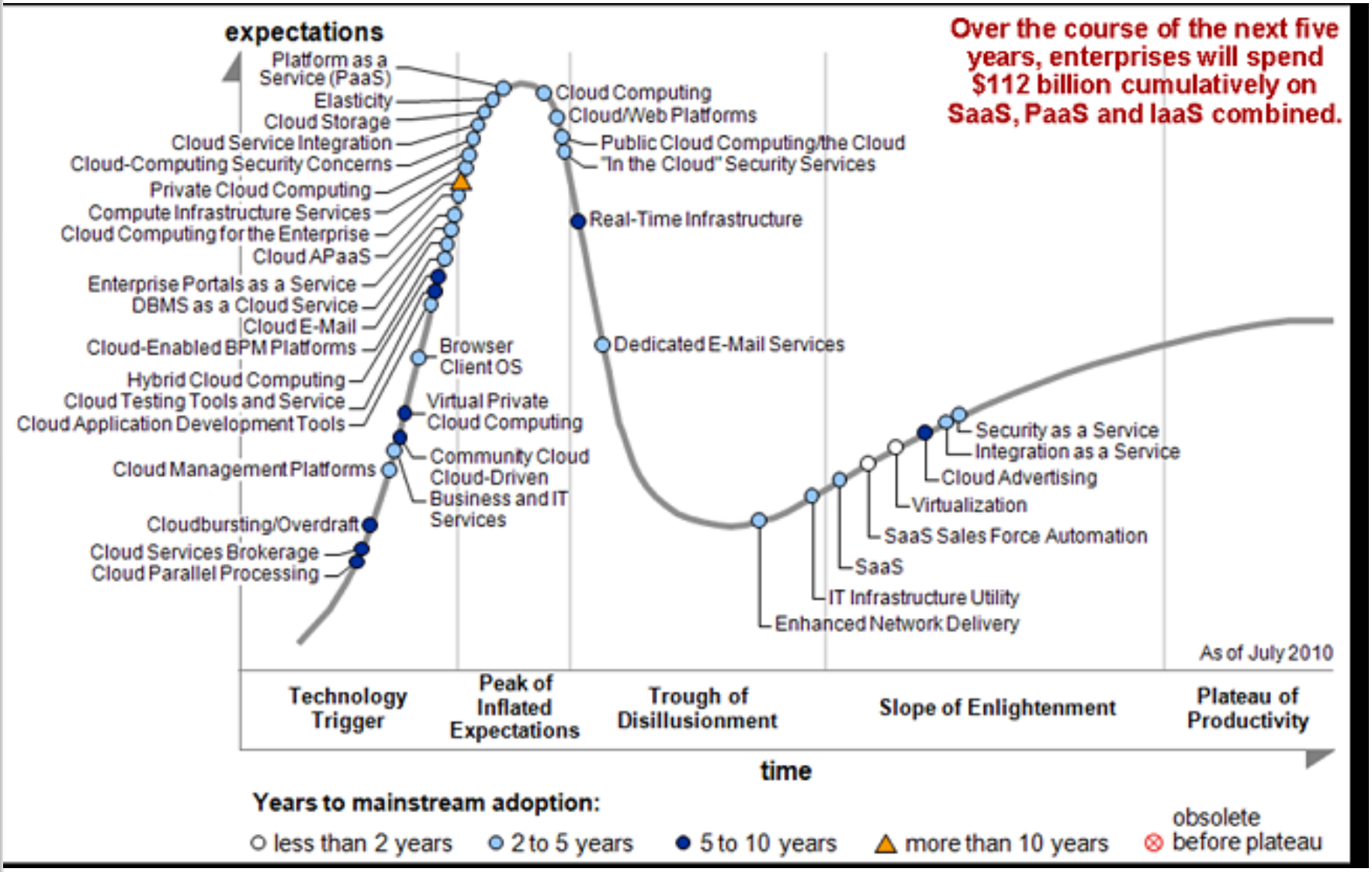
Cloud| Viziune asupra viitorului

- Urmatorii factori sunt responsabili pentru trecerea spre cloud:
  - Standardizarea aplicatiilor in browser

    - 1999: conceptul de *web application* in Java, Servleturi vers 2.2
    - 2005: Google Maps, Gmail foloseau Ajax
    - Pentru multe aplicatii actuale, Web-ul este platforma (Microsot Office versus Google Docs,…)
    - Chrome -> Google arata ca acest browser poate evolua catre functionalitatile unui sistem de operare
  - Miniaturizarea si standardizarea dispozitivelor
    - Tabletele si smartphone-urile vor fi/sunt dispozitivele principale de calcul folosite
  - Revolutia dispozitivelor mobile

[Jothy Rosenberg, et. al.
The Cloud at your Service]

Cloud| Viziune asupra viitorului



Cloud| Viziune asupra viitorului

Cloud Computing Activities by Different Age Cohorts

Internet users in each age group who do the following online activities (%)

	18-29	30-49	50-64	65+
Use webmail services such as Hotmail, Gmail, or Yahoo! mail	77%	58%	44%	27%
Store personal photos	50	34	26	19
Use online applications such as Google Documents or Adobe Photoshop Express	39	28	25	19
Store personal videos	14	6	5	2
Pay to store computer files online	9	4	5	3
Back up hard drive to an online site	7	5	5	4
Have done at least one activity	87%	71%	59%	46%
Have done at least two activities	59	39	31	21

Source: Pew Internet & American Life Project April-May 2008 Survey. N=1,553 Internet users. Margin of error is +3%

[Jothy Rosenberg, et. al.
The Cloud at your Service]

Cloud| Viziune asupra viitorului

- Zece predictii asupra modului cum va evolua cloud computing:
  - The cloud will be cheaper, more reliable, more secure, and easier to use.
  - The cloud will become a real engine of growth for early adopter companies.
  - Cloud providers' costs will be less than 25% of what corporate data centers cost.
  - Cloud mega-data centers will contain 500,000 servers costing $1B by 2020.
  - The best cloud provider operator's ratio of administrators to servers will go from 1:1,000 servers to 1:10,000 servers by 2020.
  - Open source will dominate the future of the cloud.
  - Pragmatic standards come from market leaders; Amazon's API will lead the way.
  - An ultimate ISO cloud standard will emerge.
  - Government will lead enterprises in cloud adoption.
  - SaaS will grow and stay current by using the basic web standards that will themselves continue to advance.

[Jothy Rosenberg, et. al. The Cloud at your Service]

Cloud| Concluzii

- Cloud Computing este o piata foarte complexa si care este intr-o evolutie accelerata
  - Aspectele economice sunt cheia
    - Foarte greu de inteles si controlat ☺

"I've looked at clouds from both sides now
From up and down, and still somehow
It's cloud illusions I recall...
I really don't know clouds at all" (Joni Mitchell)

Bibliografie

- Jothy Rosenberg, Arthur Mateos , The Cloud at your Service, Manning, 2011
- Tom White, Hadoop-The definitive Guide, Second edition, O'Reilly, 2011
- Katarina Stanoevska Slabeva, Thomas Wozniak, Grid and Cloud Computing - A Business Perspective on Technology and Applications, 2010, Editors Santi Ristol, Springer-Verlag Berlin Heidelberg
- Massimo Cafaro, Givani Aloisio, Grids, Clouds and Virtualization, 2011
- http://www.webopedia.com/DidYouKnow/Hardware_Software/Security/data_protection_in_the_cloud.html
- University of Pennsylvania, Cloud Computing Course – A. Haeberlen, Z. Ives, 2013
- http://www.cs.jhu.edu/~ragib/sp11/cs412/
- "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds"

  http://cseweb.ucsd.edu/~hovav/dist/cloudsec.pdf#page=13&zoom=auto,-15,600
- http://www.crn.com/slide-shows/security/300081491/the-10-biggest-data-breaches-of-2016-so-far.htm/pgno/0/5

Rezumat

- Cloud in exemple
- Aspecte de securitate in cloud-uri publice
- Cloud-uri private
- Cloud – viziune asupra viitorului

Ganduri de viitor…

- Edge Computing va inlocui Cloud Computing?☺

[http://www.informationweek.com/cloud/will-edge-computing-replace-the-cloud/a/d-id/1328929?]

Universitatea “Alexandru Ioan Cuza”
Facultatea de Informatică

Întrebări?