REPUBLIKA E SHQIPËRISË
UNIVERSITETI I TIRANËS
FAKULTETI I SHKENCAVE TË NATYRËS
DEPARTAMENTI I INFORMATIKËS

ARDI BENUSI

ZHVILLIME TË TEKNOLOGJISË “CLOUD”

TEZË DOKTORATURE

UDHËHEQËS SHKENCOR PROF. DR. ARTUR BAXHAKU

TIRANË, 2015

REPUBLIKA E SHQIPËRISË
UNIVERSITETI I TIRANËS
FAKULTETI I SHKENCAVE TË NATYRËS
DEPARTAMENTI I INFORMATIKËS

DISERTACION

i paraqitur nga:
MSc. Ardi BENUSI

udhëhequr nga
Prof. Dr. Artur BAXHAKU

Për marrjen e gradës shkencore

DOKTOR

Specialiteti: Informatikë

Tema:

Zhvillime të teknologjisë “Cloud”

Mbrohet më datë. ..../ ..../ 2015 para jurisë:

1. .....Kryetar
2. .....Anëtar (Oponent)
3. .....Anëtar (Oponent)
4. .....Anëtar
5. .....Anëtar

Përmbajtja

Lista e figurave III
Shpjegues i termave V
Hyrje VIII
1. Retë kompjuterike 1
1.1. Hyrje 1
1.2. Zanafilla e reve 2
1.3. Virtualizimi i HW 2
1.4. Kategoritë e reve 3
1.4.1. Infrastuktura si një shërbim 4
1.4.2. Platforma si një shërbim 4
1.4.3. Programet si një shërbim 5
1.5. Tipet e reve kompjuterike 6
1.6. Karakteristikat e një reje 7
1.6.1. Tiparet e MIV 8
1.7. Infrastruktura e ofruesit të shërbimit 11
1.7.1. Tiparet 11
1.7.2. Prania gjeografike 11
1.7.3. Ndërfaqja e përdoruesit 12
1.7.4. Rezervimi në avancë i kapacitetit 12
1.7.5. Shkallëzimi automatik dhe balancimi i ngarkesës 12
1.7.6. SLA 13
1.7.7. Hipervizori dhe zgjedhja e Sistemit të Operimit 13
1.8. Platforma e ofruesit të shërbimit 13
1.8.1. Gjuhët e programimit dhe framework-et 13
1.8.2. Opsionet e vazhdueshmërisë 14
1.8.3. Shembuj platformash 14
1.9. Retë publike dhe infrastruktura e shërbimit 17
1.10. Retë private, hibride dhe infrastruktura e shërbimit 18
1.11. Përmbledhje e teknologjisë virtuale 19
1.12. Përmbledhje dhe konkluzione 20
2. Arkitektura të reve kompjuterike 22
2.1. Hyrje 22
2.2. Arkitektura me një ose shumë instanca 22
2.2.1. Zgjedhja e shkallës me shumë klientë 24
2.2.2. Skema e pagesës për Microsoft Azure 26
2.3. Një përdorim tipik 27
2.4. Sistemet SAP 28
2.5. Qendra e të dhënave të virtualizuara 30
2.6. Konkluzione 32
3. Përdorimi i platformave të reve kompjuterike në GIS 33

3.1. Geographic Information System 33
3.2. Rëndësia e GIS 33
3.3. Aplikimet GIS në retë kompjuterike 34
3.4. Platforma GIS në renë kompjuterike 36
3.5. Konkluzione 38
4. Vëzhgime mbi çështjet e sigurisë në retë kompjuterike 39
4.1. Hyrje 39
4.2. Barrierat në retë kompjuterike 41
4.3. Rreziqet në retë kompjuterike 42
4.4. Siguria në rrjete 43
4.5. Siguria në nivel aplikimi 44
4.5.1. Rreziqet e sigurisë për Hipervizorin 45
4.5.2. Sulmet DoS/DDoS 45
4.5.3. Manipulimi i fushave të fshehura 46
4.5.4. Helmimi i Cookies 46
4.5.5. Captcha 47
4.5.6. Sulmi me Google 47
4.6. Siguria në ruajtjen e të dhënave 48
4.7. Sigurimi nga rreziqet e ndryshme në retë kompjuterike 49
4.8. Konkluzione 51
5. Një metodë për shkëmbimin e sigurt të të dhënave në retë kompjuterike mobile 53
5.1. Hyrje 53
5.2. Shifrimi i bazuar në identitetin e përdoruesit. 53
5.3. Rishifrimi i autorizuar 55
5.3.1. Funksionet bilineare dhe skema të përmirësuara të rishifrimit 57
5.4. Shkëmbim i sigurt i të dhënave në re 58
5.5. Sfidat në të ardhmen 60
6. Menaxhimi i identiteteve në retë kompjuterike 62
6.1. Windows CardSpace 64
6.2. OpenID 65
6.3. Prime – Menaxhimi i identiteteve dhe privatësisë për Evropën 65
6.4. SAML (Security Assertion Markup Language) 67
6.5. Shërbimi SSO për Google Apps 68
6.6. Force.com 69
6.7. Federimi në Amazon Web Services (AWS) 70
6.8. Konkluzione 70
Literatura 72

Lista e figurave

Figurë 1.1 Konvergjenca e teknologjive të ndryshme me renë kompjuterike 2

Figurë 1.2 Koncepti i virtualizimit 3

Figurë 1.3 Evoluimi i makinave virtuale 3

Figurë 1.4 Organizimi në shtresa 4

Figurë 1.5 Google App Engine 5

Figurë 1.6 Windows Azure 5

Figurë 1.7 Salesforce.com 6

Figurë 1.8 Azure Virtual Machines ofron IaaS 15

Figurë 1.9 Microsoft Azure Websites 16

Figurë 1.10 Azure Cloud Services ofron Platformë si një Shërbim 17

Figurë 1.11 Koncepti i virtualizimit 19

Figurë 2.1 Arkitekturat me një dhe shumë instanca 23

Figurë 2.2 Një skemë për zgjedhjen e arkitekturës me një ose disa instanca 25

Figurë 2.3 Një përdorim tipik i reve 27

Figurë 2.4 ERP me module 28

Figurë 2.5 Operacionet lexo dhe shkruaj në modulet ERP 29

Figurë 2.6 Sistemet SAP 29

Figurë 2.7 Abstragimet e sistemeve SAP 30

Figurë 2.8 Ndërtimi i SAP 31

Figurë 3.1 Një aplikim GIS 33

Figurë 3.2 Përdorimi i aplikimeve GIS 34

Figurë 3.3 Kalimi i GIS në retë kompjuterike 35

Figurë 3.4 Një platformë reje GIS 37

Figurë 3.5 Lista e funksioneve API 37

Figurë 4.1 Një shërbim në RE që parandalon DDoS 46

Figurë 4.2 Fushë e fshehur për përdoruesin "admin" 46

Figurë 5.1 Një skenar në retë kompjuterike mobile 53

Figurë 5.2 Shifrimi i bazuar në identitet 55

Figurë 5.3 Implementim i thjeshtë, por naiv i shifrimit të autorizuar 55

Figurë 5.4 Modeli i shkëmbimit në re 60

Figurë 6.1 Sistemi i menaxhimit të identiteteve 63

Figurë 6.2 Bashkëveprimi midis përdoruesit, aplikimit, shërbimit dhe CardSpace 65

Figurë 6.3 Identitetet e pjesshme të një entiteti 66

Figurë 6.4 Koncepti i SAML 67

Figurë 6.5 Hapat e transaksioneve SAML 69

Shpjegues i termave

ACS	Assertion Consumer Service
AD	Autoritet i deleguar
ADFS	Active Directory Federation Services
Amazon S3	Amazon Simple Storage Service
AMI	Amazon Machine Images
API	Application Programming Interface
AWS	Amazon Web Services
BGP	Border Gateway Protocol
C3	Citrix Cloud Center
CAD	Computer Aided Design
CI	Instancë qendrore
CLI	Command Line Interface
CRM	Customer relationship management
DBDH	bilinear Diffie-Hellman
DBMS	Database Management System
DDoS	Distributed Denail of Service Attack
DDH	Diffie-Hellman
DI	Instancat Dialoguese
DNS	Domain Name Server
DNSSEC	Domain Name Server Security Extensions
dSaaS	Data Sotrage as a Service
EC2	Elastic Cloud Computing 2
ERP	Entreprise Resource Planning

FHE	Fully Homomorphic Encryption
GH	Google Hacking
GHDB	Google Hacking Database
GIS	Geographic Information System
GUI	Graphical User Interface
HD	Hard Disk
HDV	Hard Disk Virtual
HTML	Hypertext Markup Language
HW	Hardware
I/O, H/D	Input/Output, Hyrje/Dalje
IaaS	Infrastructure as a Service
IDM	Identity Management
IDP	Identity Provider
IDS	Intrusion Dedection System
IIS	Internet Information Services
IV	Infrastruktura Virtuale
MA	Microsoft Azure
MCC	Mobile Cloud Computing
MITM	Man in the Middle
MIV	Menaxhim i infrastrukturës Virtuale
MSB	Menaxhimi i Shërbimeve të Biznesit
MV	Makinë Virtuale
NIST	Instituti Kombëtar i Standardeve dhe Teknologjisë
OS	Operating System

P2V	Physical to Virtual
PaaS	Platform as a Service
RAM	Random Access Memory
RDBMS	Relational Database Management System
SA	Sistem Autonom
SaaS	Software as a Servicve
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SAP	Systeme Anwendungen Produkte, Systems Applications and Products
SLA	Service-Level Agreement
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SP	Service Provider
SSO	Single Sign On
SW	Software
TI	Teknologjia e Informacionit
UI	User Interface
URL	Uniform Resource Locator
VPN	Virtual Private Network
WS	Web Services
WSDL	Web Services Description Language
XML	EXtensible Markup Language
XSS	Croos Site Scripting

Hyrje

Ideja e një rrjeti kompjuterik galaktik u dha rreth fundit të viteve 60 nga J.C.R. Licklider, i cili ishte përgjegjës për zhvillimin e Arpanet (Advanced Research Projects Agency Network). Vizioni i tij kërkonte që çdo njeri të aksesonte çfarëdo lloj programi në çdo cep të botës që ai ndodhej. Ishte një vizion që sot "tingëllon" pak a shumë me termin "Re kompjuterike".

Pas viteve gjashtëdhjetë, teknologjia Cloud është zhvilluar kryesisht me lindjen dhe evolucionin e Web 2.0. Me tej teknologjia "Cloud" u zhvillua me hapa gjigandë ku mund të përmenden:

1. Koncepti i shpërndarjes së aplikimeve enterprise nëpërmjet një ndërfaqeje web.
2. Shërbime komerciale web që u lejojnë kompanive të vogla dhe individëve të marrin me qira kompjutera nga ku mund të publikojnë në internet aplikimet e tyre.
3. Aplikime enterprise të ofruara nëpërmjet shërbimeve si Google Aps apo Microsoft.
4. Maturimi i teknologjisë së virtualizimit.

Shumë veta e kanë kuptuar rëndësinë e reve kompjuterike dhe të atyre çka ofrojnë përdorimi i tyre si p.sh kapacitete ruajtëse të mëdha të informacionit, ulje të kostove etj. E megjithatë drejtuesit e teknologjisë së informacionit janë të shqetësuar për sigurinë e të dhënave dhe ekziston akoma një dilemë: Brenda apo jashtë resë kompjuterike? Shumica janë skeptikë dhe ky skepticizëm lidhet kryesisht me elemente të sigurisë së të dhënave, privatësisë së klientëve, shpejtësisë së përpunimit dhe afishimit të informacionit të ruajtur në re.

Ky punim ka si qëllim studimin e reve kompjuterike; karakteristikat e një reje, tipet e tyre, modelet e ndryshme. Studimi është pajisur me një gamë të madhe shembujsh nga ofruesit më të mëdhenj të këtyre shërbimeve që operojnë sot në treg dhe që kanë ndryshuar rrënjësisht mënyrën e konceptimit dhe projektimit të reve kompjuterike.

Në vazhdim paraqiten arkitekturat më të rëndësishme të reve kompjuterike duke evidentuar modelet me një dhe shumë instanca e duke paraqitur sfidat dhe rreziqet e ndryshme në lidhje me klientët të cilëve u ofrohen shërbimet.

Më tej studiohet rasti i migrimit të informacionit nga një sistem GIS tradicional, në një re kompjuterike, paraqiten sfidat e këtij kalimi, avantazhet dhe disavantazhet dhe sugjerohet aplikimi i një modeli aplikimi GIS së bashku me API përkatëse.

Një nga çështjet kryesore të trajtuara është çështja e sigurisë, e cila ngrihet nga shumë autorë e studiues të ndryshëm si thelbësore për marrjen e një vendimi përfundimtar në favor të reve kompjuterike. Këtu analizohen rreziqet e shumta duke i krahasuar me rreziqet në sistemet tradicionale dhe duke sugjeruar zgjidhje të ndryshme. Skemat e sugjeruar janë të ndërtuara në mënyrë që të mbulojnë çështje të tilla të sigurisë dhe privatësisë si: konfidencialiteti, integriteti, autentikimi, rikuperimi i të dhënave në rast fatkeqësie. Një skemë të vetme për parandalimin e rreziqeve të ndryshme nuk mund të ketë, pasi problemet e sigurisë janë të shumta dhe më të ndjeshme sesa në rastin e sistemeve tradicionalë. Megjithatë kombinime të skemave të ndryshme janë të mundshme dhe efektive.

Retë kompjuterike mobile janë një derivat shumë i përhapur kohët e fundit i reve kompjuterike. Për shkak të fuqisë së kufizuar procesuese, baterisë së kufizuar, kapacitetit të vogël të ruajtjes së të dhënave, modelet e reve kompjuterike janë zgjidhja e vetme në rastin

mobile. Në këtë punim jepet një skemë e sigurt për transferimin e informacionit nga një përdorues mobile në tjetrin duke përdorur renë kompjuterike si magazinë të dhënash. Sistemi Elgamal, së bashku me rishifrimin e autorizuar dhe transformimet bilineare, janë përdorur për të siguruar një komunikim të sigurt në një re kompjuterike mobile.

Menaxhimi i identiteteve në retë kompjuterike është studiuar në tre aspekte. I pari është ai nga një IDM drejt një reje kompjuterike, pra transferimi nga një klient drejt një reje. I dyti është transferimi i informacionit nga një re drejt një IDM-je dhe i treti është menaxhimi i identiteteve nga një re kompjuterike drejt një tjetre. Nga autorë dhe studiues të ndryshëm arrihet në përfundimin se nuk ka një përgjigje të saktë në atë që një IDM është i duhur në të gjitha kontekstet. Menaxhimi i identiteteve shikohet si një sfidë më vete në problemet e reve kompjuterike, saqë shumë ofrues të SaaS kanë ndërtuar dhe krijuar funksionet IAM si për shembull duke aplikuar API për sisteme të federuar e duke ndërtuar diçka që i ngjason SSO. Trendi tjetër ka të bëjë me lulëzimin e tregjeve IAMaaS, ose IAM si një shërbim, ku ofrues të ndryshëm kanë ndërtuar funksionet IAM nga ose drejt reve kompjuterike.

Qëllimi dhe rëndësia e studimit

Punimi “Zhvillime të teknologjisë Cloud” ka si qëllim një studim sa më të gjerë të reve kompjuterike dhe shprehet në favor të kalimit në re të aplikimeve dhe kompanive të ndryshme. Studimi evidenton se çështja aq e diskutuar e sigurisë në retë kompjuterike është shumë e studiuar dhe pyetjes së shtruar brenda apo jashtë resë, mund t’i përgjigjet me një “po” gati të plotë në favor të kalimit në retë kompjuterike. Pavarësisht se retë kompjuterike po bëhen gjithmonë e më të pëlqyeshme nga kompanitë dhe individët, probleme të ndryshme ngrihen të cilët janë studiuar dhe evidentuar për të dhënë një tablo sa më reale të problemeve dhe rreziqeve të ndryshme gjatë kalimit në re. Në disa raste janë dhënë sugjerimet e duhura dhe zgjidhjet e plota.

Punimi shërben si trampolinë për studime të tjera dhe mund të përdoret nga studiues të tjerë për të zgjeruar akoma më shumë çështje të tilla të reve si; shifrimet praktike homomorfike, sistemet e unifikuara të identiteteve, çështjet e sigurisë në datawarehouse etj.

1. Retë kompjuterike

1.1. Hyrje

Tashmë janë bërë realitet teknologji të tilla si grup kompjuterësh, rrjete dhe së fundmi retë kompjuterike. Qëllimi i krijimit të tyre është përdorimi i këtyre burime të fuqishme dhe të virtualizuara, në dukje si një i tërë, për qëllime të ndryshme të individëve, kompanive dhe më gjerë.

Një synim i rëndësishëm i këtyre teknologjive është dobia që sjellin në fushën informatike. Këto shërbime informatike që ofrohen, janë një model i mirë biznesi duke përdorur pushtetin informatik në shërbimet publike; si ujë, gaz, energji elektrike dhe në telefoni. Kështu konsumatori paguan aq sa konsumon.

Re kompjuterike është një term i përdorur nga kompanitë e mëdha kompjuterike si Amazon, Google dhe Microsoft, për shërbimet komerciale informatike që ato ofrojnë. Qëllimi kryesor i këtij modeli është ofrimi i ruajtjes të të dhënave (storage), dhënia e programeve 'si shërbim', për biznese apo individë të cilët i aksesojnë këto në çdo kohë dhe nga çdo vend ku ato ndodhen [1, 17].

Reja kompjuterike përshkruhet si: iluzionin i burimeve të pafundme, apo mundësia për të paguar "aq sa duhet" as më shumë e as më pak; ndërsa sipas NIST (Instituti Kombëtar i Standardeve dhe Teknologjisë) përcaktohet si: paguaj aq sa e përdor, përdor në çdo kohë që të duhen këto burime informatike (rrjete, servera, të dhënat , aplikacione apo shërbime), merr aq sa të nevojitet, shfrytëzoi kur të duash këto burime.

E përmbledhur e gjitha sa më sipër, një re përshkruhet si:

- Paguaj aq sa përdor.
- Kapacitete elastike dhe iluzion të burimeve të pafundme.
- Menaxhim i ndërfaqes sipas dëshirës.
- Burime të virtualizuara.

Retë kompjuterike përfshijnë gjithashtu edhe API-s; programe zhvilluese të cilat lejojnë programuesit të përdorin apo të zhvillojnë më tej aplikacionet që ata përdorin. Qëllimi kryesor do ishte që konsumatorët të përdornin 'Renë' si infrastrukturë të TI për punën e përditshme duke hequr dorë përfundimisht nga makinat dhe shërbimet lokale [5].

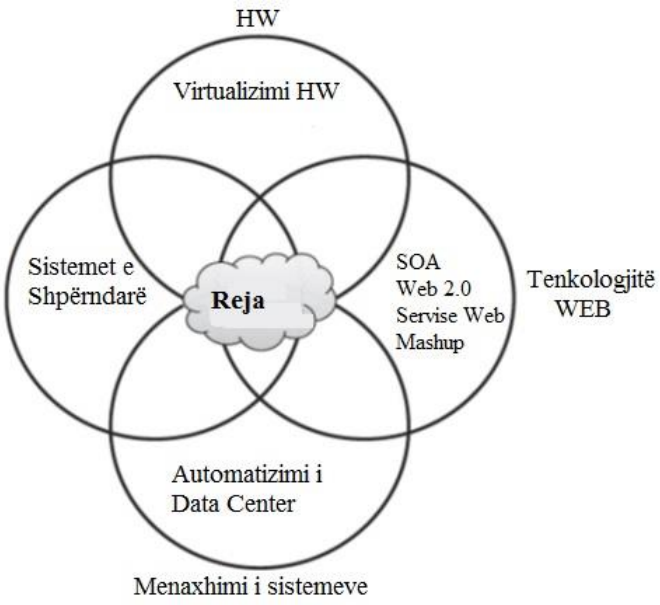
Ky kapitull ka për qëllim të hedhë një vështrim të përgjithshëm mbi retë kompjuterike si; historikun, karakteristikat, modelet dhe platformat e ndryshme duke analizuar hap pas hapi teknologjitë e nevojshme që kanë çuar në sistemet aktuale të reve. Gjithashtu një aspekt i trajtuar është ai i klientëve që përdorin renë, duke analizuar kërkesat dhe nevojat e konsumatorëve për një shërbim të sigurt dhe funksional.

1.2. Zanafilla e reve

Për të gjetur rrënjët nga vjen kjo iniciativë dhe kjo fillesë në teknologjinë e reve, mjafton të përmenden zhvillimet teknologjike në:

- Hardware (virtualizimin, procesorët me shumë shtresa).
- Zhvillimin e teknologjisë së internetit (shërbimet Web, arkitekturat services-oriented, Web 2.0).
- Shpërndarja e informacionit dhe teknologjisë (grupimet ,rrjetat).
- Menaxhimi i sistemeve (autonom, automatizimi i të dhënave në qendrat e të dhënave).

Figura më poshtë paraqet pikërisht këtë konvergjencë të teknologjisë drejt zhvillimit dhe përparimit të reve kompjuterike në teknologjinë e sotme.



Figurë 1.1 Konvergjenca e teknologjive të ndryshme me renë kompjuterike

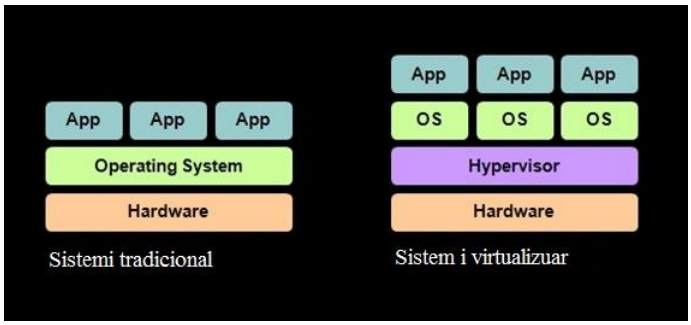
Ky model sjell avantazhe si për konsumatorin ashtu edhe për ofruesin e shërbimeve të TI-së. Konsumatori redukton kostot e TI-së duke zgjedhur një shërbim më pak të kushtueshëm nga ofruesit e jashtëm të këtyre shërbimeve, nuk investon në infrastrukturë e nuk trajnon dhe punëson personel të tepërt. Modeli sipas kërkesës, i lejon konsumatorit të përshtatë përdorimin e TI-së, ta rrisë ose ta zvogëlojë sipas nevojës që ka dhe që mund t‘i paraqitet [3].

1.3. Virtualizimi i HW

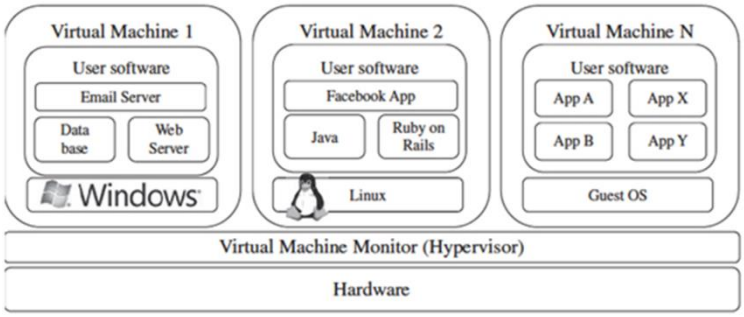
Shërbimet e resë kompjuterike zakonisht mbështeten nga disa qendra të dhënash, të cilat përbëhen nga mijëra kompjutera. Këto qendra të dhënash janë ndërtuar për t‘u shërbyer shumë përdoruesve dhe shumë aplikimeve të ndryshme. Për këtë arsye, virtualizimi konsiderohet dhe përdoret gjerësisht në shumicën e këtyre operacioneve të qendrave të të dhënave dhe mirëmbajtjen e tyre. Ideja e virtualizimit të burimeve të sistemit kompjuterik, e cila përfshin procesorët, memorien dhe pjesët I/O, ka kohë që

është zhvilluar dhe synon ndarjen dhe përdorimin sa më të mirë të sistemit kompjuterik. Virtualizimi HW, lejon përdorimin e disa sistemeve të shfrytëzimit dhe programeve në një platformë fizike të vetme.

Tashmë, përdorimi i teknologjisë me procesorë me shumë shtresa, pjesët HW që ndihmojnë në virtualizimin dhe migrimi që bëhet në makinat virtuale, ka kontribuar në adoptimin në rritje të virtualizimit në sistemet e serverave.



Figurë 1.2 Koncepti i virtualizimit



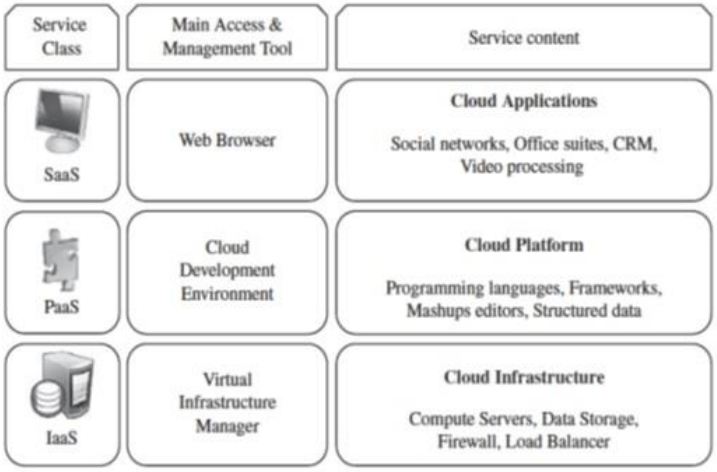
Figurë 1.3 Evoluimi i makinave virtuale

1.4. Kategoritë e reve

Shërbimet që ofrohen në retë kompjuterike janë të ndara në tri kategori, të cilat vijnë si pasojë e kapaciteteve që ofrojnë si dhe modelit të shërbimit.

1. Infrastruktura si një shërbim.
2. Platforma si një shërbim.
3. Programet si një shërbim.

Figura e mëposhtme paraqet organizimin në shtresa të resë duke filluar nga infrastruktura fizike në atë aplikative.



Figurë 1.4 Organizimi në shtresa

Këto nivele mund të shihen edhe si shtresa arkitekture, ku shërbimet e një shtrese më të lartë, mund të jenë të përbërë nga shërbimet e shtresës bazë.

Ky model reference shpjegon rolin e secilit nivel në një arkitekturë të integruar.

Mjediset e zhvillimit të reve janë të ndërtuara në krye të shërbimeve të infrastrukturës për të ofruar zhvillimin e aplikimit dhe në këtë nivel ndodhen modele të ndryshme programimi, API-s dhe editues të ndryshëm që mundësojnë krijimin e një hapësire për biznese të ndryshme, Web dhe aplikime shkencore [1, 3 ,4].

1.4.1. Infrastuktura si një shërbim

Ofrimi i burimeve të virtualizuara (ruajtja e të dhënave, komunikimi, llogaritja ose procesimi) sipas nevojës apo kërkesës, njihet si „Infrastruktura si një Shërbim“, IaaS.

Kjo infrastrukturë në renë kompjuterike bën të mundur sipas kërkesave, sigurimin e serverave të cilët mundësojnë zgjedhje të sistemeve të operimit dhe paketës së programeve që nevojiten. Kjo infrastrukturë shërbimesh është e pozicionuar në shtresën e fundit të sistemit të resë kompjuterike.

Amazon Web Services kryesisht ofron IaaS, e cila në rastin e shërbimit EC2 ofron makina virtuale me një paketë programesh të cilat mund të përshtaten njëlloj me serverin fizik të zgjedhur nga përdoruesi. Përdoruesit i jepen të drejta që i mundësojnë një numër të madh aktivitetesh në server si : ndezje dhe fikje të serverit, mundësi të instalimit të programeve, eksplorimi i HD “virtualisht”, si dhe konfigurimi i të drejtave të hyrjes në server dhe rregullave të firewall-it.

1.4.2. Platforma si një shërbim

Një infrastrukturë tjetër, që ofron një nivel më të lartë e të pavarur dhe, që e bën renë të programueshme lehtësisht, njihet si Platforma si një shërbim, ose si PaaS. Kjo platformë e resë u lejon zhvilluesve të programeve të krijojnë e të vendosin aplikacione në server pa pasur nevojë të dinë më parë burimet HW; numrin e

procesorëve, memorien e brendshme apo të jashtme që zënë aplikacionet që ata përdorin apo zhvillojnë. Gjithashtu, shumë modele programimi dhe shërbime të specializuara si ; aksesimi i të dhënave, mënyra e autentikimit dhe pagesa, janë paketa të cilat mund t'i përdorë lehtësisht zhvilluesi në dobi të tij.

Google AppEngine është një shembull i PaaS, e cila ofron mundësinë e zhvillimit dhe hostimit të aplikacioneve Web, e që zakonisht shkruhet në një gjuhë programimi si Python dhe Java. Gjithashtu Windows Azure është një shembull tjetër i kësaj platforme.

Ndërtimi i këtyre platformave përfshin edhe shërbimin e-mail, chatin e hyrje në shërbime të tjera. Slogani i tyre është: Fokusohu në aplikacionin tënd, të tjerat na i lër neve. Ky është një shembull i mirë i asaj çfarë ofron platforma si një shërbim.

Figurë 1.5 Google App Engine

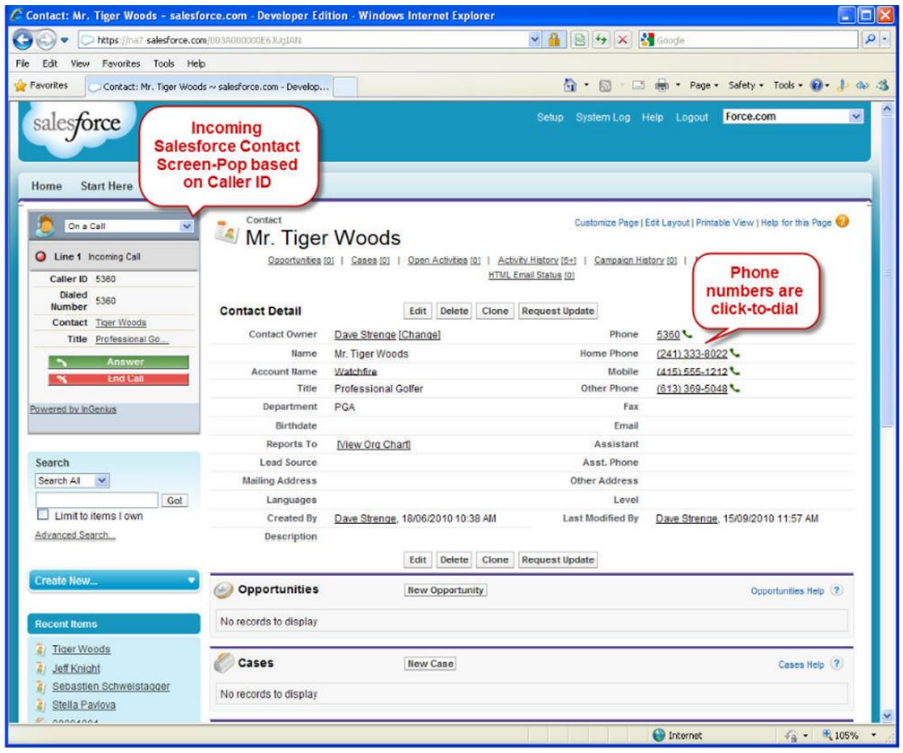
Figurë 1.6 Windows Azure

1.4.3. Programet si një shërbim

Aplikacionet qëndrojnë në pjesën më të larte të resë për nga mënyra e vendosjes. Shërbimet e këtyre ofruesve, mund të aksesohen nga përdoruesit nëpërmjet portaleve Web, gjë e cila mundësohet nga kjo shtresë. Përdoruesit kalojnë nga një program i instaluar në kompjuterin e tij, në një shërbim online, i cili u ofron atyre të njëjtat funksione si më parë. Aplikacionet tradicionale të wordit, excel, powerpoint etj., mund të aksesohen nga një shërbim në Web.

Ky model aplikacionesh i ofruar, i njohur si "Programet si një shërbim SaaS", mundëson që përdoruesit të mos kujdesen fare as për mirëmbajtjen e programit (instalim, update, ndryshime versionesh etj.) dhe as për testimin dhe funksionimin e tyre.

Salesforce.com përfaqëson një model SaaS e siguron mundësinë e përdorimit të aplikacioneve për biznese, ku këto të fundit janë vendosur në re nga ku përdoruesit mund të përshtatin dhe aksesojne aplikacionin në çdo kohë dhe nga çdo vendndodhje e tyre [1].



Figurë 1.7 Salesforce.com

1.5. Tipet e reve kompjuterike

Retë kompjuterike kryesisht perceptohen dhe shfaqen si shërbime kompjuterike publike, por në fakt ka dhe modele të tjera në varësi të vendndodhjes fizike të tyre dhe mënyrës së shpërndarjes e qëllimit që ato kanë. Në këtë aspekt, duke iu referuar mënyrës së shërbimit, retë mund të klasifikohen në publike, private, për përdorim të gjerë dhe hibride.

Reja publike është një re e ndërtuar për një publik të gjerë dhe në formën 'pay as you go', ndërsa reja private konceptohet si një qendër të dhënash të brendshme të një biznesi, apo të një organizate e cila nuk është e disponueshme për publikun e gjerë.

Në shumicën e rasteve, ndërtimi i një reje private nënkupton ristrukturimin e një infrastrukture aktuale duke shtuar virtualizimin dhe renë si një ndërfaqe. Kjo gjë i lejon përdoruesit të ndërveprojnë me qendrën e të dhënave lokale dhe ka të njëjtat avantazhe me retë publike, pra mund të aksesojë serverat virtualë, mund të ndryshojë dhe të modifikojë ndërfaqen, matjen dhe faturimin për përdorimin e tij. Reja 'për një përdorim të gjerë' është ndarje ndërmjet organizatave dhe mbulon disa komunitete specifike të cilët kanë të përbashkët qëllimin, si p.sh misionet fetare, ushtarake etj.

Një re hibride ose e ndërthurur konsiderohet një re private e mbështetur në kapacitetet kompjuterike të një reje publike.

1.6. Karakteristikat e një reje

Karakteristika të caktuara të një reje janë thelbësore për të mundësuar shërbimet që me të vërtetë përfaqësojnë modelin e një reje dhe për të kënaqur pritjet e konsumatorëve. Këto karakteristika mund të grupohen në:

a) Vetëshërbimin e serviseve.
b) Matja dhe faturimi për përdorim.
c) Elasticiteti.
d) Personalizimi.

a. Vetëshërbimi

Konsumatorët e shërbimeve në re kërkojnë të aksesojnë burimet dhe për të plotësuar kërkesat e mëdha, retë duhet të lejojnë kontrollin e vetëshërbimeve të serviseve në mënyrë që konsumatorët të mund t'i kërkojnë, t'i rregullojnë, t'i paguajnë dhe t'i përdorin këto shërbime pa ndërhyrjen e operatorëve apo personave të tjerë të specializuar.

b. Matja dhe faturimi për përdorim

Retë kompjuterike u lejojnë konsumatorëve të kërkojnë dhe të përdorin vetëm atë sasi të nevojshme për të cilën kanë nevojë. Shërbimet duhet të jenë me çmimin bazë për orë; pra konsumatori duhet të paguajë vetëm për aq orë sa e përdor shërbimin, duke i dhënë mundësinë përdoruesit që t'i lërë të lira burimet në momentin kur ato nuk janë të nevojshme e të mos paguajë për këtë kohë.

Për këto arsye, retë duhet të lejojnë zbatimin e tregtimit efikas të shërbimeve të tilla si çmimi, llogaritja dhe faturimi. Matja duhet të bëhet në përputhje me rrethanat e ndryshme si dhe me llojet e shërbimeve (p.sh. ruajtjen, përpunimin, dhe bandwidth) dhe përdorimit të tyre, duke siguruar një transparencë të madhe [2].

c. Elasticiteti

Retë kompjuterike japin iluzionin e burimeve të pafundme kompjuterike në dispozicion të

kërkesave të konsumatorit. Prandaj shumë përdorues e presin krahëhapur këtë inovacion, për të siguruar burime në çdo kohë e sasi. Në veçanti, pritet që burimet shtesë të mund të jenë sa më elastike duke parashikuar ndoshta automatikisht, kur ngarkesa e aplikimit rritet dhe kur kjo ngarkesë bie.

d. Personalizimi

Burimet e marra me qira nga reja duhet të jenë shumë të përshtatshme. Në rastin e shërbimeve të infrastrukturës, përshtatje do të thotë lejimi i përdoruesit për të vendosur pajisje të specializuara virtuale, të cilave do t'u jepen privilegje të veçanta në serverin virtual.

Klasat e tjera të shërbimeve (PaaS dhe SaaS) ofrojnë fleksibilitet më pak dhe nuk janë të përshtatshme për qëllime të përgjithshme informatike, por ende pritet të sigurojnë një nivel të caktuar të përshtatjes.

Një ndër sfidat më të mëdha që IaaS has kur ndërton infrastrukturën e një reje, është menaxhimi i burimeve fizike dhe virtuale, pra serverat, ruajtja e të dhënave dhe rrjeti. Orkestrimi i këtyre burimeve duhet të realizohet në mënyrë sa më të shpejtë dhe dinamike edhe për sigurinë e aplikimeve, e përgjegjës për këtë orkestrimin është menaxhimi i infrastrukturës virtuale (MIV). Ky lloj programi është i ngjashëm me një sistem operativ tradicional, por, në vend që të merret me një kompjuter të vetëm, ai agregon burime nga shumë kompjutera njëkohësisht, duke i paraqitur ato si një pamje uniforme para përdoruesit dhe para aplikacioneve.

Duke u nisur nga këndvështrimi i një reje si „tools“ apo mjete, është sugjeruar një diferencim ndërmjet dy kategorive të këtyre mjeteve të përdorura për të menaxhuar retë.

Kategoria e parë: cloud toolkits përfshin ata që ekspozojnë një ndërfaqe remote dhe të sigurt për krijimin, kontrollin dhe monitorimin e burimeve virtuale, por që nuk janë të specializuara në menaxhimin e infrastrukturës virtuale (IV).

Kategoria e dytë: menaxherët e infrastrukturës virtuale, të cilët ofrojnë karakteristika të avancuara të tilla si balancimin e ngarkesës automatike dhe konsolidimin e serverave, por nuk ekspozojnë ndërfaqe remote në re. Megjithatë, është vënë re se ka një mbivendosje midis kategorive; cloud-toolkits mund edhe të menaxhojë infrastrukturën virtuale edhe pse ata zakonisht ofrojnë karakteristika më pak të sofistikuara se sa menaxherët e specializuar.

Disponueshmëria e një reje remote si ndërfaqe dhe aftësia e menaxhimit të shumë përdoruesve si dhe e të drejtave të këtyre përdoruesve, janë karakteristikat kryesore që do të dallonin "cloud toolkits" nga "VIM-s."

1.6.1. Tiparet e MIV

Suporti për virtualizimin

Aspekti i marrjes me qira nga shumë konsumatorë të reve, kërkon që konsumatorëve të shumtë me kërkesa të ndryshme e të pabarabarta t‘u vihet në shërbim një infrastrukturë e vetme hardware.

Burimet e virtualizuara si CPU, memorie, etj, kanë një fleksibilitet të caktuar për përcaktimin e madhësive të tyre si dhe një fleksibilitet për ridimensionimin e tyre. Këto karakteristika e bëjnë virtualizimin hardware një teknologji ideale për të krijuar një infrastrukturë virtuale, që paraqet ose e ndan qendrën e të dhënave (data center) në një qiramarrje të shumëfishtë.

Vetëservise, kërkesa për sigurimin e burimeve

Aksesimi i burimeve nga vetëshërbimet, është perceptuar si një nga karakteristikat më tërheqëse të reve.

Kjo karakteristikë u mundëson përdoruesve të përdorin në mënyrë të drejtpërdrejt shërbimet nga retë, të tilla si konfigurime, politika të sigurisë etj., pa qenë e nevojshme bashkëveprimi me një administrator sistemi. Kjo aftësi redukton kohën për konsumatorin, eliminon punën intensive e shkresat zyrtare, kërkon më pak persona të angazhuar nga TI.

Paraqitja e një ndërfaqeje për vetëshërbimet, përmes të cilit përdoruesit mund të ndërveprojnë lehtësisht me sistemin, është një tipar shumë i dëshirueshëm edhe nga një menaxher i infrastrukturës virtuale.

Multiple Backend Hypervisors

Modele dhe programe të ndryshme virtualizimi ofrojnë përfitime të ndryshme. Kështu disa menaxherë të VI, mundohen të sigurojnë një shtresë uniforme, menaxhuese, pa marrë parasysh teknologjinë virtuale që është përdorur.

Kjo karakteristikë është më e dukshme për infrastrukturat virtuale open-source, të cilat zakonisht ofrojnë drivera automatikë për të bashkëvepruar me hipervizorë të ndryshëm. Në këtë drejtim, qëllimi i hipervizorit është që të sigurojë një API uniforme të cilën menaxherët e VI të mund ta përdorin për të menaxhuar makinat virtuale në nyjat e virtualizuara duke përdorur operacionet standarde që veçojnë thirrjet specifike të hipervizorit.

Virtualizimi i ruajtjes së të dhënave

Virtualizimi i ruajtjes apo i akumulimit do të thotë veçimi i magazinimit logjik nga ruajtja fizike. Konsolidimi i të gjitha pajisjeve të magazinimit të disponueshëm në një qendër të dhënash, lejon krijimin e disqeve virtuale të pavarura nga pajisjet. Pajisjet e ruajtjes shpesh janë të organizuara në një „Storage Area Network“ (SAN) dhe u bashkëngjiten serverave me anë të protokolleve të tilla si Channel Fibre, iSCSI dhe NFS. Një kontrollues magazinimi siguron shtresën abstrakte ndërmjet ruajtjes virtuale dhe asaj fizike.

Në sferën e menaxhimit VI, suporti i virtualizimit të magazinimit apo akumulimit shpeshherë është i kufizuar për produktet komerciale të kompanive të tilla si VMWare dhe Citrix.

Rrjetet Virtuale

Rrjetet virtuale lejojnë krijimin e një rrjeti të izoluar në krye të një infrastrukture fizike të pavarur nga topologjia fizike. Një LAN virtual (VLAN) lejon izolimin e trafikut që ndan një switched network, duke lejuar MV-le të grupohen në të njëjtën broadcast domain. Përveç kësaj, një VLAN mund të konfigurohet për të bllokuar trafikun që e ka fillesën nga makinat virtuale të rrjeteve të tjera.

Në mënyrë të ngjashme, koncepti VPN është përdorur për të përshkruar një mbishtresë të rrjetit të sigurt dhe privat në krye të një rrjeti publik (më së shpeshti në Internet publik). Suporti për krijimin dhe konfigurimin e rrjeteve virtuale të grupit VMs në një qendër të dhënash lejohet nga shumica e menaxherëve VI. Përveç kësaj, menaxherët VI që bashkëveprojnë me retë publike shpesh mbështesin VPN të sigurt duke lejuar lidhjen lokale dhe remote të makinave virtuale.

Alokimi i Burimeve Dinamike

Rritja e vetëdijes së konsumit të energjisë në qendrat e të dhënave, ka inkurajuar praktikën e konsolidimit dinamik të VMs në një numër sa më të vogël të përdorimit të serverave. Në infrastrukturën e reve, ku kërkesat e aplikimeve nga përdoruesit janë të ndryshueshme dhe dinamike, menaxhimi i kapaciteteve dhe parashikimi i kërkesave bëhen të komplikuara.

Ky fakt sjell si rrjedhojë nevojën për alokimin e burimeve dinamike duke synuar një harmonizim të kohës për furnizim dhe kërkesë. Reduktimi i konsumit të energjisë dhe menaxhimi më i mirë i SLA-ve mund të arrihet me një riplanifikim dinamik të VMs në makina fizike në intervale të rregullta. Makinave që nuk u janë caktuar ndonjë MV, mund të fiken apo të jenë në një gjendje që të harxhojnë sa më pak energji.

Në të njëjtën mënyrë, temperaturat e larta mund të shmangen duke iu larguar pikave të nxehta. Një numër i menaxherëve VI e përmban këtë tipar që vazhdimisht monitoron shfrytëzimin e burimeve dhe rialokon burimet e disponueshme ndërmjet VMs sipas nevojave të aplikimit.

Grupimet virtuale

Disa menaxherë të IV mund të menaxhojnë si një të vetme grupe të veçanta makinash virtuale. Ky tipar është i dobishëm për sigurimin e grupeve virtuale dhe të MV-le të ndërlidhura për aplikacionet me shumë shtresa të internetit.

Rezervimi dhe mekanizmi i negocimit

Kur përdoruesi kërkon burime të disponueshme kompjuterike në një kohë specifike të mëvonshme, këto kërkesa janë quajtur ‘rezervim i mëparshëm’, në kontrast me kërkesën kur përdoruesi i kërkon këto burime kur të jenë të disponueshme. Për të plotësuar kërkesa të tilla komplekse, duhet që të lërohen ato burime të dhëna me qira. Kjo gjë ndodh në retë ku burimet janë të pakta dhe ku jo të gjithë mund të jenë të kënaqur njëkohësisht, prandaj aplikohen prioritetet dhe rezervat për të kënaqur kërkesat e tyre.

Në funksion të saj dhënia me qira rinegociohet, duke u lejuar ofruesit dhe konsumatorit të modifikojnë ose të propozojnë mundësi të tjera derisa zgjidhja të arrihet. Kjo gjë ndodh kur konsumatori nuk kënaqet nga ajo çka ofrohet dhe ofruesi mundohet të krijojë mundësi të tjera për të plotësuar kërkesat e tij. Kjo gjë ka ndodhur më parë në OpenPEX, duke rinegociuar me përdoruesit me shkëmbime ofertash dhe kundërofertash.

Disponueshmëria e lartë dhe rikthimi i të dhënave

Disponueshmëria e lartë është tipari kryesor i menaxhuesve të IV, e cila synon minimizimin dhe parandalimin e rënies së aplikacioneve apo dëmtimin e të dhënave. Për të përmbushur këtë është siguruar një mekanizëm i cili zbulon nëse ka dëmtim të serverave fizikë dhe virtualë. Nëse konstatohet një gjë e tillë, riniset puna nga serverat e tjerë që nuk kanë probleme të tilla.

Kjo mënyrë mbron hostuesin por jo MV. Në rastet kur një aplikacion kritik dhe i rëndësishëm nuk zgjidhet duke rindezur MV, atëherë merren masa për të parë nivelet

e tjera të ruajtjes së tyre në MV. Një e tillë është mbajtja e MV-le në një server fizik të dytë.

Monitorimi i dështimeve të komponentëve të sistemit si p.sh i serverave, i MV-le, i disqeve dhe i rrjetit është gjithmonë i pranishëm dhe i mundur. Përveç kësaj duhet të ketë një dublim të shërbimit të MV në rast të ndonjë problemi me shërbimin apo me MV.

Ruajtja e të dhënave në renë kompjuterike duhet të merret shumë në konsideratë dhe të përfshihet në menaxhimin e MV-le. Periodikisht duhet të bëhet backup i të dhënave në një numër të madh MV-le dhe secila prej tyre me disa disqe bashkangjitur të bëhet pa luhatje në performancën e sistemeve, pasi kjo mund të sillte të tjera pasoja. Kështu, disa menaxhues të IV, ofrojnë një mekanizëm mbrojtës i cili bën një backup rritës të imazheve të MV-le. Shpeshherë zgjidhen si kohë të përshtatshme orët pas mesnate për të ruajtur nga ngarkimet e tepërta serverat dhe rrjetin.

1.7. Infrastruktura e ofruesit të shërbimit

Infrastruktura publike e ofruesit të shërbimit në përgjithësi ofron servera virtualë të cilët përmbajnë një ose me shumë CPU, kanë disa sisteme shfrytëzimi dhe paketa programesh të personalizuara, kanë hapësirë të madhe të ruajtjes së të dhënave dhe lehtësira komunikimi.

1.7.1. Tiparet

Duke u bazuar në një grup të përbashkët të karakteristikave, ofertat e IaaS mund të dallohen nga disponueshmëria e disa tipare të specializuara të cilat ndikojnë në koston e ulët; gjë që vihet re nga përdoruesit kur transferohen në re. Tiparet më të rëndësishme janë:

(i) shpërndarja gjeografike e qendrës të të dhënave
(ii) variacioni i ndërfaqes së përdoruesit dhe API për të hyrë në sistem
(iii) komponentët dhe shërbimet e specializuara që ndihmojnë aplikacione të veçanta (p.sh, balancuesit, firewalls)
(iv) zgjedhja e platformës virtuale dhe sistemeve të operimit
(v) metoda të ndryshme të faturimit dhe të periudhës (p.sh së parapaguar përkundër asaj të paguar më vonë, ose për orë kundrejt pagesës për muaj).

1.7.2. Prania gjeografike

Për të përmirësuar disponueshmërinë dhe përgjegjshmërinë, një ofrues i shërbimeve në re, zakonisht ndërton disa qendra të shpërndara të të dhënave në mbarë botën. Për shembull, Amazon Web Services paraqet konceptin e "Zonave të disponueshmërisë" dhe "rajone", për shërbimin e saj EC2.

Zonat janë të ndërtuara me parimin për të që të qenë të izoluara nga dështimet në zonat e tjera si edhe me shpërndaje më të lirë dhe mundësi lidhjeje të rrjetit me zonat e tjera të të njëjtit rajon.

Rajonet, nga ana tjetër, janë gjeografikisht të shpërndara dhe ndodhen në zona të veçanta gjeografike apo vende të ndryshme.

1.7.3. Ndërfaqja e përdoruesit

Një ofrues IaaS duhet të mundësojë mënyra të shumta aksesi në renë e tij, por kjo varet nga përdorues të ndryshëm dhe preferencat e tyre.

Llojet e ndryshme të ndërfaqeve të përdoruesit (UI), ofrojnë nivele të ndryshme hyrjeje dhe aksesi; më të zakonshmet janë ndërfaqet grafike të përdoruesit (GUI), command-line (CLI) dhe shërbimet Web (WS) dhe API.

Ndërfaqet GUI janë të preferuara nga përdoruesit të cilët kanë nevojë për të nisur, rregulluar dhe monitoruar serverat virtualë pa qenë e nevojshme të përsëritet procesi disa herë.

Nga ana tjetër ndërfaqet CLI ofrojnë më shumë fleksibilitet dhe mundësi të detyrave të përsëritura me anë të skripteve automatike (p.sh., të startojnë dhe të mbyllin disa servera virtualë në intervale të caktuara sipas dëshirës se përdoruesit).

Web dhe API ofrojnë aksese në programim duke përdorur HTTP standarde dhe lejojnë kështu shërbime të ndërlikuara për t'u ndërtuar në krye të reve IaaS.

1.7.4. Rezervimi në avancë i kapacitetit

Rezervimet në avancë i lejojnë përdoruesit të kërkojnë nga ofruesit e IaaS rezervim burimesh për një kohë të caktuar, duke siguruar që burimet e këtyre reve të jenë të përdorshme nga përdoruesit në kohën e kërkuar. Shumica e reve mbështesin formën që kur përdoruesi kërkon një shërbim të caktuar, burimet janë përherë të përdorshme.

Amazon Reserved Instances, është një formë e rezervimit në avancë të kapacitetit, e cila e lejon përdoruesin të paguajë një shumë fikse parash paradhënie, që të garantojë burimet në çdo kohë për periudhën e marrëveshjes së arritur më parë. Vetëm periudha të gjata nga 1 deri në 3 vjet ofrohen nga kjo kompani, prandaj edhe përdoruesit nuk mund të shprehin pakënaqësi ndaj kësaj forme, pasi s’mund të bëjnë një rezervim për orë apo për një ditë të caktuar.

1.7.5. Shkallëzimi automatik dhe balancimi i ngarkesës

Siç u përmend edhe më herët në këtë kapitull, elasticiteti është një karakteristikë kryesore e modelit të reve. Aplikimet shpesh duhet të ngrihen dhe të ulen për të përmbushur kushtet e ndryshme të ngarkesës që vjen gjatë punës .

Shkallëzimi automatik është një tipar shumë i dëshirueshëm i reve IaaS. Shkallëzimi automatik i lejon përdoruesit të vendosë kushte si p.sh, kur ata duan që aplikacionet e tyre të rrisin në bazë të kërkesës specifike numrin e transaksioneve për sekondë, apo numrin e përdoruesve të njëkohshëm në sistem.

Kur numri i serverave virtualë rritet me një shkallë të caktuar, trafiku në hyrje duhet të shpërndahet automatikisht midis serverave që janë në dispozicion.

Ky aktivitet u mundëson aplikacioneve të përgjigjen menjëherë ndaj rritjes së trafikut e gjithashtu lejon një tolerancë më të madhe ndaj ndërprerjeve të shërbimeve.

1.7.6. SLA

Service-level agreement janë të ofruara nga IaaS për të shprehur angazhimin e tyre për ofrimin e një kualiteti të caktuar të shërbimit. Për konsumatorët ajo shërben si një garanci. Një SLA zakonisht përfshin disponueshmërinë dhe garanton një shërbim pa ndërprerje. Shumica e ofruesve të IaaS e përqendrojnë SLA-në në garantimin e disponueshmërinë dhe duke specifikuar përqindjen minimale të kohës gjatë së cilës shërbimi do të jetë në dispozicion për një periudhë të caktuar.

1.7.7. Hipervizori dhe zgjedhja e Sistemit të Operimit

Tradicionalisht, shërbimet që ofrojnë IaaS janë të bazuara dhe përshtatura më shumë për burimet e hapura (open source) si p.sh XEN. Ofruesit e IaaS duhet të kenë eksperiencë të mirë në Linux, në rrjete, në virtualizim, në menaxhimin e burimeve si dhe në shumë aspekte të tjera të virtualizimit dhe sistemeve të operimit, që të mund të menaxhojnë atë çka ata ofrojnë dhe për të ruajtur klientët e tyre në re.

Kohët e fundit, ka pasur një ngritje të platformave IaaS të tilla si, VMWare vCloud dhe Citrix Cloud Center (C3), të cilat kanë ulur pengesat dhe barrierat e hyrjes për kompetitorët IaaS, duke çuar në zgjerim të shpejtë të tregut për platformën IaaS [4].

1.8. Platforma e ofruesit të shërbimit

Platformat e ofruesit të shërbimit në re, zakonisht ofrojnë zhvillimin dhe vendosjen e mjedisit që u lejojnë përdoruesve të krijojnë dhe të ekzekutojnë aplikacionet e tyre në një nivel të ulët të të drejtave në platformë. Përveç kësaj, gjuhë programimi specifike dhe framework-e janë në dispozicion të përdoruesve, si edhe shërbime të tjera të tilla si; ruajtja e të dhënave në mënyrë të vazhdueshme dhe përdorimi i cache-ve.

1.8.1. Gjuhët e programimit dhe framework-et

Modelet e programimit të vëna në dispozicion nga ofruesit e IaaS përcaktojnë se si përdoruesit mund të krijojnë aplikacionet e tyre duke përdorur nivele të larta të abstraksionit dhe si t‘i zbatojnë me efikasitet ato në platformën e reve.

Çdo model synon zgjidhje të efektshme të një problemi të veçantë. Në re, aktivitetet më të zakonshme që kërkojnë modele të specializuara janë:

- përpunimi i të dhënave të mëdha nga grupe kompjuterash (modeli MapReduce)
- zhvillimi i kërkesave ndaj shërbimeve dhe të aplikacioneve në internet
- përcaktimi dhe orkestrimi i proceseve të biznesit në formën e workflows (Modeli Workflow)
- performancë të lartë ekzekutimi të detyrave të ndryshme kompjuterike.

Për lehtësi të përdoruesit, PaaS ofron zakonisht gjuhë të ndryshme programimi. Gjuhët më të njohura dhe të përdorura, perfshijnë Python dhe Java (Google AppEngine), .NET (Microsoft Azure) dhe Ruby (Heroku). Force.com p.sh ka ndërtuar vetë një gjuhë programimi të quajtur Apex, e cila ofron nivel të lartë dhe funksionalitete të shumta në platformë.
Një gamë e gjerë e programeve „framework“ u janë ofruar zhvilluesve në platformë, gjithmonë duke u mbështetur në kërkesat funksionale dhe në fokusin që aplikimi mund të ketë. Ofruesit e reve që bazohen në Web dhe në aplikime hostimi, zakonisht ofrojnë framework-et më të zakonshme dhe më të njohurat si Ruby on Rail, Spring, Java EE dhe .Net-i.

1.8.2. Opsionet e vazhdueshmërisë

Problemi i vazhdueshmërisë së shërbimit është shumë thelbësor. Vazhdueshmëria lejon që aplikacionet të ruhen në gjendjen që ato janë aktualisht dhe në momentin që mund të ketë dëmtime apo probleme, mund të bëhet rikthimi i tyre në gjendjen e mëparshme. Gjithashtu ruhen edhe të dhënat e përdoruesit. Tradicionalisht, zhvilluesit e Web dhe të aplikacioneve kanë zgjedhur gjithmonë databaza relacionale si më komode. Këto databaza kanë një strukturë të besueshme dhe shpejtësi të mirë të përpunimit dhe ruajtjes së informacionit, por nuk mund të zgjerohen shumë (p.sh në petabytes), pasi mund të sjellin probleme në funksionim.

Në retë kompjuterike, teknologjitë e ruajtjes e të shpërndarjes janë më të fuqishme dhe më të shkallëzuara në krahasim me strukturat relacionale. Për shembull, Amazon SimpleDB dhe Google AppEngine ofrojnë më pak skema dhe relacione të cilat automatikisht indeksohen nga shërbimet e bazës së të dhënave. Kërkimi i informacionit është vetëm në disa tabela individuale dhe operacionet bashkuese mbi tabelat nuk lejohen për shkak të uljes së performancës dhe shkallëzimit.

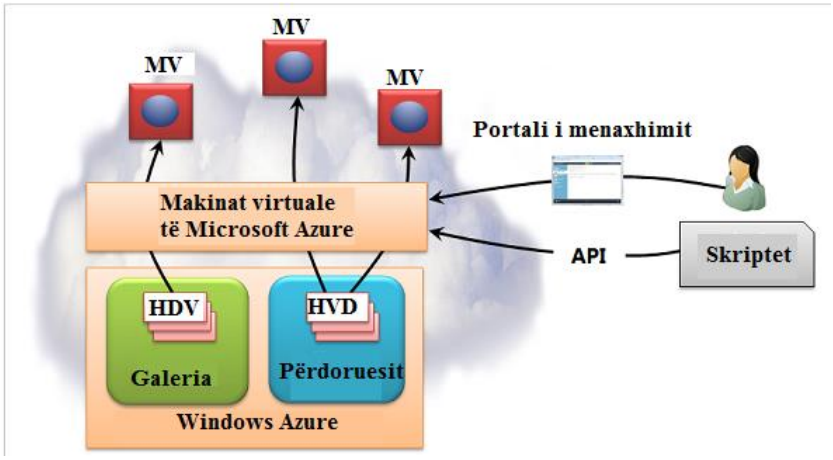
1.8.3. Shembuj platformash

1.8.3.1. Microsoft Azure

Microsoft Cloud Azure u ofron shërbimet e tij zhvilluesve, të tilla si: Stack NET (C #, VB.Net, ASP.NET). Përveç këtyre edhe Java & Ruby SDK për shërbimet .NET është gjithashtu në dispozicion.

Sistemi Azure përbëhet nga disa elemente. Kontrolluesi *Windows Azure Fabric Controller*, ofron përshkallëzim dhe besueshmëri duke menaxhuar burimet e kujtesës dhe balancimin e ngarkesës. *.NET Service Bus*, regjistron dhe lidh aplikimet së bashku. *.NET AccessControl* identifikon ofruesin, gjithashtu përfshin direktoritë dhe *Windows LiveID*. Së fundmi, *.NET Workflow* lejon ndërtimin dhe ekzekutimin e instancës.

Azure Virtual Machines u lejon zhvilluesve dhe personave të TI të krijojnë dhe të përdorin makinat virtuale në re. IaaS mund të përdoret në mënyra të ndryshme. Figura e mëposhtme tregon komponentët bazë.



Figurë 1.8 Azure Virtual Machines ofron IaaS

Një përdorues mund të krijojë makina virtuale duke përdorur ose portalin e menaxhimit, ose API dhe skriptet e vëna në dispozicion. Portali i menaxhimit mund të aksesohet nga shfletuesit popullorë të internetit si Explore, Mozilla dhe Chrome. Për të krijuar një makinë virtuale, një përdorues duhet të zgjedhë një hard disk virtual (HDV) nga imazhet e makinave virtuale, të cilat ruhen në Microsoft Azure. HDV-e ruhen në galerinë e imazheve dhe përfshijnë imazhe sistemesh shfrytëzimi si Windows ose Linux, por edhe imazhe platformash të tjera pasi kërkesa për sisteme të reja është gjithmonë e në rritje. Shembuj përfshijnë:

- Windows Server
- Linux servers si Suse, Ubuntu and CentOS
- SQL Server
- BizTalk Server
- SharePoint Server

Madhësitë e disqeve virtualë listohen në librarinë e Azure:

- Shumë i vogël, me procesor të ndarë dhe 768 MB memorie.
- I vogël, me 1 bërthamë dhe 1.75 GB memorie.
- Mesatar, me 2 bërthama dhe 3.5 GB memorie.
- I madh, me 4 bërthama dhe 7 GB memorie.
- Shumë i madh, me 8 bërthama dhe 14 GB memorie.
- A6, me 4 bërthama dhe 28 GB memorie.
- A7, me 8 bërthama dhe 56 GB memorie.

Azure Virtual Machines mund të përdoren në një varietet mundësish.

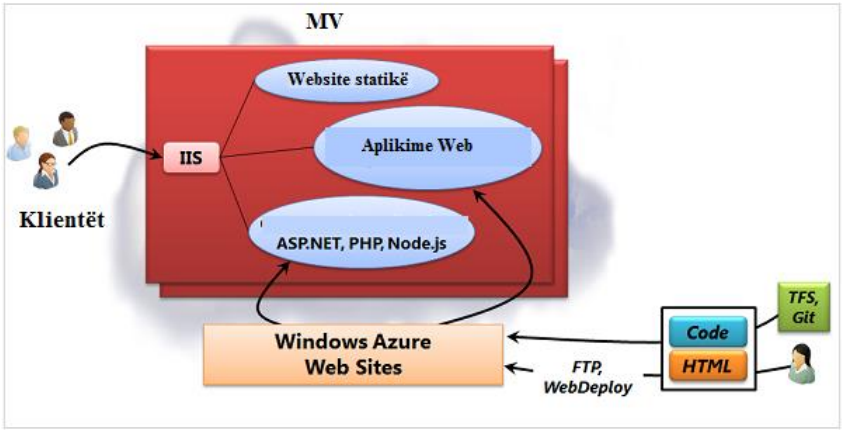
- MV për zhvillime dhe test.

- Ekzekutim aplikimesh në re. Mund të blihen makina virtuale për qendrat e të dhënave për të ekzekutuar aplikimet e një përdoruesi sipas nevojës, lëshimit dhe fshirjes së makinave kur ato nuk duhen më.
- Zgjerim i një qendre të dhënash në një re publike. Duke përdorur rrjetin virtual Azure, një kompani mund të krijojë një rrjet virtual, i cili jep idenë e një rrjeti, pjesë e rrjetit të kompanisë. Kjo lejon ekzekutimin e aplikimeve si SharePoint në Microsoft Azure, me avantazhin e një sistemi më pak të kushtueshëm dhe më lehtë të konfigurueshëm. Gjithashtu mund të ndërtohen baza të dhënash si Sql Server etj.
- Rikuperim ndaj fatkeqësive. Në vend që të paguhet për ruajtjen e kopjeve shtesë të të dhënave, rikuperimi IaaS i ofruar nga Azure, lejon të paguash për burime shtesë vetëm kur ato nevojiten dhe pa kosto shtesë tjetër.

Azure Websites

Duke përdorur PaaS, Azure bën të gjithë punën e MV-le që ekzekutojnë aplikimet e përdoruesve. Azure Websites është shërbim i plotë për ndërtimin e faqeve dhe aplikimeve web.

Në figurën e mëposhtme jepet struktura e Microsoft Azure Websites.

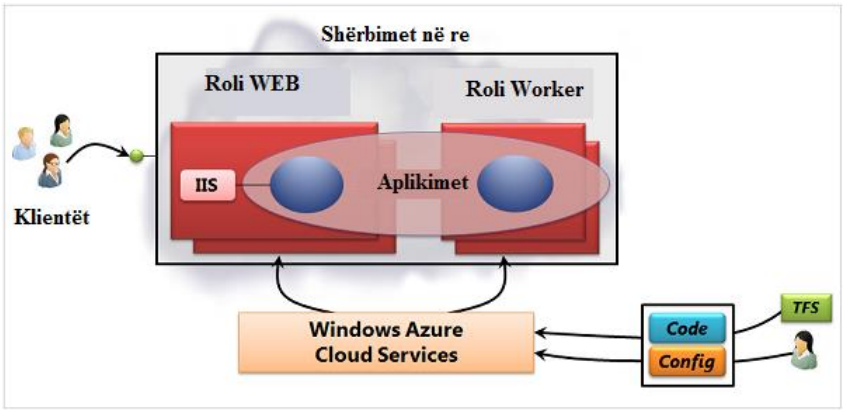


Figurë 1.9 Microsoft Azure Websites

Zhvilluesit mund të krijojnë aplikime të ndryshme duke përdorur teknologjitë ASP.Net, PHP, Node.js dhe Python. Aplikimet Web mund të përdorin aspekte të tjera të Azure si Service Bus, databazën SQL Server dhe Blob Storage.

Cloud Services

Komponenti i tretë, shërbimet në re, janë një tjetër shembull i PaaS. Teknologjia e ofruar është projektuar për t'u ardhur në ndihmë aplikimeve të përshkallëzuara, të besueshme dhe të lira në kosto operimi. Përdoruesit mund të instalojnë programet e tyre në makinat virtuale dhe mund t'i kontrollojnë ato kudo ku ato ndodhen. Figura e mëposhtme ilustron idenë e Azure:



Figurë 1.10 Azure Cloud Services ofron Platformë si një Shërbim

Teknologjia e Azure ofron dy opsione të ndryshme: rolin web në të cilin ekzekutohet një variant i një serveri Windows me IIS, kurse instanca worker mban të njëjtin version Windows por pa IIS. Një aplikim mbështetet në një kombinim të këtyre dy opsioneve. P.sh një aplikim i thjeshtë mund të përdorë rolin web, kurse një më kompleks mund të përdorë rolin web për të menaxhuar kërkesat e përdoruesve dhe më pas t'ia kalojë kërkesat një roli worker për përpunim.

Siç sugjeron edhe figura e mësipërme, të gjitha MV-le pjesë e një aplikimi të vetëm, ekzekutohen nën të njëjtin shërbim të resë, e për shkak të kësaj, përdoruesit aksesojnë aplikimet nëpërmjet një adrese IP të vetme, me kërkesa të balancuara automatikisht midis aplikimeve të makinave virtuale. Platforma do t'i ndërtojë makinat virtuale në atë mënyrë që të evitojë ndërprerjet e shërbimeve të ofruara nga aplikimet në rast fatkeqësie. Balancimi i ngarkesës së aplikimit dhe ndarja nga makinat virtuale e bën Azure Cloud Services një ofrues platformash si një shërbim dhe jo ofrues të infrastrukturës si një shërbim.

1.8.3.2. Force.com

Në bashkëveprim me shërbimin Salesforce.com, PaaS lejon zhvilluesit që të krijojnë funksionalitete të cilat i integrojnë në aplikacionin *Salesforce CRM SaaS*. Force.com u ofron gjithashtu zhvilluesve dy mundësi të cilat mund t'i përdorim në platformën e saj SaaS:

- Pritësi *Apex* ose aplikacioni *Visualforce*. Apex ngjan me gjuhën Java dhe përdoret për të krijuar apikimet SalesForce.
  Visualforce është një sintaksë e ngjashme me XML dhe përdoret për ndërtimin e ndërfaqeve të përdoruesve në HTML, AJAX apo në FLEX, për të menaxhuar në SalesForce sistemet CRM.
- Një aplikacion tjetër i përfshirë në platformë është *AppExchange*, i cili në direktorinë e tij ofron programe falas për shitje.

1.9. Retë publike dhe infrastruktura e shërbimit

Retë publike ose retë e jashtme i përshkruajnë retë kompjuterike në kuptimin tradicional, ku burimet janë të aksesueshme me anë të aplikacioneve të internetit dhe ku shërbimet sigurohen nga një ofrues, i cili ndan burimet dhe faturon klientët për

shërbimet kompjuterike bazë. Përdoruesit paguajnë vetëm për kapacitetin e burimeve të siguruara në një kohë të caktuar.

Ka mjaft shembuj të shitësve që në mënyrë publike ofrojnë infrastrukturën si një shërbim. Amazon Elastic Compute Cloud (EC2), por tregu tashmë prej kohësh lulëzon nga shumë kompetitorë të tjerë si GoGrid, Joyent Accelerator, Rackspace, AppNexus, FlexiScale, Manjrasoft Aneka etj.

Amazon Elastic Compute Cloud (EC2) është një shërbim që ofron kapacitete llogaritëse elastike IaaS në re. Këto shërbime mund të ngrihen nëpërmjet shërbime Web (SOAP apo REST) dhe të administrohen me *Amazon Web Service* (AWS), ose *elastic command line* (EC2). Ky shërbim siguron qindra instanca Amazon të instaluara më parë, AMI (Amazon Machine Images) me një shumëllojshmëri të sistemeve të operimit (p.sh. Linux, OpenSolaris, ose Windows) dhe programe të ngarkuara më parë. Kjo u siguron përdoruesve një kontroll të plotë të burimeve informatike dhe lejon të punohet në mjedisin dhe infrastrukturën e Amazon lehtësisht. Amazon EC2 zvogëlon kohën e nevojshme për krijimin dhe vënien në punë të serverit të ri për pak minuta, duke lejuar një kapacitet të shpejtë dhe të shkallëzuar të burimeve, lart e poshtë, siç janë kërkesat e tij.

Amazon ofron disa lloje instancash në varësi të madhësisë sipas:

a) burimeve (të vogla, të mëdha, dhe shumë të mëdha)
b) nevojave të CPU (të mesëm dhe shumë të lartë)
c) madhësisë së kujtesës (shumë e madhe, dy herë më e madhe dhe e katërfishtë, por edhe më shumë).

1.10. Retë private, hibride dhe infrastruktura e shërbimit

Një re private ka për qëllim funksionimin publik të resë, por me burime private duke mbajtur nën kontroll të dhënat e një organizate dhe burimet për të përmbushur kërkesat e sigurisë dhe të privatësisë. Retë private ekspozojnë një qendër të dhënash shumë të virtualizuar e cila është e vendosur brenda firewall-it të organizatës. Një re private mund të përmbajë një hapësirë private të dedikuar për kompaninë brenda qendrës së të dhënave të një reje, e projektuar vetëm për të trajtuar ngarkesat e punës së kompanisë.

Retë private shfaqin karakteristikat e mëposhtme:

- Lejojnë shërbime dhe llogaritje për përdoruesit e një organizate kryesisht me vetë-shërbim.
- Optimizojnë burimet informatike dhe përdorimin e serverave.
- Mbajnë ngarkesa të ndryshme të dhënash.
- Automatizojnë dhe sigurojnë një menaxhim dhe kontroll të mjediseve të virtualizuara.

Disa shembuj resh private janë Eucalyptus dhe OpenNebula.

Është gjithashtu e rëndësishme të nënvizohet edhe tipi i tretë i reve, i cili quhet ‘re hibride’, e cila është një kombinim i burimeve të reve private të brendshme me ato

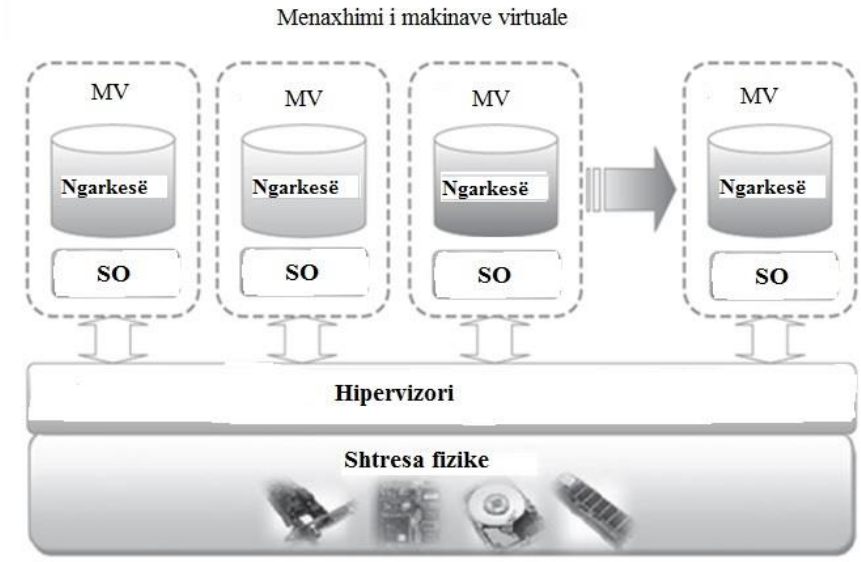
publike të jashtme që ekzistojnë së bashku, duke mundësuar dhënien e shërbimeve dhe funksioneve jokritike në renë publike dhe mbajtjen e atyre kritike në renë e brendshme.

1.11. Përmbledhje e teknologjisë virtuale

Virtualizimi ka revolucionarizuar teknologjitë e qendrës së të dhënave nëpërmjet disa teknikave që sigurojnë dhe menaxhojnë infrastrukturën dinamike të qendrës të të dhënave.

Virtualizimi mund të përcaktohet si pjesë përbërëse e burimeve informatike; ruajtja e informacionit, përpunimi i informacionit, memoria, rrjetet dhe I/O. Ky është një koncept i ngjashëm me rivalitetin, ku një sistem pretendon të jetë një sistem tjetër, ndërsa virtualizimi është një sistem i pretenduar të jetë dy ose më shumë sisteme brenda të njëjtit sistem.

Në figurën e mëposhtme, shtresa virtuale do të ndajë burimet fizike të shtresës fizike në makina virtuale të shumta me ngarkesa të ndryshme pune. Virtualizimi planifikon, shpërndan burimet fizike dhe bën që çdo makinë virtuale të „mendojë“ se është vetëm ajo zotëruese e burimeve HW.



Figurë 1.11 Koncepti i virtualizimit

Teknologjia e makinave virtuale i bën ato mjaft elastike dhe lehtësisht të menaxhueshme në mjediset e reve kompjuterike, sepse ato përmirësojnë përdorimin e disa burimeve duke krijuar shumë makina virtuale në një ambient fizik të vetëm. Këto makina virtuale mund të shkallëzohen sipas nevojave.

Përgatitja e një makine virtuale mund të shpjegohet e ilustruar në figurën e mëposhtme. Hapat e krijimit të MV janë:

- Së pari, duhet përzgjedhur një server nga një gamë e gjerë serverash që ofron tregu i serverave fizikë. Serveri duhet të jetë me kapacitete të mjaftueshme

dhe me sistemet e nevojshme të shfrytëzimit që nevojiten për të përgatitur makinën virtuale.
- Duhet të instalohen programet përkatëse që kërkojnë shërbimet e kërkuara për të qenë funksionale.
- Serveri është gati të nisë punën.

Zakonisht këto janë hapat që një TI ose një specialist i qendrës së të dhënave duhet të ndjekë për të përgatitur një makine virtuale. Pra, përgatitja e një serveri përcaktohet nga kërkesat e organizatës apo kompanisë, në komponentët hardware apo software të tij si : procesori, RAM, HDD, rrjeti , sistemi i shfrytëzimit, aplikacionet etj.

Normalisht, makinat virtuale mund të përgatiten manualisht duke instaluar një OS, i cili është i përgatitur më parë me një shabllon MV, nga klonimi i një MV ekzistuese, apo nga konvertimi që i bëhet një serveri fizik ose një platformë hostimi. Serverat fizikë mund të virtualizohen dhe materializohen duke përdorur mënyra dhe teknika nga fizike në virtuale (P2V).

Pasi krijohet një makinë virtuale nga virtualizimi i një serveri fizik, ose nga ndërtimi i një serveri virtual, ky shabllon mund të ruhet për t'u përdorur më vonë.

Shumica e kompanive që menaxhojnë teknikat e virtualizimit si p.sh VMware, XenServer, etj., mundësojnë administrimin e një qendre të dhënash si dhe japin mundësi që kjo gjë të bëhet në mënyrën më të lehtë të mundshme për administratorët.

Kryerja e një procesi të tillë nga një shabllon ka vlera të shumta, sepse kursen kohën që i duhet një makine virtuale për t'u krijuar nga fillimi. Administratorët e TI mund të krijojnë shabllone të ndryshme për qëllime të ndryshme. Për shembull, mund të krijojnë një shabllon të Windows Server 2003 për departamentin e shitjeve, ose një shabllon Red Hat Linux për departamentin e inxhinierisë. Kjo i lejon administratorit që, në mënyrë të shpejtë të përgatisë sipas kërkesave një server virtual funksional.

Kjo lehtësi dhe fleksibilitet sjellin me vete edhe ndryshimet e mëdha që janë shfaqur së fundmi, ku makinat virtuale janë materializuar kaq shpejt dhe se dokumentimi e menaxhimi i tyre është bërë një sfidë më vete.

Virtualizimi mundëson mekanizma të lartë, të besueshëm, të shpejtë për vendosjen dhe menaxhimin e shërbimeve, duke mundësuar sipas nevojës klonimin dhe migrimin në kohë të shërbimeve, që përmirësojnë dukshëm besueshmërinë. Gjithsesi duhet pasur një paketë menaxhimi efektive për të kontrolluar infrastrukturën e makinave virtuale, pasi është kritike për çdo infrastrukturë në renë kompjuterike, kontrolli i shërbimeve që ofrohen.

1.12. Përmbledhje dhe konkluzione

Retë kompjuterike janë një model i ri kompjuterik që ofron mundësi të mëdha llogaritjesh dhe burime të konsiderueshme për ruajtjen e të dhënave. Individët, p.sh shkencëtarët dhe ndërmarrjet e ndryshme, mund të kenë akses në këto burime duke paguar një shumë të vogël parash, për vetëm atë që vërtet u nevojitet, as më shumë e as më pak. Këto më sipër janë një përmbledhje e shumë teknologjive që kanë çuar në krijimin e resë, duke arritur në përfundimin se ky model i ri është rezultat i një evolucioni dhe jo revolucioni.

Retë kompjuterike janë një fushë kërkimore në zhvillim që bazohet në teknologji të ndryshme, të tilla si arkitektura e orientuar drejt shërbimit (SOA), rrjetet kompjuterike dhe teknologjia virtuale. Retë ofrojnë infrastrukturën si një shërbim që është e bazuar në ‘paguaj aq sa përdor’ dhe sipas kërkesës së modelit të zgjedhur nga përdoruesi. Ky shërbim është quajtur Infrastruktura si një Shërbim (IaaS).

Në forma të ndryshme, retë synojnë të ofrojnë shërbimet e llogaritjeve, ruajtjes, rrjetit, programeve ose një kombinim të tyre, të gjitha këto "si një shërbim". Infrastruktura, platforma dhe programet ‘si një shërbim’, janë tri nomenklaturat më të zakonshme për nivelet e abstraksionit të shërbimeve kompjuterike të reve.

Me daljen e teknologjisë virtuale dhe me modelin e reve kompjuterike IaaS, është çështje minutash kryerja e të njëjtave detyra nga administratori i teknologjisë së informacionit, si p.sh për instalimin e një serveri. Gjithçka që duhet është sigurimi i një serveri virtual përmes një ndërfaqeje vetëshërbimi me disa hapa, për të kryer specifikimet e nevojshme të kërkuara. Ky skenar është një shembull i mirë për të ilustruar vlerat e virtualizimit dhe rrugën sesi makinat virtuale krijohen. E njëjta gjë mund të përshkruhet edhe për shërbimet e migrimit. Sa herë që nevojitet të bëhet një përditësim i serverave apo të caktohet detyra për kryerjen e mirëmbajtjes së tij, duhet shumë kohë dhe përpjekje për ta arritur këtë sepse operacionet janë të kushtueshme ngaqë kanë në brendësi të tyre shumë aplikime dhe përdorues. Tani, me revolucionarizimin e teknologjisë së virtualizimit dhe shërbimeve të migrimit të sistemit, bashkuar me kapacitetet e hipervizorit, mirëmbajtja, përditësimi, janë shumë të kollajshme dhe duhet një kohë relativisht e vogël për t‘i përmbushur.

Krijimi i një makine virtuale të re është çështje minutash, për të fituar shumë kohë dhe përpjekje. Migrimi në një makine virtuale është çështje milisekondash duke fituar kohë, përpjekje dhe duke i kthyer shërbimet në kohë reale për klientët e ndryshëm. Marrëveshjet SLA konsiderohen të përmbushura dhe cilësia e garantuar.

Sigurimi dhe migrimi i makinave virtuale është një proces kritik në sistemet e virtualizuara të sotme, në teknologjinë e qendrave të të dhënave dhe në përputhje me rrethanat e shërbimet të reve kompjuterike. Ato kanë një impakt të rëndësishëm në vazhdimësinë dhe disponueshmërinë e një biznesi. Në disa minuta mundet të përgatitet një server me të gjitha zbatimet e tij, për të mundësuar funksionalitetin, apo për të ofruar shërbimin.

Megjithatë siç u diskutua në këtë kapitull, sfidat dhe rreziqet e shumta duhet të zgjidhen për të garantuar suksesin afatgjatë të reve. Tendencat të dukshme në këtë sferë përfshijnë krijimin e standardeve, krijimin e vlerave, rritjen dhe shtimin e shërbimeve. Në këtë kuptim, ekzistojnë realisht mundësi të shumta për praktikuesit për të kërkuar zgjidhje të reja për retë kompjuterike.

2. Arkitektura të reve kompjuterike

2.1. Hyrje

Ndërkohë që reja kompjuterike ka shumë premisa për të gjitha ndërmarrjet e reja që kërkojnë zgjidhje informatike, ajo në të njëjtën kohë ka edhe një numër mangësish të natyrshme të tilla si:

- Përshkallëzim i kufizuar për rastin e një reje si ofrues i vetëm. Edhe pse shumica e ofruesve të ndryshëm të reve kompjuterike pretendon se ka një përshkallëzim infinit, në realitet është më se e arsyeshme të supozohet se me rritjen e raportit të shfrytëzimit të resë, ofruesit më të mëdhenj mund të fillojnë të përballen me problemet e përshkallëzimit. Në një kohë më të gjatë, problemi i përshkallëzimit mund të pritet që të përkeqësohet, pasi ofruesit shërbejnë një numër gjithnjë e në rritje të shërbimeve online, ku secili prej tyre aksesohet nga një numër i madh përdoruesish globalë në çdo kohë.
- Mungesa e ndërveprimit ndërmjet ofruesve të reve. Teknologjitë bashkëkohore të reve, kur janë projektuar, nuk kanë pasur në mendje ndërveprimin midis tyre. Kjo gjë parandalon infrastrukturën e reve të ofruesve të vegjël e të mëdhenj të hyjnë në tregun e sigurimit të reve. Në përgjithësi, kjo e „mbyt“ konkurrencën dhe i detyron konsumatorët drejt një shitësi të vetëm, pra drejt një monopoli.

Menaxhimi i shërbimeve të biznesit (MSB), është një strategji menaxhimi që i lejon bizneset të lidhin menaxhimin e TI së tyre me nivelet e larta të biznesit të tyre. Aspekt kyç i MSB është menaxhimi i marrëveshjes së SLA-ve. Zgjidhjet aktuale të reve informatike nuk janë të projektuara për të mbështetur praktikat e MSB. Si rezultat, ndërmarrjet kërkojnë transformimin e operacioneve të TI në teknologjitë e bazuara të retë duke u përballur me një hap jo shumë të madh dhe mundësisht përçarës.

Për të adresuar këto çështje, po paraqitet një model për ofruesit e reve informatike, ku çdo ofrues mund të blejë dhe të shesë nga të tjerët, sipas kërkesës dhe mundësive. Po analizohen kërkesat e një oferte për një ndërmarrje të „keqe“ të reve dhe identifikohen komponentët kryesore funksionale që duhen të jenë pjesë e kësaj afere. Përveç kësaj, duke u nisur nga kërkesat bazë zhvillohen parimet themelore për të cilat, besohet se janë guri i themelit për ofertat e reve informatike në të ardhmen.

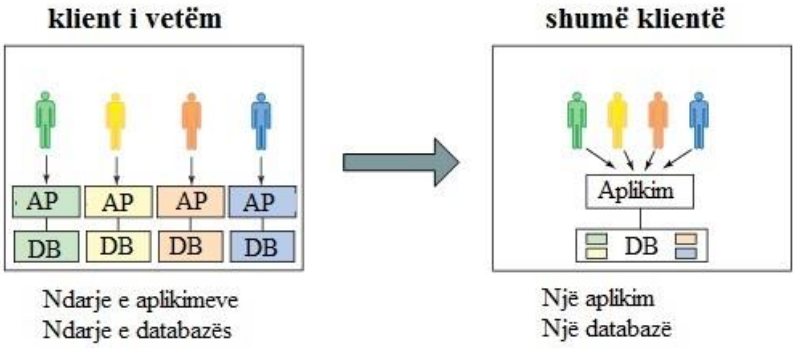
2.2. Arkitektura me një ose shumë instanca

Në një arkitekturë me shumë qiraxhinj, të dhënat nga kompani të ndryshme ruhen në të njëjtin server, zakonisht të ndara në particione për të parandaluar informacionet të përzihen nga njëra kompani në tjetrën. Meqë të gjitha aplikimet janë të vendosura në të njëjtin server, duhet të ekzistojë një standard në arkitekturën SaaS që përfshin të njëjtat konfigurime të klientëve ndaj burimeve fizike, rrjetit dhe sistemit të shfrytëzimit.

Meqë klientët ekzekutojnë programe e tyre në një instancë të vetme dhe të dhënat ruhen në një databazë të përbashkët, klientët kanë mundësi shumë të kufizuara për të bërë ndryshime në funksionet e programeve të tyre. Në këtë mënyrë një zgjidhje në

arkitekturën me një instancë të vetme është e përshtatshme për kompanitë me pak ose aspak ndryshime dhe rikonfigurime në aplikacionet e tyre. Megjithatë kjo do të varet dhe nga shkalla e lirisë për arkitekturën me një instancë të vetme që ofrohen nga retë kompjuterike.

Shumë nga ofruesit e SaaS ofrojnë versione të standardizuara që plotësojnë shumicën e nevojave të klientëve të tyre. Një aplikim i përbashkët i ndarë në shumë klientë, ndërtohet për një grup të zgjedhur klientësh dhe ofron versione aplikimesh zakonisht në versionet beta për qëllime testimi.



Figurë 2.1 Arkitekturat me një dhe shumë instanca

Shkalla ekzakte e modelit me shumë klientë, bazohet në atë se sa shumë pjesë të aplikimit bazë, ose të shtresave të SaaS janë të projektuara të ndahen midis klientëve. Një shkallë më e lartë lejon skemat e bazave të të dhënave të ndahen midis klientëve, gjithashtu ofron më shumë ndryshime dhe konfigurime në ndërfaqet e përdoruesve, llogjikën e biznesit dhe rrjedhën e informacionit. Të gjitha shtresat e SaaS ofrojnë arkitekturë me një instancë të vetme me shkallë të lartë [29].

Në shkallët më të ulëta, arkitekturat me shumë instanca janë të kufizuara tek shtresat e IaaS dhe PaaS dhe me shtresa SaaS të dedikuara për çdo klient.

Grupe homogjene klientësh ndajnë të njëjtat skema databazash dhe aplikimesh. Kjo njihet si shkalla e mesme dhe në këtë shtresë çdo grup klientësh ka version e vet të bazës së të dhënave dhe të aplikimeve.

Arkitektura SaaS me një klient të vetëm, e quajtur gjithashtu me shumë instanca, i ofron një klienti të resë një instancë të vetme. Kjo arkitekturë përdoret nga kompanitë që kanë nevojë për një shërbim të veçantë, për shkak të shpërndarjes gjeografike të klientëve të tyre, ose kërkojnë nivele të larta sigurie për aplikimet e tyre. Një këtë arkitekturë, çdo kompani ka një databazë dhe sistem të veçantë të vendosur ose një server të veçantë, ose në të njëjtin server por me protokolle shtesë sigurie duke krijuar idenë e një rrjeti dhe të një serveri virtual.

Tabelë 2.1 Shkallët e instancave dhe arkitekturat e reve

Shkallë e lartë	Shkallë e mesme	Shkallë e ulët
IaaS dhe PaaS janë arkitektura me shumë klientë. SaaS është gjithashtu plotësisht me shumë klientë.	IaaS dhe PaaS janë arkitektura me shumë klientë. Grupe të vogla SaaS janë me shumë klientë.	IaaS dhe PaaS janë arkitektura me shumë klientë. SaaS është me klient të vetëm.

Në ambientet SaaS me shumë instanca, çdo klient blen kopjen e vet të aplikimit, të cilin e ndryshon dhe e përshtat sipas nevojave. Edhe pse programi bazë i ofruesit të SaaS shërben si aplikimi final, përdoruesit kanë mundësi të bëjnë konfigurime; p.sh përdoruesit mund të shtojnë opsione në modulet e ndryshme të aplikimeve duke ndryshuar konfigurimet në bazat e brendshme të të dhënave si edhe në databazat e jashtme të kompanive partnere [30].

Si shembull po merret Salesforce.com, e cila ndodhet në spektrin më të lartë të arkitekturës me shumë klientë dhe ka 72500 klientë të cilëve u shërbejnë 8 deri 12 instanca IaaS/PaaS në raportet 1 me 5000. Me fjalë të tjera, çdo instancë u shërben 5000 klientëve që ndajnë të njëjtën skemë të bazës së të dhënave. Një sistem SaaS financiar në spektrin mesatar të arkitekturës, ka më shumë se 2500 klientë, të cilët ndajnë 10 instanca në raportin 1 me 250.

2.2.1. Zgjedhja e shkallës me shumë klientë

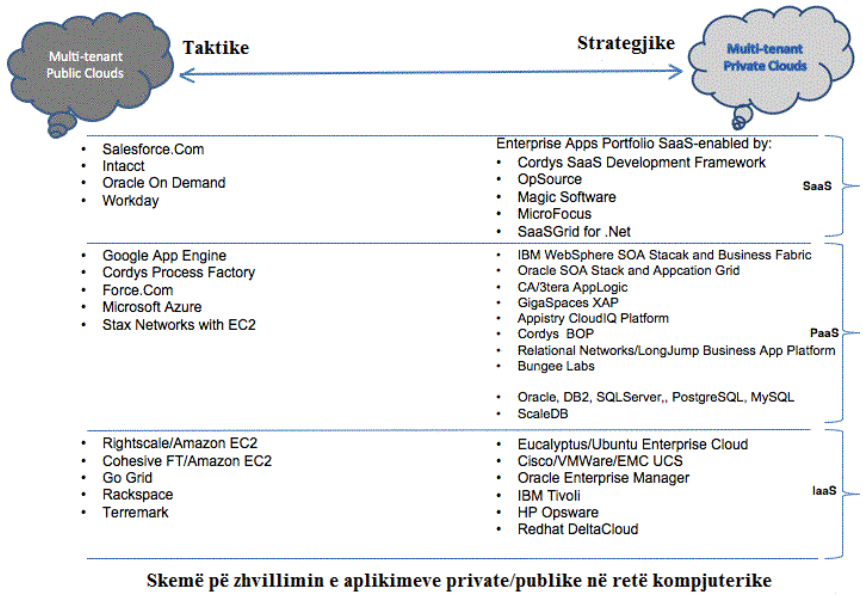
Vetëm një arkitekturë dhe një model nuk i kënaq të gjithë konsumatorët. Ambientet me shumë klientë ofrojnë nivele të kënaqshme sigurie për shumicën e përdoruesve, kurse zgjedhjet me shumë instanca mund të ofrojnë nivele sigurie shumë të larta sepse përzierja e të dhënave të klientëve të ndryshëm eliminohet. Për këtë shkak, arkitektura me klient të dedikuar është më e preferuara, ku siguria e të dhënave është një kërkesë ligjore dhe kompanitë duhet të plotësojnë protokolle specifike qeveritare të sigurisë.

Fushat që përdorin arkitekturën e dedikuar përfshijnë atë prodhuese, shitjet me pakicë, shërbimet profesionale; si financiare, farmaceutike, aeronautike dhe industritë teknologjike.

Asnjëra nga arkitekturat nuk është më e mirë se tjetra, secila ka ndryshime dhe avantazhe karakteristike që varen nga faktorë si vendndodhja gjeografike, lloji i industrisë, kërkesat e sigurisë, mundësitë e teknologjisë së informacionit etj.

Aplikime në retë kompjuterike lehtësisht mund të përdorin të njëjtën skemë të bazës së të dhënave dhe të përfitojnë nga një bashkësi opsionesh dhe programesh të cilat janë zhvilluar nga ofruesit e shërbimeve në re. Aplikimet e ofruara kanë tendencën të kenë kërkesa më të thjeshta ndaj sigurisë; si shifrimi apo autorizimi, prandaj retë publike janë më tërheqëse në platformat me instancë të vetme dhe me ngarkesë pune si email, chat, raporte shpenzimesh, trajnime punonjësish etj.

Sipas ngarkesës së të dhënave në re, menaxherëve të TI u duhet të përcaktojnë shkallën e lirisë për arkitekturën e tyre dhe të zgjedhin nga një listë ofruesish shërbimesh. Për ngarkesat që u përkasin reve private dhe atyre të një komuniteti të veçantë, përgjegjësia për projektimin e arkitekturave me shumë klientë bie mbi menaxherët e TI, të cilët duhet të vlerësojnë ofruesit e shërbimeve dhe të ndërtojnë shtresa të veçanta të Iaas, PaaS dhe SaaS duke siguruar një ambient për të ndërtuar shërbime dhe databaza të ndara.



Figurë 2.2 Një skemë për zgjedhjen e arkitekturës me një ose disa instanca

2.2.2. Skema e pagesës për Microsoft Azure

Shërbimet në re mundësojnë ekzekutimin e kodeve të përdoruesit me anë të krijimit të roleve „web“ dhe „worker“, ku e gjithë puna për ngritjen e sistemit bëhet nga Azure. Çdo instancë logjikisht izolohet nga të gjithë klientët e tjerë. Klientët mund të zgjedhin midis 5 instancave; e vogël, e vogël mesatare, mesatare, e madhe dhe shumë e madhe. Klientët faturohen për instancë në bazë të konsumit për orë.

Më poshtë jepen skemat e llogaritjes së pagesës për shërbimet e ofruara nga Microsoft Azure.

Faqet web

Mund të ekzekutohen 10 website për një rajon të caktuar në një ambient me shumë klientë. Për një bandwith prej 100GB, paguhet një çmim prej 11.64$ për muaj. Nëse kërkohet diçka më e dedikuar si p.sh një shpërndarje e ngarkesës në 3 instanca dhe një makinë virtuale të dedikuar me procesor 1.6 GHz dhe memorie 1.75 GB RAM, atëherë duhet paguar edhe një çmim prej 0.075$ për orë, duke rezultuar në një total prej 67.44$ në muaj. Tri instancat duhet të zgjidhen në mënyrë manuale nga përdoruesi. Një skemë më e mirë e ofruar nga Azure, është ajo me 10 instanca të dedikuara me shpërndarje automatike të ngarkesës nga vetë sistemi, por me një çmim pak sa më të „kripur“ prej 0.1$ për orë.

Makinat virtuale Windows

Shtresa standarde e instancave siguron një ambient llogaritës, memorie dhe burime hyrje/dalje për të ekzekutuar një gamë të madhe aplikimesh. Këto instanca përfshijnë si përshkallëzimin automatik ashtu edhe një shpërndarje të balancuar të ngarkesave.

Microsoft Azure ofron tipet D, A, G të makinave virtuale me parametra dhe çmime si më poshtë:

- Seria D, 1 bërthamë, 3.5 GB RAM, 50 GB disku i ngurtë, me çmim 0.159$ për orë.
- Seria A, 1 bërthamë, 768 MB, 20 GB disku i ngurtë, me çmim 0.02$ për orë.
- Seria G, 2 bërthama, 28 GB, 384 GB disku i ngurtë, me çmim 0.67$ për orë.

Makinat virtuale Linux

- Seria D, 1 bërthamë, 3.5 GB RAM, 50 GB disku i ngurtë, me çmim 0.085$ për orë.
- Seria A, 1 bërthamë, 768 MB, 20 GB disku i ngurtë, me çmim 0.02$ për orë.
- Seria G, 2 bërthama, 28 GB, 384 GB disku i ngurtë, me çmim 0.61$ për orë.

Sql Server

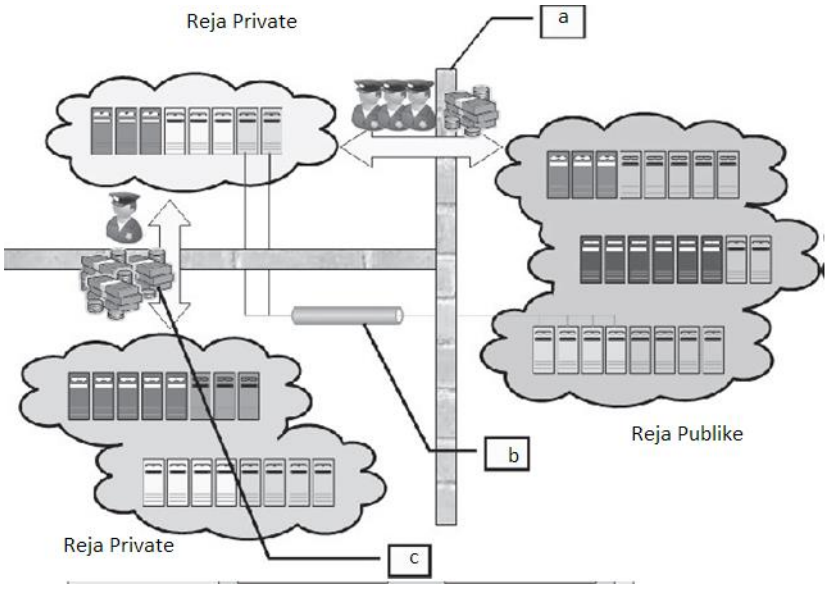
- Sql Server Web, seria D me çmim 0.191$ për orë dhe seria A me çmim 0.052$ për orë.
- Sql Server Standard, seria D me çmim 0.191$ për orë dhe seria A me çmim 0.42$ për orë.
- Sql Server Enterprise seria D me çmim 1.659$ për orë, dhe seria A me me çmim 1.52$ për orë.

Oracle

- A0 (1 GHz CPU, 768 MB RAM), Java SE me çmim 0.1$ për orë.
- A0 (1 GHz CPU, 768 MB RAM), Oracle Weblogic Server (SE) me çmim 0.52$ për orë.
- A0 (1 GHz CPU, 768 MB RAM), Oracle Weblogic Server (EE) me çmim 1.3$ për orë.
- A0 (1 GHz CPU, 768 MB RAM), Oracle Database (SE) me çmim 1.13$ për orë.
- A0 (1 GHz CPU, 768 MB RAM), Oracle Database (SE) me çmim 3.18$ për orë.

2.3. Një përdorim tipik

Si përfaqësues të një aplikimi enterprise-grade është zgjedhur për t‘u analizuar sistemi SAP. Prej tij do të zgjidhen kërkesat e përgjithshme që ky aplikim mund të ketë, siç tregohet në figurën e mëposhtme.



Figurë 2.3 Një përdorim tipik i reve

Modeli për renë informatike

a. Retë e ndryshme bashkëveprojnë duke shkëmbyer burimet e tyre e duke krijuar një shtresë të lartë izolimi midis tyre, ku secili në vetvete është një entitet i pavarur autonom.

b. Aplikimet që veprojnë në këtë re, duhet të jenë në dijeni të vendndodhjes, që do të thotë se rrjetet virtuale lokale janë të nevojshme për komunikimin e të gjitha komponentëve të aplikimit me njëri-tjetrin.
c. Ofruesit e reve dallojnë nga njëri-tjetri për sa u përket kostos dhe nivelit të sigurisë, për shembull, ndërkohë që një re publike mund të jetë e „lirë“, kompanitë do të ngurrojnë për të përdorur këto shërbime që kërkojnë një nivel të lartë sigurie.

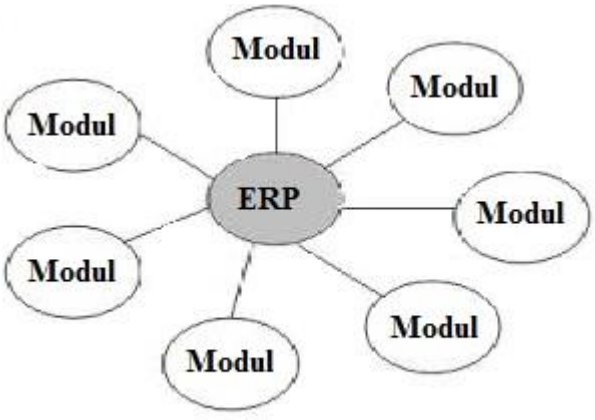
2.4. Sistemet SAP

Një sistem ERP (Entreprise Resource Planning), është një bashkësi programesh të projektuara për të lehtësuar rrjedhën e informacionit midis departamenteve ose funksioneve të një biznesi. Një sistem ERP i projektuar mirë është i aftë të procesojë informacione nga çdo pjesë e një organizate dhe çdo lloj transaksioni me një zgjidhje të vetme duke u siguruar një informacion të saktë dhe në kohë reale klientëve të biznesit.

Më poshtë jepet një përmbledhje e fushave kryesore të biznesit të aplikuara në një sistemi ERP.

Bilanc, libër arke, journal, raporte financiare, menaxhimi i llogarive, rikoncilim bankar, menaxhimi i fondeve dhe parashikime të ndryshme, investime monetare, parashikim buxheti, blerje, shitje, magazinim, hyrje, dalje, kosto, inventar, asemblim produktesh, import, eksport të mirash materiale, kosto totale të produkteve, menaxhim punonjësish, llogaritje pagash, llogaritje ditësh lejeje etj.

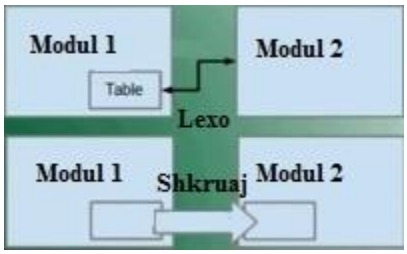
ERP ka natyrë modulare dhe është i përbërë nga disa aplikime, por të gjitha aplikimet janë të lidhur me njëri-tjetrin. Çdo modul është i fokusuar në një fushë të caktuar të biznesit, p.sh një ERP i një kompanie do të ketë një modul për të menaxhuar financat, një modul tjetër për menaxhimin e burimeve njerëzore e kështu me radhë.



Figurë 2.4 ERP me module

Module të integruara në një sistem ERP nënkuptojnë:

- Një modul mund të ndajë me një modul tjetër informacione si p.sh listën e furnitorëve.
- Informacioni nga një modul transmetohet në një modul tjetër, si p.sh një llogari bankare etj.

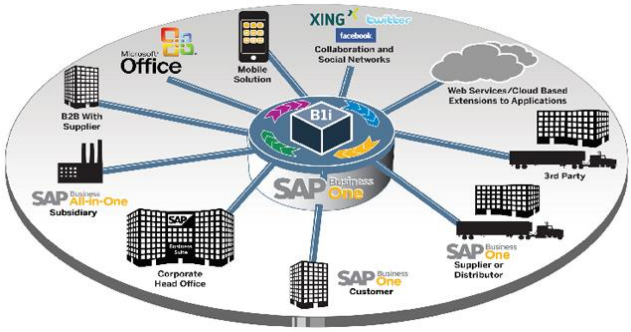


Figurë 2.5 Operacionet lexo dhe shkruaj në modulet ERP

Në figurën e mësipërme, moduli 2 nuk mban kopjet e veta të dhënave, por lexon vazhdimisht informacionet nga moduli 1 duke parandaluar kështu dublim të rekordeve.

SAP është akronim i Systems Applications and Products in Data Processing. Projektuar dhe zhvilluar nga pesë inxhinierë të IBM gjatë viteve 1970, si një alternativë ndaj programeve ERP, SAP ka marrë një zhvillim shumë të madh. Sistemet SAP janë tashmë në krye të listës për sa u përket sistemeve ERP.

SAP zhvillon produkte EPR për t'u përdorur nga kompanitë në menaxhimin e korporatave dhe bizneseve. Megjithëse ka ofrues të ndryshëm dhe të shumtë ERP, faktori kyç që i dallon është mënyra se si SAP integron të gjitha operacionet e fushave të ndryshme të biznesit.

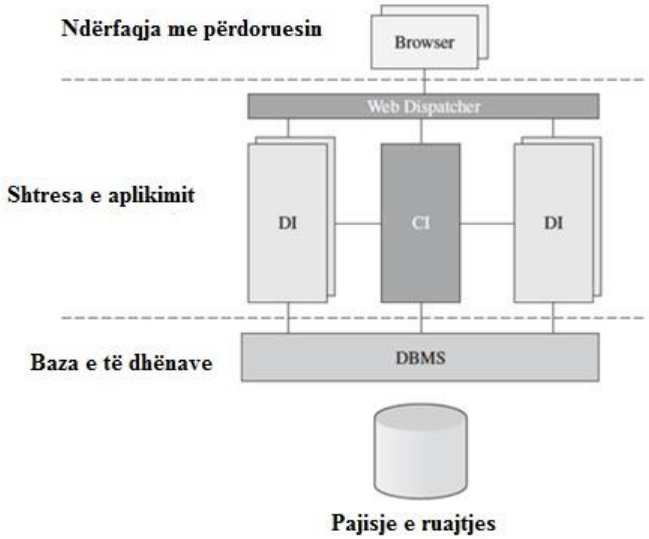


Figurë 2.6 Sistemet SAP

Sistemet SAP përdoren nga numër i ndryshëm aplikimesh biznesi që ndryshojnë nga njëri-tjetri si nga versioni ashtu dhe nga funksionalitetet si p.sh CRM, ERP. Për një tip aplikimi të dhënë, komponentët e sistemi SAP konsistojnë në pjesët e përgjithshme të përshtatura nga konfigurimi dhe pjesët e veçanta të përshtatura për një konfigurim të veçantë. Aplikimet SAP përbëhen nga disa sisteme që bashkëveprojnë me njëri-tjetrin.

Këto sisteme kanë baza të dhënash të pavarura nga njëri-tjetri dhe komunikojnë midis tyre me anë të mesazheve. Një sistem SAP është tipik i sistemeve të përbërë nga tri shtresa si më poshtë:

- Kërkesat merren nga dispatcher web i SAP. Kjo është edhe shtresa e parë, e cila bën të mundur marrjen e komandave të përdoruesve.
- Shtresa e mesme përbëhet nga dy komponentë:
  Instancat dialoguese (DI), instanca qendrore (CI) e cila kryen shërbime qendrore si kyçje në nivel qendror, mesazhet, si edhe regjistrimin e DI.
  Numri i instancave dialoguese ndryshon në varësi të përdorimit të sistemit nga përdoruesit.
- Një sistem i vetëm i menaxhimit të databazës (DBMS) përdoret nga sistemi SAP.

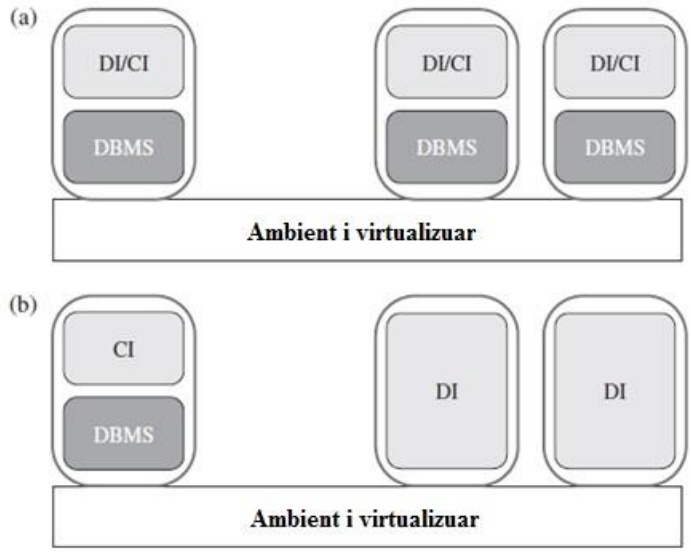


Figurë 2.7 Abstragimet e sistemeve SAP

2.5. Qendra e të dhënave të virtualizuara

Shqyrtohet rasti në të cilin qendra e të dhënave që bashkon operacione të ndryshme të aplikacioneve të SAP-it dhe të gjitha këto mjedise si p.sh, testimi, prodhimi, përdorin teknologjinë e virtualizimit. Aplikacioni u është ofruar si një shërbim klientëve të jashtëm. Qendra e të dhënave menaxhohet nga departamenti i TI të një korporate. Klientët në këtë rast konsiderohen të brendshëm, kurse reja private [14].

Një rast i veçantë është kur qendra e të dhënave shërben sipas kërkesave, programe si një shërbim, ku klientët janë të jashtëm dhe secili prej tyre merr të njëjtin version të aplikacionit, p.sh nëpërmjet një ndërfaqeje web. Sidoqoftë, çdo klient e konfiguron dhe e përshtat aplikacionin ashtu si i nevojitet atij. Është e arsyeshme të merret parasysh se çdo klient në këtë rast, është një biznes i vogël ose i mesëm.



Figurë 2.8 Ndërtimi i SAP

Në figurën e mësipërme jepen dy rastet e mundshme të implementimit të sistemit SAP. Mjedisi virtual i ekzekutimit i referohet një bashkësie komponentësh që menaxhojnë mjedise virtuale.

a) Të gjitha komponentët operojnë në të njëjtin ambient virtual pune.
b) Komponentët CI dhe DBMS operojnë secili në një mjedis ekzekutimi virtual dhe të dedikuar.

Ofruesi i infrastrukturës duhet të menaxhojë ciklin e jetës së aplikimit për qindra apo mijëra qiramarrës, duke mbajtur një kosto totale shumë të ulët të shërbimit të ofruar. Kjo përfshin rritjen e numrit të klientëve të rinj, ruajtje të bazës së të dhënave, menaxhimin e personalizimit, dhe update në versionet më të reja të software.

Procesi i shtimit të një qiramarrësi të ri në SaaS, për rastin MSB, është plotësisht i automatizuar nga një program i bazuar në një ndërfaqe interneti. Klienti i ri kalon në një seri pyetjesh për konfigurimin dhe ngarkimet për katalogun e produkteve dhe listën e klientëve. Duke ndjekur këto hapa, qiramarrësi duket sikur po përdor një version tipik prove. Sigurimi i burimeve si p.sh magazinimi, baza e të dhënave dhe aplikacioni server janë pjesë e këtij implementimi të automatizuar.

Konsumatorët faturohen në bazë të një tarife fikse mujore abonimi, ose të një çmimi të ndryshueshëm në bazë të përdorimit të aplikimit të tyre.

Ka disa qasje të njohura për qiramarrje të shumëfishtë të së njëjtës skemë të bazës së të dhënave. Pavarësisht nga qasja, klientët kanë nevojë për skemat elastike të virtualizuara ku, për shembull, komponenti DBMS dhe sistemi i ruajtjes së të dhënave janë të ndara ndërmjet qiramarrësve të ndryshëm. Arsyeja kryesore për këtë ndarje është që të mbajë në minimum kostot për klient.

Sfidat kryesore në të gjitha këto raste të përdorimit nga pikëpamja e infrastrukturës së ofruesit janë:

1. Menaxhimi i mijëra komponentëve të shërbimeve të ndryshme që përbëjnë një llojshmëri të aplikimeve, në krye të një infrastrukture komplekse.
2. Konsolidimi i shumë aplikacioneve në të njëjtën infrastrukturë, duke rritur optimizmin dhe shfrytëzimin e konsumit të energjisë së komponentëve fizikë dhe nga ana tjetër duke e mbajtur koston operacionale në minimum.
3. Garantimi i SLA-ve individuale të shumë konsumatorëve, të cilët përballen me ngarkesa pune të ndryshme dhe të luhatshme.

2.6. Konkluzione

Në zhvillimet e aplikimeve në retë kompjuterike, nuk ekziston një zgjidhje e vetme që i kënaq të gjithë konsumatorët. Pavarësisht reklamave të bukura dhe ofertave të ndryshme të publikuara në faqet e kompanive të shumta, asnjë arkitekturë e vetme nuk i kënaq të gjithë klientët dhe një zgjedhje e kujdesshme strategjike kundrejt asaj të ngarkesës duhet bërë përpara kalimit në re të të dhënave. Një zgjidhje e mesme do ishte më e "duhura", ku raportet e trafikut të informacionit që kalon në re duhet të vihen në balancë me ato të sigurisë.

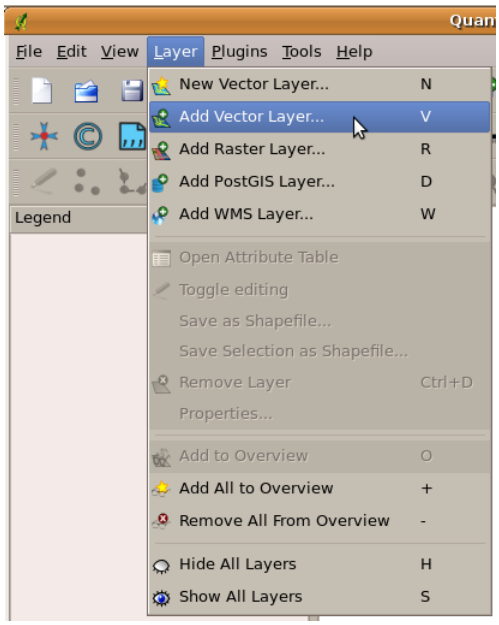
Nga autorë të ndryshëm sugjerohen si modele të përshtatshme arkitektura hibride me shumë instanca që t'u shërbejnë miliona përdoruesve anë e mbarë botës, por duke mbajtur nivele të larta sigurie dhe sigurisht, ajo që është më e "pëlqyeshme" nga klientët; kosto të ulët. Kjo arkitekturë izolon plotësisht informacionin midis klientëve të ndryshëm, duke siguruar në të njëjtën kohë të njëjtat funksione tek të gjithë përdoruesit. Pavarësisht nga qasja, klientët kanë nevojë për skemat që përshtaten lehtë dhe plotësisht të virtualizuara ku, për shembull komponenti DBMS dhe sistemi i ruajtjes së të dhënave janë të ndara ndërmjet qiramarrësve të ndryshëm.

3. Përdorimi i platformave të reve kompjuterike në GIS

3.1. Geographic Information System

GIS (Geographic Information System) është një sistem kompjuterik i integruar HW dhe SW, i cili përdoret për të krijuar, manipuluar dhe analizuar të dhëna gjeografike për të ndërtuar harta të reja dhe të dhëna tabulare. GIS përfshin Computer Aided Design (CAD) dhe DBMS, por është më shumë se sa një kombinim i tyre. Në një sistem GIS ruhet marrëdhënia midis të dhënave gjeografike të hartave të ndryshme dhe një baze të dhënash tabulare, në mënyrë që ndryshimet në harta të reflektohen në databazë. GIS lejon një ripërcaktim të marrëdhënieve midis hartave dhe mund të krijojë harta të reja në bazë të këtyre marrëdhënieve [6].

Aplikimet GIS janë programe të zakonshme me një ndërfaqe grafike ndaj përdoruesit që mund të manipulohet me anë të tastierës dhe mouse. Aplikimet GIS ofrojnë menu si File, Edit etj., të cilat kur klikohen aktivizojnë një panel veprimesh. Veprimet e aktivizuara p.sh mund t'i tregojnë GIS se si të shtojnë një shtresë të re për t'u afishuar.



Figurë 3.1 Një aplikim GIS

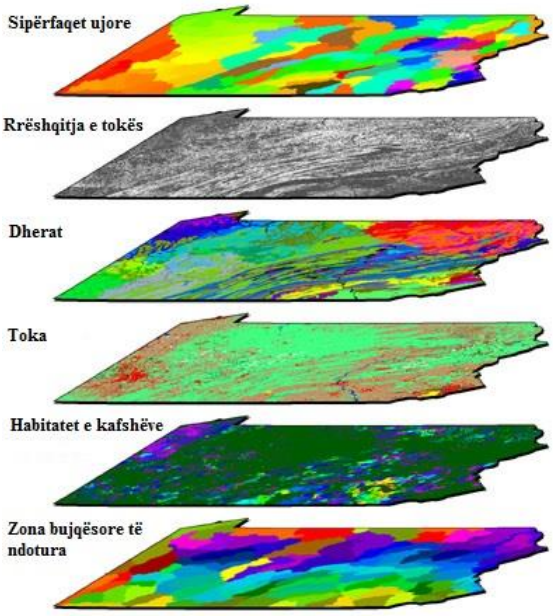
3.2. Rëndësia e GIS

GIS integron të dhëna hapësinore si edhe informacione të tjera në një sistem të vetëm. GIS siguron një ambient të përshtatur për të analizuar të dhëna gjeografike. Duke konvertuar hartat dhe çdo informacion tjetër hapësinor në formë dixhitale, GIS u lejon përdoruesve të manipulojnë dhe të afishojnë njohuritë gjeografike në një mënyrë të re. GIS krijon lidhje midis aktiviteteve të ndryshme bazuar në afërsinë gjeografike dhe duke analizuar të dhënat gjeografike, mund të arrihet në konkluzione dhe shpjegime të fakteve. Këto lidhje janë shpesh të panjohura pa përdorur GIS, por mund të kthehen në thelbësore për të kuptuar dhe menaxhuar burimet dhe aktivitet e

një sistemi. Si një shembull shërben lidhja gjeografike që krijohet midis ndërtimit të një shkolle me mbetjet toksike, apo vendet e grumbullimit të plehrave [7].

Disa nga fushat më të rëndësishme ku përdoret GIS janë:

- Aplikimet të bazuara në rrjetin e rrugëve. Është një aplikim që kërkon për adresa, menaxhon lëvizjen dhe koordinimin e makinave.
- Aplikimet e bazuara në burimet natyrore. Analiza e impaktit menaxherial dhe ambientalist të burimeve natyrore si uji, bimësia, pyjet dhe kafshët.
- Analiza të ndryshme si: Uzinat e rrezikshme me mbetje toksike dhe modelimi e shfrytëzimi i burimeve ujore.
- Habitate natyrale të kafshëve të egra dhe planifikimi i zhvendosjes në hapësira të reja.
- Ndarja zonale e tokave: Zonimi, nënndarjet e tokave, rishikimet, impakti ambinetalist etj.
- Menaxhimi i sistemeve të tubave dhe kabllove nëntokësorë për qëllime administrimi, planifikimi, monitorimi të energjisë së konsumuar etj. [8]



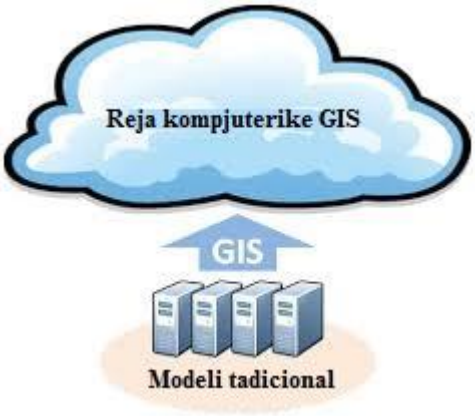
Figurë 3.2 Përdorimi i aplikimeve GIS

3.3. Aplikimet GIS në retë kompjuterike

Një nga sfidat kryesore me të cilat përballet GIS në ambientet klient-server janë të dhënat. Për shkak të rëndësisë së të dhënave, integrimi i informacioneve hapësinore bëhet një hallkë e rëndësishme për t'u konsideruar gjatë projektimit të aplikimeve GIS [9].

Retë kompjuterike lehtësojnë në mënyrë të ndjeshme menaxhimin e të dhënave duke krijuar fleksibilitet si kurrë më parë. Për shembull, duke lejuar akses përdoruesve tek motorët e kërkimit gjeografikë, bëhet më i lehtë përpunimi dhe integrimi i të dhënave krahasuar me sistemet tradicionale [9].

Megjithatë, disa skeptikë e shikojnë përfshirjen e SaaS si një komplikim shtesë ndaj problemit të të dhënave duke ngritur çështjet e sigurisë e të privatësisë, pavarësisht artikujve dhe raporteve që tregojnë se informacioni është më i sigurt në një re, se sa në qendrat private të ruajtjes së të dhënave [10].



Figurë 3.3 Kalimi i GIS në retë kompjuterike

Disa nga parimet bazë të cilat e karakterizojnë renë GIS të pranohet si një pjesëmarrës serioz në gjeneratat e ardhshme GIS janë:

1. Sigurimi i infrastrukturës së aplikimeve:

   Reja GIS ofron ambientin e dedikuar për bizneset dhe sistemet që llogarisin dhe analizojnë të dhënat gjeografike. Për kompanitë që kanë investuar më parë në GIS, burimet e ofruara në retë kompjuterike mund të shfrytëzohen për të rritur ndihmën, duke i bërë të dhënat gjeografike më të lehta për t'u analizuar dhe menaxhuar.

2. Mbështetje tek teknologjia e infrastrukturës:

   GIS në re ofron burime të virtualizuara HW dhe SW dhe akses të plotë në krijimin e të dhënave, të analizës, rifreskimit dhe shfaqjes së tyre. Programe utilitare përmirësojnë dukshëm shpërndarjen e GIS brenda një zyre, qyteti, apo përgjatë gjithë globit.

3. Ulje e kostove të implementimit:

   GIS në re u paraqet një mundësi të madhe klientëve të saj për përdorimin dhe shfrytëzimin e të dhënave hapësinore. Bizneset dhe individët nuk kanë pse të investojnë për burimet HW dhe SW, që në rastet e sistemeve GIS janë të konsiderueshme duke marrë parasysh parametrat cilësore që duhen për këto sisteme. Gjithashtu koha e ngritjes së këtyre sistemeve mund të jetë relativisht e madhe. Kostoja e sistemeve GIS është arsyeja kryesore pse shumë organizata nuk u ofrojnë klientëve të tyre aplikime GIS.

4. Ndarja e pavarur e burimeve:

   Reja GIS ofron mundësi të mëdha për krijimin e burimeve të pavarura.

Procesimi dhe ruajtja sipas kërkesave mund të balancohen përgjatë një infrastrukturë të përbashkët në të cilën, asnjë burim HW nuk i caktohet një individi të vetëm. Modeli „pay-per-use“ i faturon klientët bazuar në përdorimin e kombinuar të fuqisë procesuese, bandwith-it të përdorur dhe volumit të rekordeve të ruajtura në qendrat e të dhënave.

5. Konvertimi i të dhënave dhe i afishimit tek përdoruesit.

   Një shërbim konvertues i të dhënave nënkupton transformimin dhe importin nga një format në një bazë të dhënash. Për çdo sistem GIS, kjo është thelbësore dhe kërkon burime teknike të specializuara të cilat përfshijnë infrastrukturën, shërbimet SW dhe fuqinë njerëzore të menduarit.
   GIS në re ofron shërbimet e konvertimit të dhënave hapësinore pa asnjë burim shtesë të investuar nga klienti. Ky shërbim mund të ofrohet sipas kërkesave dhe sipas modelit „paguaj aq sa përdor“.

3.4. Platforma GIS në renë kompjuterike

Platforma GIS në të cilën do punojë SaaS-GIS duhet t‘u ofrojë klientëve të njëjtat mundësi si edhe ato të modeleve tradicionale dhe t’u shpërndahet atyre në një mënyrë krejt ndryshe. GIS si një shërbim duhet të jetë në gjendje të ruajë, analizojë, menaxhojë dhe afishojë të dhënat që lidhen me një vendndodhje gjeografike të caktuar, duke u lejuar përdoruesve të ndërtojnë kërkime interaktive, të analizojnë të dhëna hapësinore, të modifikojnë harta dhe lehtësisht të afishojnë rezultatet e këtyre operacioneve. „GIS si një shërbim“ ua ofron të gjitha funksionet klientëve të tij vetëm me anë të një ndërfaqeje standarde web. [9]

Kërkesat e ndryshme të klientëve ndaj një platforme open GIS do ishin si më poshtë:

Hapësira e ruajtes së të dhënave

- Të ruhen volume të mëdha të dhënash. Rreth 100 GB çdo ditë.
- Akses i menjëhershëm dhe i kudohershëm.
- Të dhëna të sigurta.
- Ruajtje dhe rikuperim të dhënash.
- Nivele të ndryshme aksesi dhe të drejtash.

Leximi dhe manipulimi i të dhënave

- Simbolikë e rregullt.
- Transparencë.
- Projeksione të ndryshme.
- Shpejtësi leximi dhe përpunimi.
- 2D dhe 3D.
- Zoom dhe matje.
- Opsionet e CAD, GIS, TIN, vektor.
- Krijim opsionesh.
- Mundësi ngarkimi të hartave dhe imazheve nga kompjuterat lokalë dhe lidhja me bazën e të dhënave.
- Mundësi punimi me formate të ndryshme grafikësh.

Një nga arkitekturat më të thjeshta të „vendosjes“ së GIS në një re kompjuterike është propozuar në figurën e mëposhtme. Ndërfaqja me përdoruesin është një faqe standarde interneti me mundësinë për të kërkuar në motorin e hartave gjeografike.

Figurë 3.4 Një platformë reje GIS

Baza e të dhënave përdoret për ruajtjen e të dhënave GIS, të cilat do të aksesohen dhe të procesohen nga përdoruesit nëpërmjet programeve API si p.sh hartat, shtresat, gjeo-procesimi, përdoruesit etj. Një listë e plotë e funksioneve API jepet në figurën e mëposhtme.

Figurë 3.5 Lista e funksioneve API

Motori i hartave është përgjegjës për analizat vektoriale në kohë reale, për indeksimin, procesimin e brendshëm dhe ruajtjen e të dhënave.

Ndërfaqja me përdoruesin do të jetë e thjeshtë, vetëm një interpretues në gjendje mund të lexojë kodet e teknologjisë HTML5.

HTML5 është akoma në zhvillim e sipër, megjithatë shumica e browserave janë në gjendje të kuptojnë dhe ekzekutojnë elementet e HTML5 dhe API.

Aplikimet GIS do të jenë në krye të motorit të hartave. GIS në retë kompjuterike do t’u vijë në ndihmë përdoruesve, thjesht se ka një ndërfaqe të vetme. Kështu p.sh një kompani dëshiron të dijë për infrastrukturën dhe asetet e saj dhe të departamenteve të inxhinierisë, planifikimit dhe operacioneve. Për këtë nevojitet një akses i thjeshtë tek

të dhënat. Gjithashtu një ekip që punon në ambiente jashtë zyrave të kompanisë, i dërgon sistemit informacione në kohë reale, të cilat do të ruhen drejt e në renë GIS. GIS ka për detyrë të procesojë dhe të analizojë të dhënat e mbledhura nga ekipi, duke u dhënë klientëve dhe shërbimeve të ndryshme akses tek të dhënat e përpunuara. Gjithashtu, të gjitha pjesët e projektit të destinuar për publikun e gjerë, hidhen online në një shërbim web për të informuar klientët e kompanisë [11].

3.5. Konkluzione

Asgjë dhe askush nuk mund ta ndalë revolucionin në re. Ka shumë avantazhe drejt SaaS dhe retë kompjuterike janë duke ndryshuar mënyrën sesi bizneset blejnë programe dhe menaxhojnë burimet HW.

Zgjidhja tradicionale e GIS mund të duket se do të mbijetojë akoma edhe pa renë kompjuterike, GIS nuk është përjashtimi. Disponueshmëria, kostoja e vogël dhe fleksibiliteti që ofron GIS si shërbim, do të triumfojnë kundrejt zgjidhjeve të izoluara aktuale. Në përgjithësi GIS në retë kompjuterike duken premtuese [57].

4. Vëzhgime mbi çështjet e sigurisë në retë kompjuterike

4.1. Hyrje

Interneti ka qenë gjithmonë një shtysë drejt zhvillimit të teknologjive të ndryshme. Një nga teknologjitë më të diskutuara janë retë kompjuterike. Disa nga avantazhet kryesore të përdorimit të reve kompjuterike janë:

1. Ulje e kostove HW dhe të mirëmbajtjes.
2. Akses global i të dhënave.
3. Fleksibilitet dhe procese të larta automatizimi, ku klientët nuk kanë pse të shqetësohen për azhurnimin e programeve që ata përdorin [17, 45].

Reja kompjuterike është përcaktuar si një teknikë që është në gjendje të sigurojë një infrastrukturë elastike, ku përdoruesit nuk janë pronarë, por që u siguron atyre shërbimet e kërkuara.

Në bazë të llojeve të ndryshme të shërbimeve të ofruara, retë kompjuterike kategorizohen në disa shtresa.

dSaaS- Data Sotrage as a Service ofron shërbime bazë të ruajtjes së informacionit në rrjet.

IaaS ose infrastruktura si shërbim, ofron shërbimet bazë të infrastrukturës. IaaS i referohet ndarjes së burimeve HW duke përdorur kryesisht virtualizimin, ku shumë përdorues përdorin të njëjtat burime. Përshkallëzimi i aksesit në burimet HW bëhet në bazë të kërkesave të përdoruesve dhe faturimi realizohet sipas modelit: “paguaj aq sa përdor”.

PaaS ose platforma si shërbim, është shtresa që përveç sigurimit të ambientit për aplikimet e përdoruesve, ofron dhe platforma për shërbime të orientuara. P.sh një server aplikimi Paas, u mundëson zhvilluesve të aplikacioneve të krijojnë aplikime të ndryshme web pa blerë servera dhe HW të tjerë, si dhe pa konfigurime dhe licenca shtesë.

Saas ose software si shërbim, është shtresa më e lartë që ofron aplikime më të plota sipas nevojave dhe kërkesave specifike. Saas siguron se të gjitha aplikimet janë të hedhura në internet dhe pagesa e shërbimeve të ofruar janë në bazë të përdorimit.

Pavarësisht modeleve të mësipërme, shërbimet në retë mund të projektohen në katër mënyra në varësi të kërkesave të përdoruesve:

1. Re publike:

   Infrastruktura u sigurohet shumë përdoruesve dhe menaxhohet nga një person ose kompani e tretë. Burimet mund të merren me qira në mënyrë dinamike sipas modelit “paguaj aq sa përdor”, ose mund të ofrohen pa para.

2. Re private:

Infrastruktura, u ofrohet përdoruesve specifikë dhe mirëmbahet nga vetë organizata, ose nga ndonjë person, ose kompani e tretë. Përdoren makina virtuale dhe rrjeti i përdorur është privat e i destinuar për një grup të kufizuar përdoruesish.

3. Re komuniteti:

   Infrastruktura ndahet midis organizatave të ndryshme për një qëllim të përbashkët si p.sh fetar, ushtarak etj.

4. Re hibride:

   Një kompozim i dy ose më shumë modeleve të mësipërme, të lidhura në mënyrë që transferimi i të dhënave të jetë në mënyrë transparente, pa ndikuar në modelet e tjera.

Megjithatë me përparimin e teknologjisë, derivate të këtyre modeleve zhvillohen në varësi të kërkesave të ndryshme . Me zhvillimin e teknologjive si 2G, 3G, Wi-Fi, Wi-max etj, një derivat i reve kompjuterike është zhvilluar dhe në terma popullorë quhet MCC (Mobile Cloud Computing). Re kompjuterike për mobile konsiderohet si një ndërthurje e teknologjisë celulare me infrastrukturën në retë kompjuterike, ku të dhënat dhe përpunimi i tyre realizohet në re, me të vetmin përjashtim që aksesi i tyre të bëhet nga një telefon celular. Zhvillimet e fundit teknologjike si HTML5 dhe të browserave të ndryshëm, e kanë rritur përdorimin e MCC.

Disa nga teknikat që kontribuojnë në teknologjinë e reve kompjuterike janë:

- Virtualizimi:

  Termi i referohet një ambienti në gjendje që t'u sigurojë përdoruesve të gjitha shërbimet e nevojshme që mbulohen nga HW. Tri format ekzistuese të virtualizimit të kategorizuara si: virtualizim i makinës, virtualizimi i pajisjeve të ruajtjes së informacionit dhe virtualizimi i rrjetit, kanë çuar në lindjen e reve kompjuterike. P.sh një numër makinash fizike me kapacitete mjaft të mira, por shumë pak të pashfrytëzueshme nga aplikimet e përdoruesve, mund të konsolidohen në disa makina me një shfrytëzim më efektiv.

- Shërbimet Web dhe SOA:

  Shërbimet web ofrojnë sherbime në internet duke përdorur teknologji si XML, Web Services Description Language (WSDL), Simple Object Access Protocol (SOAP) etj. Organizimi i këtyre shërbimeve menaxhohet në formën e një arkitekture të orientuar shërbimesh (SOA) nëpërmjet së cilës një detyrë e caktuar kryhet duke përdorur shumë shërbime.

- Web 2.0:

  Web 2.0, është konsideruar si një teknologji që u lejon përdoruesve të krijojnë faqe interneti, që nuk kufizohen vetëm në leximin e tyre; në fakt u mundëson

përdoruesve një ndryshim dinamik duke u krijuar atyre një platformë më krijuese.

Disa nga ofruesit e shërbimeve në retë kompjuterike janë: Amazon EC2, Amazon S3, SQS, Google, Microsoft, Salesforce.com, Sun Microsystems etj dhe secili ka karakteristikat sipas klasifikimeve të bazuara në strukturën e shërbimeve: private, publike dhe hibride.

Individë dhe organizata që përdorin internetin gjithmonë e më shumë kërkojnë të jenë anonim. Është e rëndësishme që blerjet online, dërgimi i emaileve të mos ua ekspozojnë të tjerëve identitetin, interesat dhe aktivitetet e tyre. Gjithashtu korporatat dhe organizatat ushtarake duhet të komunikojnë me organizata të tjera pa ua shfaqur ekzistencën e këtyre komunikimeve konkurrentëve ose "armiqve".

Me rritjen e dukshme të migrimit të infrastrukturës në një re kompjuterike, çështjet e sigurisë dhe privatësisë janë bërë më të sofistikuara. Nëpërmjet rritjes së kërkesave për akses në aplikacione të ndryshme, mundësia për sulme kibernetike gjithashtu rritet. Individë të ndryshëm në mënyrë të shpeshtë duhet të japin online kredencialet për identifikimin e tyre dhe gjatë këtij procesi, një ndërhyrës i paautorizuar mund të "vjedhë" informacione të rëndësishme të përdoruesit. Skemat e mëposhtme duhet të jenë të ndërtuara në mënyrë që të mbulohen çështje të tilla të sigurisë dhe privatësisë si: konfidencialiteti, integriteti, autentikimi, rikuperimi i të dhënave në rast fatkeqësie [27].

- Një skemë shifrimi për fshehtësinë e të dhënave. Në retë kompjuterike duhen të dallohen çështjet e privatësisë së të dhënave në transit dhe atyre të ruajtura në disqet e ngurtë.
- Ofruesve të shërbimeve në retë kompjuterike duhet t'u jepet akses i kufizuar në të dhënat e përdoruesve, vetëm menaxhim i tyre pa pasur mundësi të shohin dhe lexojnë përmbajtjen e informacionit.
- Backup i të dhënave dhe replikimi i tyre duke siguruar rikuperim të shpejtë të informacionit të humbur në rast fatkeqësie.

4.2. Barrierat në retë kompjuterike

Shumë kompani dhe organizata nuk e marrin dot vendimin për të kaluar shërbimet dhe të dhënat e tyre në retë kompjuterike. Kjo lidhet me besimin që u mungon atyre për sa u përket çështjeve të sigurisë dhe privatësisë. Disa nga kufizimet që justifikojnë mungesën e besimit janë:

1. Konfidencialiteti dhe siguria

Ofruesit e shërbimeve në retë kompjuterike këmbëngulin se makinat e tyre dhe informacioni që ruhen në to janë të mbrojtur mjaft mirë ndaj sulmeve dhe vjedhjeve të ndryshme. Gjithashtu ky informacion në re është më i sigurt se në kompjuterët personalë të përdoruesve të ndryshëm.

Megjithatë ka pasur mjaft raste kur siguria është cenuar dhe i gjithë sistemi është bërë jo-funksional për orë të tëra [42, 43].

Një re publike shërben si host për një numër të ndryshëm makinash virtuale dhe siguria në këtë tip reje është më e cenueshme, sepse me rritjen e përdoruesve, numri dhe natyra e rreziqeve janë më të mëdha. Migrimi në një re private është një zgjedhje më e sigurt me mundësinë e një kalimi të mundshëm në një re publike.

2. Disponueshmëria, vonesat, performanca

Vonesat në marrjen, hedhjen dhe përpunimin e informacionit kanë qenë gjithmonë një problem sidomos në lëvizjen e të dhënave nga një re në tjetrën. Shifrimi dhe deshifrimi i informacionit pa dyshim që rrisin kohët e informacionit në re. Vonesat në rrjet në rastet kur kërkesat nga përdoruesit e reve janë në nivelin maksimal, shtojnë vonesat në marrjen dhe dërgimin e informacionit. Performanca e sistemit është një faktor tjetër që duhet marrë në konsideratë. Problemet që lindin nga kapacitetet e sistemit si rezultat i kërkesave të shumta nga klientët, ndikojnë në performancën e sistemit dhe rrisin kohën e aksesit.

3. Portabiliteti dhe ndërveprimi

Klientëve të ndryshëm u lind nevoja të transferojnë të dhënat e tyre në re të ndryshme për shkak të perfomancës më të mirë, apo për shkak të shërbimeve shtesë që ua ofrojnë vetëm disa re kompjuterike. Në shumicën e rasteve kjo ka qenë një gjë e pamundur, për shkak të platformave të ndryshme të përdoruara dhe të aplikimeve specifike të ofruara dhe ndërveprimi midis sistemeve të ndryshme nuk ka rezultuar gjithmonë më i efektshëm. Gjithashtu menaxhimi dhe transportimi i çelësave kriptografikë për të dhënat e shifruara nga njëra re në tjetrën, ka rezultuar një detyrë jo e lehtë.

4. Rrjetet me fibër optike dhe rrjedhja e informacionit

Është vënë re një rritje e rrezikut ndaj sigurisë për të dhënat në transit nga klientët në retë kompjuterike dhe anasjelltas. Siguria e të dhënave që dalin nga një data-center në një tjetër, është e një rëndësie primare dhe është thyer shumë herë [47]. Ky transferim bëhet në një rrjet me fibra optike, i cili konsiderohej i sigurt deri në momentin kur u gjet një pajisje përgjuese nëpërmjet së cilës të dhënat kopjoheshin në mënyrë jo të ligjshme. Pajisje që përgjojnë kabujt e fibrave optike mund të vendosen nëntokë duke bërë të lehtë rrjedhjen e informacionit dhe të pazbulueshme praninë e këtyre pajisjeve. Në këto kushte është thelbësore të arrihet siguria e informacionit në transit përgjatë rrjeteve kompjuterike.

4.3. Rreziqet në retë kompjuterike

Përdorimi i SaaS në retë kompjuterike u bë i mundur nga zhvillimi i teknologjisë Web 2.0 duke i lehtësuar përdoruesit nga detyra të tilla si instalimi i programeve dhe mirëmbajtja e tyre. Në këto ambiente, siguria është bërë gjithmonë e më shumë një kërkesë parësore. Më poshtë jepen disa nga elementet bazë të sigurisë të lindura nga sulmet e ndryshme në teknologjinë Web 2.0.

Sulmet SQL injections, realizohen kur një kod dëmtues ndërfutet në një kod standard SQL dhe në këtë mënyrë një ndërhyrës i paautorizuar ndërhyn në databazë dhe akseson informacion sensitiv.

Sulmet me Cros Site Scripting (XSS), realizohen kur një skript dëmtues futet brenda përmbajtjes së faqes së internetit. Më të prekura janë faqet me përmbajtje dinamike të informacionit. Shumë shpesh tek përdoruesit e internetit hapen faqe të vogla në të cilat pa dashje, ose thjesht për kuriozitet klikohet duke i dhënë një ndërhyrësi të paautorizuar akses në informacione sensitive dhe personale. Në mënjanimin e këtyre rreziqeve, teknika të tilla si filtruesi aktiv i përmbajtjes, parandalimi i rrjedhjes së informacionit, diktimi i dobësive të aplikimeve web janë krijuar dhe aktivizuar [16].

Një nga klasat e sulmeve në SaaS etiketohen si *Zoti X*, apo *Man in the Middle attacks (MITM)*. Në këto sulme një ndërhyrës futet në mes të komunikimit midis dy përdoruesve duke u dërguar atyre informacione pavlerë, por që i nevojiten atij për të kuptuar dhe deshifruar informacione sensitive. Përdorimi i nënshkrimeve dixhitale në kriptografinë me çelësa publike dhe zgjedhja me kujdes e algoritmeve të forta kriptografike, bën të mundur parandalimin e sulmeve ndaj programeve të tilla si: Dssniff, Cain, EtterCap, AirJack etj.

Siguria në nivele të ndryshme është e nevojshme për të siguruar një implementim korrekt në retë kompjuterike si: siguria në aksesin e serverave, siguria në internet, siguria e bazës së të dhënave, siguria në fshehtësinë e informacionit, siguria në nivel rrjeti kompjuterik, siguria e të dhënave në shtresën fizike dhe atë të aplikimeve, siguria në aksesin e programeve.

4.4. Siguria në rrjete

Për të pasur një siguri të mirë në rrjeta duhen marrë parasysh konfidencialiteti dhe integriteti në rrjet, akses i kontrolluar në rrjet dhe mirëmbajtje e sigurisë kundrejt rreziqeve të jashtme. Problemet e lidhura me nivelin e sigurisë në rrjetet kompjuterike përmblidhen në: sulmet DNS, sulmet me përgjim, ripërdorimi i adresës IP, DoS ose mohim i shërbimit, DSoS ose mohim i shpërndarë i shërbimit etj.

Sulmet DNS (Domain Name Server): Një server DNS shërben për përkthimin e emrit të një domain-i në një adresë IP, për arsye se adresat numerike të internetit janë të vështira për t'u memorizuar. Një nga sulmet më tipike, është ai kur një përdorues rrugëtohet gjatë përkthimit të një emri në IP, në një tjetër re kompjuterike të ndërtuar nga Z. X dhe bie viktimë e një mashtrimi kibernetik, gjatë të cilit mund të japë informacione sensitive si pini i kartës së kreditit apo informacione të tjera personale. Me gjithë realizimin e protokolleve të ndryshme si DNSSEC (Domain Name Server Security Extensions), ka raste kur këto masa sigurie nuk janë të mjaftueshme dhe rruga e duhur e komunikimit midis dërguesit dhe marrësit është ndryshuar nga persona të tretë ose programe dëmtuese, duke shkaktuar probleme në sigurinë e transmetimit.

Sulmet me përgjim: Ky sulm starton nga një aplikim i cili përgjon paketat TCP/IP që kalojnë në rrjet dhe, nëse trafiku i kapur nuk është i shifruar me një kriptosistem të fortë, ai mund të lexohet dhe të interpretohet nga Z. X, duke marrë informacione të rëndësishme për përdoruesit e shërbimeve në re. Një program përgjues drejt për së drejti në kartën e rrjetit të një kompjuteri, mund të marrë informacione jo vetëm nga kompjuteri, kartën e rrjetit të cilit po përgjon, por edhe nga sisteme të tjera që komunikojnë me kompjuterin e sulmuar.

Sulmet me IP të përdorur më parë: Çdo nyjeje në rrjet i vihet një adresë IP, e cila është një numër i fundmë. Me largimin e një përdoruesi nga rrjeti, kjo adresë rrjeti i caktohet një përdoruesi tjetër. Ky ndryshim minon në disa raste sigurinë e përdoruesit të ri, sepse ka një diferencë kohe midis ndryshimit të IP-s në serverin DNS dhe pastrimit të rekordit të vjetër nga memoriet cache. Në këtë mënyrë, megjithëse adresa e vjetër i shënohet një përdoruesi të ri, ekziston një mundësi jo për t'u neglizhuar, në të cilën të dhënat e përdoruesit të ri të aksesohen nga një përdorues tjetër duke shkaktuar probleme të privatësisë.

Sulmet me IP: IP hijacking (prefix hijacking ose route hijacking) janë marrja në mënyrë të paligjshme e një grupi adresash IP duke korruptuar tabelat e rrugëtimit. Komunikimi global në internet bëhet i mundur nëpërmjet lidhjes së dy ose më shumë përdoruesve me anë të adresave të internetit duke kaluar paketat nga njëri ruter në tjetrin në mënyrë të vazhdueshme sa më afër marrësit. Në nivel global adresat individuale grupohen së bashku në prefikse të cilat vendosen dhe janë pronë e një sistemi autonom (SA) dhe tabelat e rrugëtimit midis sistemeve autonome mirëmbahen me anë të protokollit BGP (Border Gateway Protocol). Një grup rrjetesh që vepron nën një policë rrugëtimi të vetme të jashtme, njihet si sistem autonom. Çdo sistem autonom ka një numër unik identifikues. IP hijacking mund të ndodhë qëllimisht ose jo në një nga mënyrat e mëposhtme:

- Një SA publikon një prefiks për të cilin nuk është ai zotëruesi.
- SA transmeton një prefiks të gabuar në vend të një prefiksi të saktë të zotëruar nga një SA tjetër.
- Një SA njofton për ekzistencën e një rrugëtimi më të shkurtër drejt një sistemi autonom të kompromentuar nga sulmi kibernetik, pavarësisht nëse rrugëtimi ekziston apo jo.

Në rastet e mësipërme, trafiku rrugëtohet në një adresë krejt tjetër nga ajo tek e cila është destinuar. Thuhet se ka rrjedhje të informacionit në një destinacion krejt tjetër. Incidente të tilla janë raportuar në shumë raste nga Google në 2l005, industria e telekomunikacionit CTBC në Brazil 2008, sulmet kibernetike kineze në 2010, ku China Telecom publikoi rreth 37000 prefikse që nuk i zotëronte, duke shkaktuar ndërprerje globale të shërbimeve. Një sistem i sigurt për sistemet autonome mund të gjendet i shpjeguar tek [48].

4.5. Siguria në nivel aplikimi

Nga vëzhgimet e shumta për sigurinë e përdorimit të internetit është vënë re që edhe pse siguria në nivel rrjeti kompjuterik është e lartë, ekzistojnë defekte në aplikimet e ndërtuara të cilat u lejojnë ndërhyrësve të paautorizuar akses të informacionit. Rreziqet e sigurisë në nivel aplikimi përfshijnë sulmet XSS, Cookie Poisoning, manipulimi i fushave të fshehura, sulme me SQL injections, DoS/DDoS, Backdoor, CAPTCHA breaking etj., duke rezultuar në një përdorim të paautorizuar të aplikimit.

Një sulm fillohet nga një përdorues apo aplikues të cilët janë të maskuar si përdorues të zakonshëm të aplikimit dhe sistemi i njeh ata si të besueshëm, u jep atyre akses të plotë duke rënë pre e sulmit. Me zhvillimet teknologjike, politikat e sigurisë janë bërë të papërdorshme. Ka pasur raste kur siguria e sistemit është thyer nga përdorues të maskuar si përdorues legjitim. Imitimi i një përdoruesi të besueshëm është sot mjaft i

lehtë duke marrë nën kontroll një sistem të tërë pa lënë gjurmë. Është e nevojshme instalimi i niveleve më të larta të sigurisë për të minimizuar këto rreziqe.

4.5.1. Rreziqet e sigurisë për Hipervizorin

Retë kompjuterike bazohen tërësisht në konceptin e virtualizimit. Në një ambient të virtualizuar, menaxhuesi dhe kontrolluesi që lejojnë ekzekutimin e platformave të ndryshme në një HW të vetëm, njihet si hipervizor dhe u siguron makinave virtuale një ambient HW të pavarur nga njëra-tjetra. Me rritjen e numrit, si të makinave virtuale, ashtu edhe të sistemeve operative që punojnë në të njëjtin HW, rriten edhe shqetësimet ndaj rreziqeve të sigurisë. Mund të ndodhë që një sistem operimi të ekzekutojë një kod dëmtues duke ulur të gjitha shërbimet e ngritura në re. Nëse një ndërhyrës i paautorizuar arrin të marrë kontrollin e hipervizorit, ai mund të bëjë ndryshime në çdo njërën nga makinat virtuale, pra, mund të sigurojë kontroll mbi informacionet personale të përdoruesve.

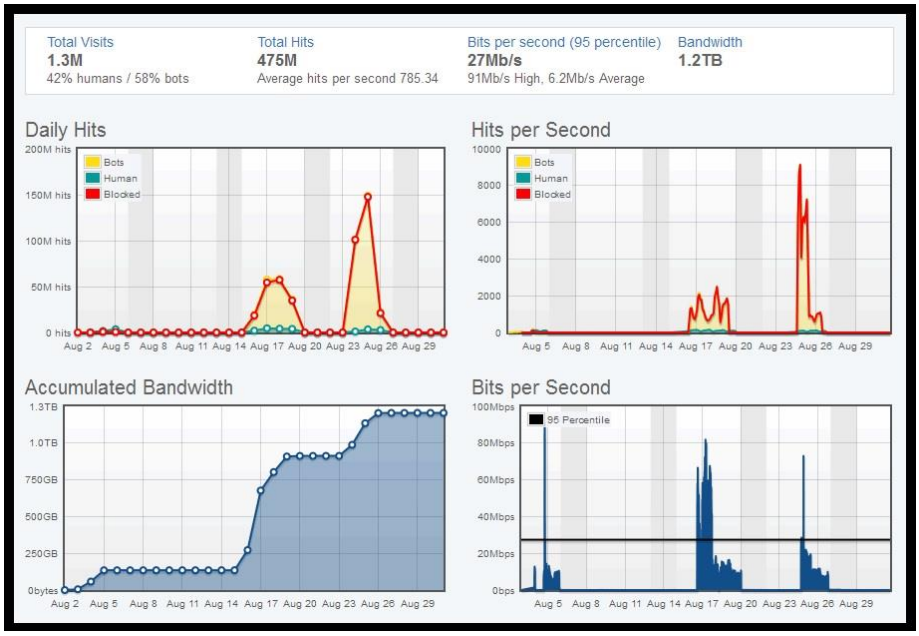
Një sistem mbrojtës i avancuar mund të ndërtohet duke monitoruar aktivitetin e makinave virtuale dhe ndërkomunikim midis komponentëve të ndryshme të infrastrukturës së resë kompjuterike [49].

4.5.2. Sulmet DoS/DDoS

Konsiderohen të tilla përpjekjet për t'i bërë shërbimet e përdoruesve legjitimë të paaksesueshme. Në këtë sulm, serveri i shërbimit "bombardohet" nga një numër i madh kërkesash duke e kthyer shërbimin të paarritshëm nga përdoruesit e sistemit. Serveri refuzon t'u përgjigjet kërkesave të përdoruesve për shkak tashmë të mungesës së burimeve të nevojshme për të procesuar kërkesat. Pjesë të ndryshme të resë kompjuterike bëhen të paaksesueshme si rezultat i konsumit të madh të bandwith nga kërkesat e shumta në pritje. Kur sulmi vjen nga disa makina, atëherë ai njihet me emrin DDoS (Distributed Denail of Service Attack). Avantazhi i një sulmi efektiv me DDoS është se disa makina të infektuara janë shumë më të vështira për t'u identifikuar dhe pastruar. Sulmi DdoS mbështetet nga tre sisteme dinamike funksionale: sistemi master, sistem skllav dhe një sistem viktimë. Sulmi nis nga masteri i cili është organizatori dhe inicializuesi i një sulmi të tillë. Skllavi është sistemi i rrjetit që i siguron masterit platformën e nevojshme nga e cila do të nisë sulmin drejt sistemit viktimë. DDoS është operacional në dy faza: e para është faza e ndërhyrjes, ku masteri mundohet të infektojë makina jo shumë të rëndësishme për sistemin, të cilat i përdor më pas për të kompromentuar makina më të rëndësishme. Hapi tjetër është instalimi i miniprogameve DoS duke filluar sulmin ndaj sistemit viktimë, qoftë ky server apo makinë. Mënyra e ndërprerjes së shërbimi ndryshon nga DoS vetëm nga mënyra se si inicializohet sulmi. Site i CNN u bë pre e një sulmi të tillë duke u ndërprerë shërbimin mijërave përdoruesve në të gjithë globin për një periudhë prej tri orësh.

Metoda parandaluese më efektive ndaj sulmeve DoS/DDoS është përdorimi i një sistemi diktues ndaj ndërhyrjeve, IDS (Intrusion Dedection System). Në çdo re kompjuterike instalohet një IDS, të cilat komunikojnë nëpërmjet shkëmbimit të informacionit. Në rast se një re specifike sulmohet me DoS, atëherë retë e tjera njoftohen për sulmin. Një sistem i tillë federativ është shumë efektiv. Një mbrojte e përdorur në makinat virtuale ndaj sulmeve DDoS në retë kompjuterike është paraqitur

tek [50]. Në sistemin e implementimit të reve kompjuterike Eucalyptus, instalimi i IDS në të gjitha makinat fizike që janë mbartëse të makinave virtuale të përdoruesve, ka rezultuar i efektshëm [51].



Figurë 4.1 Një shërbim në RE që parandalon DDoS

4.5.3. Manipulimi i fushave të fshehura

Gjatë lundrimit në një faqe web, ka disa fusha të cilat u janë fshehur përdoruesve të faqes dhe përdoren për shërbime administrative nga projektuesit e site-t. Këto fusha mund të manipulohen lehtë nga ndërhyrësit e paautorizuar. Informacioni më pas i ndryshuar postohet në faqen ekzistuese apo drejtohet në një faqe tjetër sipas dëshirës së sulmuesit [49]. Duke evituar përdorimin e fushave të fshehura në fjalëkalimet, çmimet, numrat e kartave të kreditit dhe duke i ruajtur këto në baza të dhënash bëhet e mundur minimizimi i sulmeve të tilla.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<!-- Copyright 2010 Google Inc. -->
▼<html>
 ▶<head>…</head>
 ▼<body screen_capture_injected="true">
  ▶<div class="menu">…</div>
   <h2>Gruyere: New Snippet</h2>
  ▼<div class="content">
    <h3>Add a new snippet.</h3>
   ▼<div style="width:600">
    ▼<form method="get" action="http://google-
      gruyere.appspot.com/611788451095/newsnippet2">
      <textarea name="snippet" rows="5" style="width:
      100%"></textarea>
      <input type="hidden" name="username" value="admin">
     </form>
    </div>
   </div>
```

Figurë 4.2 Fushë e fshehur për përdoruesin "admin"

4.5.4. Helmimi i Cookies

Duke ndryshuar përmbajtjen e një cookie në internet, një sulmues mund të sigurojë akses të paautorizuar në një aplikim ose faqe web. Një cookie përmban informacione

mbi identitetin e përdoruesit dhe mund të falsifikohet nëse nuk merren masa si pastrimi periodik, apo shifrimi kriptografik i tyre. Në rastin e mëposhtëm hapet një faqe dinamike, *finalizoblerjen.asp*, e cila postohet nga përdoruesi nëpërmjet browser-t në serverin e aplikimit, duke i treguar aplikimit se është gati të përfundojë blerjen. Kjo kërkesë ka një cookie që përmban parametrat e mëposhtëm: *IDSesioni*, një identifikues unik i përdoruesit me aplikimin, *MadhesiaShportës* e cila ruan numrin e artikujve të blerë, çmimin e çdo artikulli dhe totalin e blerjes. Kur postohet faqja, skripti në finalizoblerjen.asp, lexon nga kompjuteri i përdoruesit parametrat e cookie dhe debiton llogarinë e përdoruesit me vlerën e lexuar nga totali. Një ndërhyrës mund të rrisë artificialisht p.sh vlerën e totalit të blerjes për të përfituar zbritje.

*GET / finalizoblerjen.asp?checkout=PO HTTP/1.0 Host: www.blejonline.com.al Accept: */* Referrer: http://www. blejonline.com.al/afishoprodukt.asp*

Cookie: IDSesioni =570321ASDD23SA2321; MadhesiaShportës=3; Artikull1=220; Artikull2=3210; Artikull3=100; Total=3530;

4.5.5. Captcha

Captcha është një program i destinuar të dallojë nëse komunikimi vjen nga një njeri apo makinë dhe është zhvilluar si një metodë për të parandaluar shfrytëzimin e internetit nga programet robotë ose kompjuterat. Captcha përdoret për të parandaluar spamet ose eksplorimin pakufi të burimeve nga programet robotë. Sulmet me ditëlindje apo regjistrimet e shumëfishta në portalet e internetit parandalohen me anë të kësaj metode. Megjithatë në shërbimet e Gmail dhe Hotmail, kjo metodë është thyer nga ndërhyrës të cilët përdorin programe konvertues të tekstit të shkruar ose përdorin audion e sistemit për të dëgjuar dhe kuptuar karakteret e Captcha.

4.5.6. Sulmi me Google

Një sulm i tillë sulm bazohet në motorin e kërkimit Google, i cili është shumë i përdorur nga përdoruesit në të gjithë globin. Motori i kërkimi google, tek i cili futesh tek adresa www.google.com, ofron shumë opsione si përkthim të dokumenteve, kërkime në web, imazhe, bloge, lajme e shumë të tjera, por këto opsione u ofrojnë mundësi edhe përdoruesve të "këqij" të internetit duke përfshirë; piratët kompjuterike, vjedhësit e identitetit si edhe terroristët. Aplikacionet dëmtuese që bazohen në motorin e kërkimit google, përmblidhen në një term të vetëm "Google Hacking".

Zakonisht një ndërhyrës tenton të gjejë dobësi dhe informacione në sistemin që dëshiron të komprometojë, duke kërkuar në google dhe më pas nis një sulm bazuar në informacionin e mbledhur. Operatorët e avancuar u sigurojnë ndërhyrësve të paautorizuar një platformë nga ku mund të nisin sulmet e tyre. Më poshtë jepet lista e operatorëve të avancuar Google si edhe përdorimi i tyre.

Tabelë 4.1: Lista e operatorëve të avancuar Google

Operatori	**Qëllimi**	**Vepron me operatorët e tjerë?**	**Përdoret vetëm?**	**Web**	**Imazhe**	**Grupe**	**Lajme**
Intitle	Kërko për titull	Po	Po	po	Po	Po	po
allintitle	Kërko për titull	Jo	Po	po	Po	Po	po
Inurl	Kërko URL	Po	Po	po	Po	jo 100%	po
Allinurl	Kërko URL	Jo	Po	po	Po	Po	po
Filetype	Tip skedar	Po	Jo	po	Po	Jo	jo 100%
allintext	Kërko në faqe	jo 100%	Po	po	Po	Po	po
Site	Kërko për site specifik	Po	Po	po	Po	Jo	jo 100%
Link	Kërko link në faqe	Jo	Po	po	Jo	jo	jo 100%
inanchor	kërko link <a>	Po	Po	po	Po	jo 100%	po
numrange	kërko numër	Po	Po	po	Jo	jo	jo 100%
daterange	kërko në diapazon	Po	Jo	po	jo 100%	jo 100%	jo 100%
Author	kërko autor	Po	Po	jo	Jo	po	jo 100%
Group	kërko grup me emër	jo 100%	Po	jo	Jo	po	jo 100%
insubject	kërko grup me subjekt	Po	Po	po	Po	po	po
Msgid	kërko grup me msgid	Po	Po	jo 100%	jo 100%	po	jo 100%

4.6. Siguria në ruajtjen e të dhënave

Të dhënat e përdoruesve merren dhe ruhen në qendra të mëdha të ruajtjes së të dhënave të njohura si "data centres", duke u siguruar kompanive apo edhe individëve të veçantë një ambient për të ruajtur të dhënat e tyre. Ofruesit e shërbimeve në retë kompjuterike pretendojnë se të dhënat e ruajtura në serverat e tyre janë të sigurta dhe

të mbrojtura nga çdo dëmtim, humbje apo vjedhje e mundshme, por ka raste të dokumentuara kur të dhënat janë modifikuar si rezultat i thyerjes së sigurisë ose si rezultat i gabimeve njerëzore. Shërbimet e fushatave të marketingut nëpërmjet emaileve të disa kompanive kryesore si JP Morgan Chase, CitiBank, Barclays Bank, zinxhirët e hoteleve si Marriot dhe Hilton, Best Buy, u dëmtuan kur një sasi e madhe informacioni e klientëve të këtyre kompanive si email-et dhe të dhëna bankare iu ekspozuan personave të paautorizuar. Një incident i ngjashëm ka ndodhur me shërbimin EC2 të Amazon, ku disa nga klientët kryesorë të saj pësuan humbje të mëdha. Një nga aspektet e tjera të sigurisë qëndron se programe dëmtuese mund të lançohen nga domain-e të njohura publike për të askesuar databazat e mbrojtura të reve kompjuterike. Në shërbimin e Amazon të njohur si shërbimi i ruajtjes me 3 "S" (**S**imple **S**torage **S**olution), kode dëmtuese u futën në bazat e të dhënave dhe fillimi i këtij lloji sulmi u krijua nga një burim i tretë i besuar. Amazon u bë pre e sulmeve të tilla nga ku një makinë virtuale e besuar në të njëjtin server me të dhënat e dëmtuara, mundi me lehtësi të aksesojë informacione konfidenciale. Përveç sulmeve nga programe apo kode dëmtuese, gabimet njerëzore janë të pashmangshme. Raste të tilla ku administratorët e shërbimeve kanë fshirë të dhënat e klientëve ekzistues duke shkaktuar humbje të pazëvendësueshme të informacionit janë të evidentuara si në rastin e MediaMax [20, 46].

4.7. Sigurimi nga rreziqet e ndryshme në retë kompjuterike

Ofrues të ndryshëm të reve kompjuterike kanë adoptuar teknika të ndryshme për të mbrojtur shërbimet e ofruara ndaj klientëve të tyre nga sulmet e ndryshme si Sql injection, XSS, DoS, DDoS dhe sulmet me kërkim në motorin Google. Disa nga teknikat standarde që diktojnë sulmet e mësipërme janë: Ndalimi i përdorimit të kodeve dinamike SQL në kodet burim, kontrolli dhe filtrimi i të gjitha vlerave të ndërfutura nga përdoruesit, ndalimi i përdorimit të karaktereve të veçanta etj.

Baza e të dhënave *Google Hacking* (*GHDB*), përmban kërkime të ndryshme për të dhëna sensitive si p.sh mesazhe gabimesh që përmbajnë shumë informacione, skedarë me fjalëkalime përdoruesish, faqe portalesh me emra përdoruesish, informacione mbi sesione të klientëve të ndryshëm, informacione që cenojnë sigurinë në rrjetet kompjuterike si loge të sistemeve të sigurisë etj. Disa zgjidhje të ndryshme ofrohen nga programet që kontrollojnë cenueshmërinë e faqeve web ndaj sulmeve me kërkim në google. Këto programe në mënyrë automatike kërkojnë për elemente që mund të cenojnë sigurinë e aplikimeve web. Përdoruesit duhet të jenë të ndërgjegjshëm dhe të kujdesshëm në përdorimin e aplikimeve web për të mos ruajtur informacione sensitive të cilat mund të ekspozohen me anë të kërkimit google.

Simptomat e një sulmi DoS/DDoS janë: reduktimi i shpejtësisë së sistemit dhe ngadalësim në ekzekutimin e programeve, një numër i madh kërkesash nga një numër i madh përdoruesish, reduktim i ndjeshëm i burimeve të sistemit. Sulmet DDoS janë shumë të dëmshme, sepse ezaurojnë burimet e sistemit duke rrezikuar mosfunksionimin e një sistemi të tërë, megjithatë një monitorim i kujdesshëm i rrjetit mund të mbajë të tilla sulme nën kontroll. Tabela e mëposhtme jep një analizë të disa skemave ekzistuese të sigurisë të aplikuara në retë kompjuterike.

Tabelë 4.2: Skemat ekzistuese të sigurisë

Skema	**Metoda**	**Avantazhet**	**Kufizimet**
Siguria e të dhënave.	Përdorimi i funksioneve homomorfike së bashku me kodet gabimndreqëse Reed-Solomon [20, 21].	1. Operacione dinamike fshi, shto, ndrysho mbi blloqet e të dhënave në sisteme të shpërndara të ruajtjes së informacionit. 2. Efikas në zbulimin dhe korrigjimin e modifikimeve të ndryshme si rezultat i gabimeve të tipit "bizantin" ose ndërhyrjeve të paautorizuara. 3. Efikas në lokalizimin e makinës së kompromentuar/dëmtuar në një sistem të shpërndarë.	Gabime të tjera më granulare duhet të merren në konsideratë.
Siguria e identiteteve dixhitale të përdoruesve.	Përdorimi i skemave aktive, ku përdoret protokolli me njohje zero dhe ndarjet e sekretit Shamir dhe Ben-Or, Goldwasser dhe Wigderson.	Nuk kërkon një burim të tretë të besueshëm për verifikimin e identitetit siç përdoren rëndom në skemat *PRIME, Windows CardSpace, Open ID*. Reja kompjuterike mund të përdoret në këtë rast vetëm për shifrimin dhe deshifrim.	Skema aktive mund të mos ekzekutohet fare në makinën që kërkon shërbim, duke kompromentuar skemën. Identiteti i përdoruesit ngelet i fshehtë, por atij i mohohet shërbimi.
Model i besueshëm për sigurinë në retë hibride.	1. Ndarje e domain për ofruesit dhe përdoruesit me anë të një agjenti të besueshëm. 2. Strategji të ndryshme për ofruesit e shërbimeve dhe klientët.	1. Ndihmon klientët të evitojnë shërbimet keqdashëse. 2. Ndihmon ofruesit e shërbimeve të parandalojnë bashkëpunimin me përdorues keqdashës.	Siguri e kufizuar, përshkallëzimi i kufizuar. Kjo skemë parandalon një numë të kufizuar rreziqesh dhe mund të aplikohet në ambiente të kufizuara.

Virtualizim i sigurt. [52]	1. Bazohet në idenë e një sistemi të avancuar për mbrojtjen e makinave virtuale dhe krijimin e një shtrese të mesme të shpërndarë. 2. Sjella e komponentëve të resë kompjuterike mund të monitorohet me anë të logeve dhe kontrollit periodik të skedarëve të ekzekutueshëm të sistemit.	Një rrjet i virtualizuar është objekt i sulmeve të ndryshme që mund të lançohen nga një makinë virtuale që ekzekuton një sistem shfrytëzimi të çfarëdoshëm. Sjellja e një sistemi të tillë mund të monitorohet pa u diktuar nga makina virtuale duke bllokuar çdo aktivitet të dyshimtë dhe njoftuar sistemin përgjegjës të sigurisë.	Performanca e sistemit bie në mënyrë progresive e ndikon negativisht në implementimin e këtij sistemi.
Rrjet virtual në ambientet e reve.	Ofruesit e reve kompjuterike kanë sugjeruar të maskojnë strukturën e brendshme të shërbimeve të tyre si edhe politikat e vendosjes së fileve dhe të fokusohen në rreziqet e kanalit të transmetimit duke ulur mundësinë e rrjedhjes së informacionit.	Siguron identifikim e kundërshtarëve ose palës sulmuese. Duke fshehur strukturën e rrjetit virtual, pala kundërshtare mund të gjejë vendndodhje të tjera të makinave virtuale, por jo të makinës "target".	Rrezikon pjesë të tjera të sistemit. Nuk garanton një siguri të plotë të sistemit.
Border Gateway Protocol (BGP) [53]	Një sistem i "mirë" BGP (PGBGP) është sugjeruar, arkitektura e të cilit sugjeron kontrollet e rasteve kur një sistem autonom njofton veten e tij si destinacion të gabuar për të dhënat e transferuara drejt tij.	Kontrollon sistemet autonome dhe gjen anomali për të siguruar që informacioni të mos drejtohet në sistemin e gabuar. Është elastik në ekzekutimin e protokollit PGBGP në vetëm disa nga sistemet autonome krahasuar me ekzekutimin në gjithë rrjetin.	I ndjeshëm ndaj sulmeve DoS. Kjo metodë merret parasysh vetëm në rrugëtimin e mesazheve kontrolluese, por nuk verifikon rrugën aktuale që ndjek trafiku i informacionit.

4.8. Konkluzione

Me rritjen e dukshme të migrimit të infrastrukturës në një re kompjuterike, çështjet e sigurisë dhe privatësisë janë bërë më të sofistikuara. Nëpërmjet rritjes së kërkesave për akses në aplikacione të ndryshme, mundësia për sulme kibernetike gjithashtu rritet. Individë të ndryshëm në mënyrë të shpeshtë duhet të japin online kredencialet për identifikimn e tyre dhe gjatë këtij procesi, një ndërhyrës i paautorizuar mund të "vjedhë" informacione të rëndësishme të përdoruesit. Skemat e mëposhtme duhet të jenë të ndërtuara në mënyrë që të mbulohen çështje të tilla të sigurisë dhe privatësisë si: konfidencialiteti, integriteti, autentikimi, rikuperimi i të dhënave në rast fatkeqësie.

Një skemë të vetme për parandalimin e rreziqeve të ndryshme nuk mund të ketë, pasi problemet e sigurisë janë të shumta dhe më të ndjeshme sesa në rastin e sistemeve tradicionalë. Një sistem si ai i propozuar tek [20, 21] nuk merr në konsideratë konfidencialitetin e të dhënave, sepse ai kufizohet vetëm tek ndreqja e gabimeve me anë të kodeve lineare, por ai mund të kombinohet me një sistem tradicional të kriptografisë me çelësa publikë.

5. Një metodë për shkëmbimin e sigurt të të dhënave në retë kompjuterike mobile

5.1. Hyrje

Teknologjitë 2G, 3G, Wi-Fi, Wi-Max kanë bërë të mundur lindjen e një derivati të ri në retë kompjuterike të njohura si retë kompjuterike mobile, në të cilat përpunimi i të dhënave ndodh në renë kompjuterike dhe mund të aksesohet nëpërmjet një celulari. Në këtë kapitull do të preken çështjet e ngritjes dhe funksionimit të një shërbimi të sigurt shkëmbimi të dhënash midis dy përdoruesve, i pari krijuesi i skedarit dhe i dyti marrësi i autorizuar. Reja mobile përdoret për ruajtjen e shifruar të skedarit pa i zbuluar përmbajtjen kompanisë që ofron shërbimin në re. Pajisjet mobile janë të pajisura me bateri e kështu kanë një fuqi përpunimi të kufizuar, kapacitet ruajtës të kufizuar, më pak siguri, në disa raste internet të kufizuar dhe të paparashikuar si dhe më pak energji. Kufizimet e mësipërme krijojnë pengesa serioze për aplikime që kërkojnë përpunime intensive dhe kapacitete ruajtëse të konsiderueshme. Për të rritur mundësitë, kapacitetet, jetëgjatësinë e baterisë, të dhënat që kërkojnë fuqi llogaritëse dhe hapësirë ruajtëse të mëdha dhe të pamjaftueshme si ato të aparateve celulare, shërbimet e ofruara mund të transferohen në retë kompjuterike [12, 13].

Figurë 5.1 Një skenar në retë kompjuterike mobile

5.2. Shifrimi i bazuar në identitetin e përdoruesit.

Shifrimi i bazuar në identitetin e përdoruesit përbën një zhvillim të rëndësishëm ndaj problemit të menaxhimit të çelësave. Ky shifrim mund të përdorë si çelës publik një varg karakteresh të çfarëdoshme, duke bërë të mundur shifrimin e të dhënave pa nevojën e një certifikate. Mbrojtja e shifruar sigurohet nga një server që kontrollon krijimin dinamik të çelësave të deshifrimit që u korrespondojnë identiteteve publike të përdoruesve. Duke ndarë autentikimin dhe autorizimin nga procesi i përftimit të çelësave, e drejta për të krijuar çelësa privatë mund të kontrollohet në mënyrë dinamike. Natyra "pa gjendje" e këtij lloji shifrimi e bën këtë të fundit shumë të thjeshtë.

Shifrimi i bazuar në identitetin e përdoruesit është një teknologji shifrimi që llogarit çelësin publik nga identiteti i një përdoruesi dhe çelësin korrespondues privat nga çelësi publik. Kjo llogaritje mund të kryhet sipas kërkesave në kohë reale, përparësi

kjo e dukshme kundrejt sistemeve të tjera me çelësa publike që përftohen rastësisht dhe shpërndahen përpara vendosjes së komunikimit të sigurt [22, 55]. Aftësia për të llogaritur çelësin publik të marrësit eliminon nevojën e dërguesit dhe marrësit të komunikojnë me njëri-tjetrin direkt ose nëpërmjet një direktorie shërbimesh përpara se të dërgojnë mesazhe të sigurta. Si identifikues për krijimin e çelësave publike shërbejnë adresat e emaileve, numrat mobile, IMEI etj. Procesi i shifrimit mund të inicializohet nga dërguesi i mesazhit i cili llogarit çelësin publik të marrësit nga një identifikues unik i këtij të fundit si p.sh numri i telefonit ose adresa e emailit. Një server i besueshëm dhe i sigurt i quajtur ndërtuesi i çelësave private, përdor një algoritëm shifrimi dhe llogarit çelësin korrespondues privat nga çelësi publik. Marrësi përfton të njëjtin çelës privat nga serveri pa u merakosur për shpërndarjen e çelësit të tij publik.

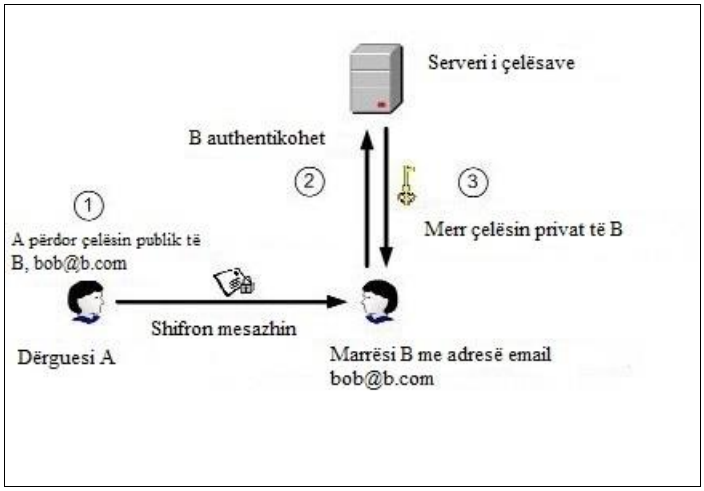
Diagrama e mëposhtme ilustron faktin se si përdoruesi A i dërgon një mesazh të shifruar përdoruesit B duke përdorur skemën e shifrimit bazuar në identitetin e përdoruesit B.

1. Përdoruesi A dërgon një mesazh të shifruar duke përdorur adresën e tij të email-t si çelës publik.

2. Përdoruesi B identifikohet në serverin e çelësave për të nxjerrë çelësin e tij privat. B e kërkon informacionin nga serveri, ndërsa ky i fundit kontakton një direktori shërbimesh ose një shërbim tjetër autentikimi dhe sfidon përdoruesin me një seri pyetjesh dhe përgjigjesh duke verifikuar identitetin e këtij të fundit. Gjatë këtij shkëmbimi informacioni midis B dhe serverit, politika të ndryshme të sigurisë mund të aplikohen si p.sh përdoruesi mund të mos jetë përdorues aktiv dhe mesazhi i kthehet A përsëri.

3. Serveri i çelësave i kthen B-s çelësin e tij privat dhe mesazhi deshifrohet. B mund të ruajë në celularin e tij çelësin privat dhe të deshifrojë mesazhet edhe kur serveri nuk përgjigjet. Përdoruesit B nuk i duhet ndonjë program i veçantë përpara se A t'i çojë atij një mesazh të shifruar.

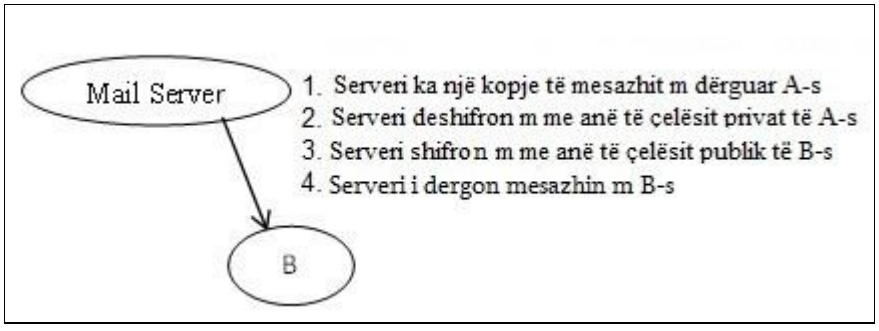
I vetmi informacion që serveri i çelësave ruan gjithmonë është një çelës sekret master, i cili është një numër i rastit i madh, i njohur vetëm nga serveri. Pas instalimit të programit tek aparati i përdoruesit, çelësi master përdoret nga serveri për të përftuar çelësin publik dhe çelësin privat të marrësit.



Figurë 5.2 Shifrimi i bazuar në identitet

5.3. Rishifrimi i autorizuar

Qëllimi i kësaj metode të re kriptografike është rishifrimi i një teksti të shifruar më parë me një çelës privat, me një tjetër çelës privat të ndryshëm nga i pari. Një shembull i përditshëm është rasti i emaileve të shifruara që duhet të bëhen "forward" nga përdoruesi A tek B. Përdoruesi A merr një mail të shifruar me çelësin e tij publik dhe meqë vetëm ai ka çelësin privat, vetëm ai mund të deshifrojë emailin e mbërritur. Kur përdoruesi A largohet me pushime, ai kërkon t'ia delegojë detyrat përdoruesit B duke i bërë forward çdo email të tijin, por ai nuk do t'i japë B-s çelësin e vet privat. Mënyra më e thjeshtë dhe naive njëkohësisht do të ishte që, vetë serveri i emaileve të deshifronte mesazhet e A-s duke përdorur çelësin privat të këtij të fundit të ruajtur në server dhe më pas të rishifronte të njëjtin email duke përdorur çelësin privat të B-s. Kjo metodë është e thjeshtë sepse e gjithë ngarkesa bie mbi serverin e emaileve që ka një kopje të gjithë mesazheve të shifruara dhe çelësin privat të përdoruesit A. Njëkohësisht kjo metodë paraqet edhe një përafrim naiv, sepse serveri i emaileve mundet aksidentalisht ose qëllimisht të ndryshojë mesazhet e A-s, prandaj nuk mund të jetë një burim i besueshëm [15].



Figurë 5.3 Implementim i thjeshtë, por naiv i shifrimit të autorizuar

Në vitin 1998 Blaze, Bleumer dhe Shtrauss sugjeruan rishifrimin automatik të njohur si metoda BBS [18]. U rifut koncepti i rishifrimit $RE_{A\to B}$ që autorizon rishifrimin nga një çelës privat në tjetrin pa ditur përmbajtjen e tekstit të hapur. Skema bazohet në kriptosistemin ElGamal.

- Gjenerimi i çelësave:

  $< g >= \mathbb{G}$ me rend q të thjeshtë të grupit.

  $SK_a = a \in \mathbb{Z}_q^*$, $SK_b = b \in \mathbb{Z}_q^*$, ku a a, b zgjidhen rastësisht.

  $PK_a = g^a$, $PK_b = g^b$

  $RE_{A \to B} = b \cdot a^{-1} (\mod q)$

- Shifrimi:

  Mesazhi $m \in \mathbb{G}$, një numër i rastit $k \in \mathbb{Z}_q^*$

  Mesazhi i shifruar për A është $C_a = (g^k \cdot m, g^{ak})$

- Deshifrimi:

  $m = \frac{g^k \cdot m}{(g^{ak})^{a^{-1}}}$, çelësi privat a përdoret nga A për të deshifruar m

- Rishifrimi i autorizuar:

  $C_a = (g^k \cdot m, g^{ak})$

  $C^b = (g^k \cdot m, (g^{ak})^{RE_{A \to B}}) = (g^k \cdot m, (g^{ak})^{b \cdot a^{-1}}) = (g^k \cdot m, g^{bk})$, që jep mesazhin e shifruar duke përdorur çelësin privat të B-s.

Në fund të fazës së shifrimit, përdoruesi A ka rishifruar m duke përdorur çelësin publik të B-s dhe serveri i mesazheve mund të nisë mesazhin e shifruar drejt B dhe vetëm ai mund të deshifrojë duke përdorur çelësin e tij privat. Teksti i shifruar bazohet në kriptosistemin ElGamal dhe serveri i mesazheve duke mos ditur a dhe b, nuk mund të bëjë dallimin midis $RE_{A \to B}$ dhe një elementi çfarëdo nga $\mathbb{Z}_q$. Megjithë përmirësimin e metodës së shifrimit mund të vihen re këto:

1. Serveri mund të llogarisë të anasjellin e $RE_{A \to B} (mod\, q)$, duke e lejuar këtë të fundit të rishifrojë të gjitha mesazhet e B drejt A.

2. Nëse serveri bashkëpunon me A-në në dëm të B, është e lehtë si për serverin ashtu edhe për A të llogarisin çelësin privat të B-s. Në të njëjtën mënyrë, B me serverin mund të bashkëpunojnë në dëm të A-së duke llogaritur çelësin privat të këtij të fundit.

3. $RE_{A \to B}$ kërkon që B të ndajë çelësin e tij sekret, kështu që të dy përdoruesit varen nga një përdorues i tretë i besueshëm. Ndarja e çelësave kuptohet që është një veti e padëshirueshme. Kërkohet një sistem në të cilin $RE_{A \to B}$ bazohet vetëm në çelësin sekret të A-s dhe atë publik të B-s. Edhe pse

shkëmbimi i sigurt i çelësave është i mundur në kriptografi, kjo veti nuk është shumë e dëshirueshme meqë A dhe B nuk kanë njohje të mëparshme dhe komunikimi i ndërsjellë është jo gjithmonë i mundur [24, 25].

5.3.1. Funksionet bilineare dhe skema të përmirësuara të rishifrimit

Le të jenë $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3$ grupe ciklike të të njëjtit rendi q.

Një funksion bilinear i $\mathbb{G}_1 \times \mathbb{G}_2$ tek $\mathbb{G}_3$ është një funksion $e: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$ i tillë që për çdo $g_1 \in \mathbb{G}_1$, $g_2 \in \mathbb{G}_2$, a, $b \in \mathbb{Z}_q$,

$$e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$$

Në skemat me rishifrim të autorizuar, $\mathbb{G}_1 = \mathbb{G}_2$, $\mathbb{G}_1 =< g >$, $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ është lehtësisht i llogaritshëm nga ana kompjuterike dhe $< e(g,g) >= \mathbb{G}_2$ [23].

Problemi Diffie-Hellman (DDH) në funksionet bilineare është nga ana kompjuterike një problem i lehtë meqë funksioni *e* është lehtësisht i llogaritshëm. Kriptosistemet që përdorin funksionet bilineare bazohen në problemin bilinear Diffie-Hellman (DBDH) dhe të anasjellit të tij (k-DBDHI).

- Problemi DBDH: Jepen $(g, g^a, g^b, g^c (g \in \mathbb{G}_1), U \in \mathbb{G}_2)$, a është

  $$U = e(g,g)^{abc} ?$$

  Pra a është e mundur të dallohet $e(g,g)^{abc}$ nga një element i zgjedhur rastësisht $U \in \mathbb{G}_2$?

- Problemi k-DBDHI: Jepen $(g, g^t, g^{t^2}, \cdots g^{t^k} (g \in \mathbb{G}_1), U \in \mathbb{G}_2)$, a është:

  $$U = e(g,g)^{t^{-1}} ?$$

  Pra a është e mundur të dallohet $e(g,g)^{t^{-1}}$ nga një element i zgjedhur rastësisht $U \in \mathbb{G}_2$?

Algoritmi i përmirësuar bazuar në transformimet bilineare është si më poshtë:

- Përftimi i çelësave:

  $< g >= \mathbb{G}_1$ me rend q të thjeshtë të grupit.

  $SK_a = a \in \mathbb{Z}_q^*$, $SK_b = b \in \mathbb{Z}_q^*$, ku a, b zgjidhen rastësisht.

  $PK_a = g^a$, $PK_b = g^b$

  $U = e(g,g)$

$$RE_{A\to B} = (g^b)^{a^{-1}} = g^{\frac{b}{a}}$$

- Shifrimi:

  Mesazhi $m \in \mathbb{G}_2$, një numër i rastit $k \in \mathbb{Z}_q^*$

  Mesazhi i shifruar për A është $C_a = (U^k \cdot m, g^{ak})$

- Deshifrimi:

  $m = \frac{U^k \cdot m}{e(g^{ak}, g^{a^{-1}})} = \frac{U^k \cdot m}{U^k}$, çelësi privat a përdoret nga A për deshifrimin e mesazhit m

- Rishifrimi:

  $C_a = (U^k \cdot m, \mathrm{g}^{ak})$

  $C_b = (U^k \cdot m, e(g^{ak}, RE_{A\to B})) = (U^k \cdot m, e(g^{ak}, g^{\frac{b}{a}})) = (U^k \cdot m, U^{kb})$

  Deshifrimi mund të bëhet vetëm nga B me anë të çelësit të tij privat b :

  $m = \frac{U^k \cdot m}{(U^{kb})^{b^{-1}}}$

Disa nga avantazhet e skemës së mësipërme:

1. A-ja përdor vetëm çelësin e tij privat dhe çelësin privat të B-s për të rishifruar mesazhin. Nuk ka komunikim për shkëmbim çelësash.
2. Serveri nuk mund të rishifrojë mesazhin e përdoruesit B për A, sepse nuk mund të llogarisë $g^{a\cdot b^{-1}}$ nga $g^{b\cdot a^{-1}}$, me supozimin që DDH është problem i vështirë.
3. Serveri nuk mund të lexojë mesazhin e shifruar për B, pa pasur vetë çelësin privat.
4. Edhe duke bashkëpunuar me A, serveri nuk mund të llogarisë çelësin privat b nga $RE_{A\to B}$.
5. DBDHI së bashku me skemën ElGamal garantojnë sigurinë e kësaj skeme [28, 55].

5.4. Shkëmbim i sigurt i të dhënave në re

Kombinimi i shifrimit bazuar në identitet me rishifrimin e autorizuar, ofron një shërbim të sigurt për shkëmbimin e informacionit duke siguruar jo vetëm fshehtësinë

e të dhënave, por edhe një kontroll me kosto minimale për rifreskimin e politikave të aksesit si në rastin e rekordeve të pacientëve ose dokumenteve të ruajtura në një platformë mobile. Në rastin e skedarëve të ruajtur në një re mobile do të merren parasysh tre komponentë:

1. Krijuesi i dokumentit (A). Krijuesi i këtij dokumenti mund të jetë një kompani, një individ i një organizate ose një departament i tërë me politikat e sigurisë për dhënie aksesi të privilegjuar në dokumentet e kompanisë.

2. Marrësit e skedarit (B) mund të jenë individi, kompania, institucioni, departamenti, të cilëve u është dhënë aksesi të shkarkojnë një kopje të lexueshme të dokumenteve nga pajisjet e ruajtjes në renë kompjuterike.

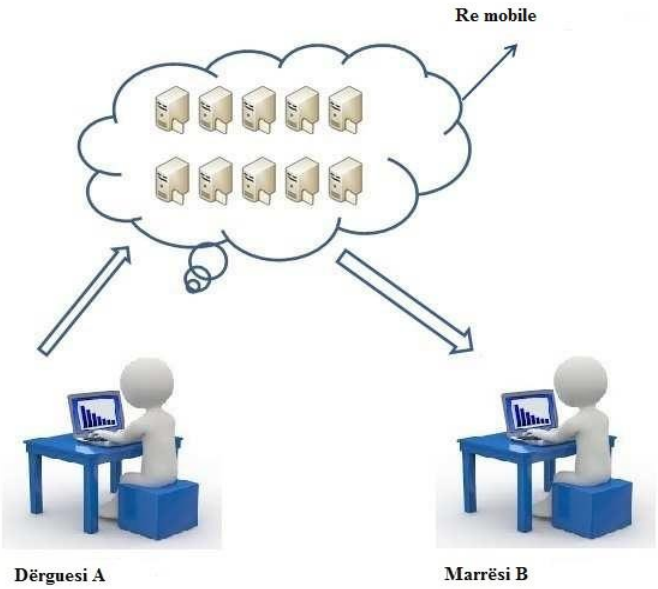
3. Ofruesi i shërbimit në re është një ofrues shërbimesh në renë kompjuterike mobile me detyrën që t'u ofrojë hapësirë ruajtjeje të dhënave të ndryshme që duhet të shkëmbejnë me njëri-tjetrin përdoruesit A dhe B. Ofruesi i shërbimit ka dhe përgjegjësi të tjera si autentikimin e përdoruese në re, menaxhimin dhe krijimin e burimeve në mënyrë sa më efikase dhe të shpejtë. Në krijimin e çelësit master, ofruesi i shërbimit mund të konsiderohet si një entitet gjysmë i besueshëm, por edhe një entitet i tretë mund të merret në konsideratë. Integriteti i skedarëve nuk merret parasysh, ai konsiderohet i zgjidhur dhe një skemë e sigurt mund të gjendet tek [19] ku kodet Reed-Solomn së bashku me mesazhet homomorfike janë përdorur për të siguruar integritetin e të dhënave nga modifikimet e mundshme si rezultat i dëmtimeve ose gabimeve të tipit "Bizantin".

Në modelet e rrjeteve për shkëmbim të sigurt të informacionit një program jo fort i besueshëm i hostuar në një re mobile, transformon një bllok të shifruar të një dokumenti me çelësin publik të A, në një bllok të shifruar duke përdorur çelësin publik të B. Në këtë skemë përdoren shifrimi i bazuar në indentitein e A së bashku me rishifrimin e autorizuar. Identiteti i A konvertohet në një string binar $ID \in \{0,1\}^*$ dhe si identifikues publik mund të shërbejnë adresa emailit, numri i celularit ose çdo element publik që identifikon një entitet në mënyrë të vetme.

Funksioni bilinear $e: \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ zgjidhet me kujdes dhe është lehtësisht i llogaritshëm në grupet ciklike $\mathbb{G}_1$ dhe $\mathbb{G}_2$ me rend të thjeshtë q. Funksioni prerës $H: \{0,1\}^* \to \mathbb{G}_1$ përdoret për konvertimin e identitetit të përdoruesve në një element të $\mathbb{G}_1$. Skema funksionon si më poshtë:

1. Zgjidhen parametrat e sistemit ($\mathbb{G}_1$, $\mathbb{G}_2$, g , e) së bashku me çelësin master MK. MK krijohet nga një burim gjysmë i besueshëm i ruajtur në re dhe përdoret për krijimin e çelësave privatë për identifikimin e përdoruesve në re.

2. Përdoruesit mobile duhet të regjistrohen në sistem për të marrë një çelës sekret SK të përftuar si kombinim i identitetit të përdoruesit duke përdorur MK dhe funksionin prerës. Një përdorues duhet të shkarkojë një aplikacion mobile në aparatin e tij dhe gjatë fazës së instalimit krijohet çelësi sekret SK_{ID}. Skema e shifrimit bazuar në identitetin e përdoruesit është përdorur për shkëmbimin e çelësave privatë dhe publikë.



Figurë 5.4 Modeli i shkëmbimit në re

3. Përdoruesi A i cili zotëron dokumentin, e ndan atë në n copa dhe e konverton në një element $m_i \in \mathbb{G}_2$. Duke përdorur identitetin e përdoruesit ID_A si çelës publik, mesazhi shifrohet dhe më pas copa e shifruar $EF(m_i)$ ngarkohet në renë e serverit:

$$EF_A(m_i) = (m_i \cdot e(g,g)^k, g^{k \cdot SK_A}),$$

ku $k \in \mathbb{Z}_q^*$ është një numër i rastit.

4. Pas ngarkimit të skedarit në re, A përfton çelësat e rishifrimit dhe transformon bllokun $EF_A(m_i)$ të shifruar me çelësin e tij publik, në një bllok të ri $EF_B(m_i)$ të shifruar me çelësin publik të B.

5. Marrësi B kërkon nga reja mobile skedarin e rishifruar dhe reja verifikon identitetin e këtij të fundit. Nëse verifikimi përfundon me sukses, reja i dërgon B-s dokumentin e shifruar dhe në bazë të transformimit bilinear, marrësi deshifron të dhënat pa ndërhyrjen e dërguesit.

5.5. Sfidat në të ardhmen

Shifrimet e plota homomorfike (FHE) po shikohen gjithmonë e më shumë si një e ardhme premtuese për sa i përket informacionit të ruajtur në re. Edhe pse aktualisht konsiderohen si jopraktike për t'u realizuar, kërkimet janë gjithmonë e më intensive [54, 55].

Duke shfrytëzuar kapacitetet ruajtëse të një reje, përdoruesi A ruan të shifruar informacionin në re, pasi ai është "mosbesues" ndaj ofruesit të shërbimit në re. Të dhënat e përdoruesit mund të jenë sensitive si p.sh kartela personale e pacientit, apo balanca e një llogarie bankare. Në rast se atij i duhet të kryejë llogaritje mbi të dhënat e shifruara si p.sh një afishim të llogarisë bankare, apo një raport mbi të dhënat e tij

mjekësore, proceset e ngritura në re duhet të kryejnë llogaritje aritmetike dhe logjike mbi të dhënat e shifruara dhe rezultati i këtyre llogaritjeve t'i kthehet përdoruesit në mënyrë gjithashtu të shifruar. Përdoruesi duke pasur çelësin privat, vetëm ai mund të deshifrojë rezultatin e llogaritjeve. Reja në këtë rast punon mbi të dhëna të shifruara dhe rezultati i jepet kërkuesit i shifruar.

Kjo skemë "konkurron" skemën e propozuar në këtë kapitull, por aplikimet janë të kufizuar në skema kryesisht larg skemave praktike. Megjithatë shifrimet homomorfike mbeten shumë interesante dhe gjasa të jenë një sprovë e vërtetë në të ardhmen [54].

6. Menaxhimi i identiteteve në retë kompjuterike

Një identitet është një bashkësi karakteristikash unike të një individi, subjekti apo objekti. Një identitet i përdorur për qëllime identifikimi njihet si identifikues [44].

Ashtu si edhe në botën reale, identifikues të ndryshëm dixhitalë, përdoren në kontekste të ndryshme. Është e zakonshme, për shembull, të ruhen në identitete të ndryshme informacione të ndryshme. Një identitet i përdorur në Amazon lidhet me një numër karte krediti, kurse një tjetër në MySpace, nuk shoqërohet me një informacion të tillë. Rregullat për t‘u pajisur me një identitet të caktuar janë gjithashtu të ndryshme. Pajisja me një identitet në Amazon është e thjeshtë: mjafton një emër përdoruesi dhe një fjalëkalim, por jo kaq e thjeshtë në ambientet e punës, ku kërkohet të paktën aprovimi i administratorit që mirëmban rrjetin e brendshëm.

Entitete të ndryshme mund të kenë shumë identitete dhe menaxhimi i tyre bëhet i vështirë, prandaj dhe lind nevoja e një sistemi që i menaxhon këto identitete. Një sistem menaxhues identitetesh (IDM) vendos se çfarë informacioni personal duhet të transmetohet për të siguruar një shërbim të caktuar. IDM kryen detyrat e mëposhtme:

1. Krijon identitetet: Ruan informacionet personale të një entiteti në një identitet.

2. Ruan përdorimin e të dhënave të një identiteti. Krijon loge aktiviteti të një identieti në një sistem të caktuar shërbimesh dhe krijon një ndërfaqe aksesi të këto loge.

3. Fshin një identitet: I cakton identitetit një datë skadence. Të dhënat personale bëhen të paaksesueshme mbas datës së skadencës.

Pavarësisht llojit të ndryshëm të identiteteve, një gjë e vetme i bashkon ato: gjatë transmetimit në rrjet, çdo identitet dixhital përfaqësohet me një identifikues sigurie. Identifikuesi i sigurisë është një varg bytesh që identifikon dhe përfaqëson një identitet dixhital. Një identifikues i thjeshtë do të ishte emri i përdoruesit, kurse një tjetër më kompleks do të përmbante emrin, mbiemrin, adresën, numrin e telefonit dhe mbase më shumë të dhëna se kaq. Identifikuesit e sigurisë mund të përmbajnë dhe informacione sensitive si p.sh numër karte krediti [35].

Tabelë 6.1: Identifikuesi i sigurisë

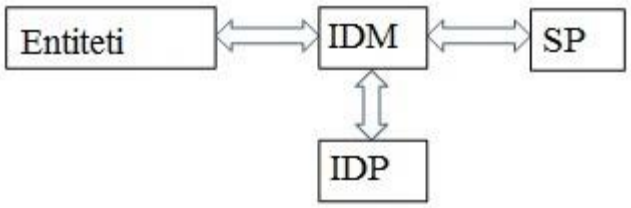
Identifikuesi i sigurisë
Pohim 1
Pohim 2
...
Pohim n

Ideja bazë e çdo identifikuesi është e njëjtë - janë grup pohimesh në formate të ndryshme. Rasti më i thjeshtë është një emër përdoruesi i afishuar si një varg karakteresh, por një format më kompleks do të ishin certifikatat X.509 dhe tiketat Kerberos.

Identifikuesi i sigurisë si term është pak i gabuar, meqë një identifikues sigurie mund të përmbajë informacione që nuk kanë të bëjnë me sigurinë.

Përdoruesi, që paraqet këtë informacion sigurie, duhet të bindë sistemin se është vërtet personi që pretendon të jetë, ku një mënyrë e thjeshtë është dërgimi i një fjalëkalimi së bashku me informacionet e tjera. Një metodë më e mirë do ishte nënshkrimi dixhital i të gjitha pjesëve të identifikuesit të sigurisë duke përdorur një çelës privat dhe më pas transmetimi i çelësit publik p.sh, me anë të një certifikate. Elementet e sigurisë që përfaqësojnë një identitet dixhital, duhet t'i sigurojnë kontrolluesit të identitetit, që informacioni i përket pikërisht entitetit që pretendon të jetë, pasi ky i fundit ka transmetuar pohimet e sigurisë [41, 56].

Bazuar në idenë e përgjithshme të një burimi të tretë të besueshëm kur testohet identiteti i një entiteti, janë ndërtuar shumë sisteme menaxhuese të identiteteve. Ndërveprimi i përdoruesve ose identiteteve me IDM dhe ofruesit e shërbimeve (SP) jepet në figurën e mëposhtme:



Figurë 6.1 Sistemi i menaxhimit të identiteteve

Komponentët bazë të një IDM janë:

1. Ofruesi i identiteteve (IDP), lëshon identitete dixhitalë. Për shembull kompanitë e kartave të kreditit krijojnë dhe shpërndajnë identitete për të mundësuar pagesa, qeveritë krijojnë identitet për qytetarët etj.

   Për identitetin dixhital të krijuar nga një punëdhënës, ofruesi i identitetit është zakonisht një sistem si Acitve Directory.

   Identitetet dixhitalë të krijuara nga ofrues të ndryshëm, përmbajnë informacione të ndryshme dhe sigurojnë nivele të ndryshme sigurie për identifikimin e përdoruesve.

2. Ofruesi i shërbimeve (SP) , u ofron përdoruesve shërbime të ndryshme bazuar në identitetet e krijuara më parë. Për shembull, një përdorues me anë të identitetit të tij dixhital, paguan faturat në një shërbim të ofruar online nga kompania e shpërndarjes së energjisë.

3. Entiteti duhet të provojë identitetin e tij përpara se të marrë shërbimin e kërkuar.

   Entitetet janë shpesh njerëzit, por edhe organizatat, aplikimet, kompjuterat mund të krijojnë identitete dixhitalë.

4. Menaxhuesi i identiteteve (IDM), është një burimi i tretë i besueshëm si nga IDP, por edhe dhe entiteti e shërben për krijimin, mirëmbajtjen, verifikimin e

identiteteve dixhitalë. Verifikuesi i identitetit gjykon mbi korrektësinë ose jo të një pohimi në identifikuesin e sigurisë.

Në modelet tradicionale, IDM janë kryesisht të bazuara në modelin e centralizuar rreth aplikimit, ku çdo aplikim ruan gjurmë të entiteteve që përdorin aplikimin. Në retë kompjuterike, entitetet mund të kenë shumë llogari në shërbime të ndryshme. Gjithashtu entitetet mund të përdorin shërbime të ndryshme të ofruara nga një sistem i vetëm (p.sh Gmail dhe Google Docs ofrohen nga google) [31].

Një përdorues i resë duhet të japë informacion personal i cili përdoret për ta identifikuar këtë të fundit duke lënë një gjurmë të dhënash personale që, mund të përdoren për të lokalizuar në mënyrë të vetme përdoruesin. Në rast se këto të dhëna nuk mbrohen në mënyrën e duhur, informacioni mund të keqpërdoret. Një nga sfidat e sotme në retë kompjuterike është se si të sigurohet informacioni nga përdorimet e paautorizuara duke parandaluar krime serioze si ai i privatësisë apo vjedhjes së identitetit.

Retë kompjuterike kanë si nevojë një model të bazuar rreth përdoruesit dhe jo rreth aplikimit. Kërkesa për një shërbim të caktuar duhet të lidhet me entitetin që e kërkon këtë shërbim, duke zvogëluar numrin e identiteteve dixhitalë që lidhen me entitetin [39].

6.1. Windows CardSpace

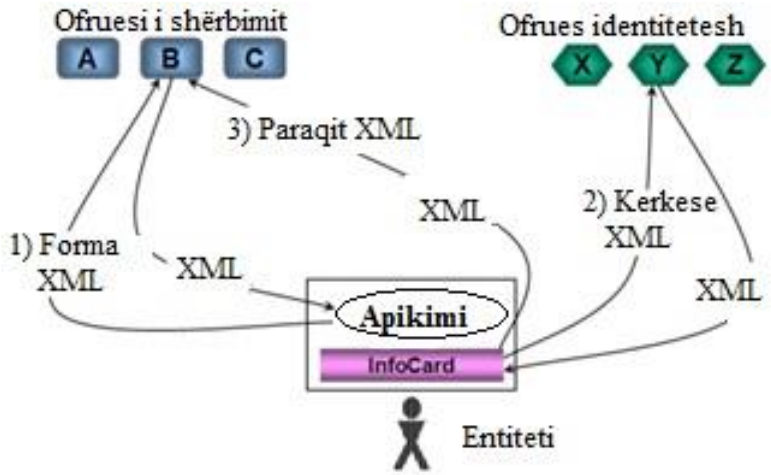
Webiste ose aplikimi i bazuar në CardSpace kur kryen autentikimin e një përdoruesi, i kërkon këtij të fundit disa informacione. Përdoruesi zgjedh midis një “InfoCards” midis disave të paraqitura dhe më pas CardSpace kontakton një IDP për të marrë një identitet sigurie në formën e një XML të nënshkruar me firmë dixhitale. XML përmban informacionin e kërkuar dhe ky i fundit i komunikohet aplikimit të përdoruesit.

Një browser/aplikim që ka të implementuar CardSpace, mund të përdorë sisteme të treta për të garantuar procesin normal të autentikimit. Gjithashtu entiteti mund të zgjedhë një ofrues identitetesh midis disave të afishuar në aplikimin e tij. Pavarësisht nga zgjedhja, shkëmbimi midis pjesëtareve të ndryshëm kalon në tre hapa:

Si fillim, aplikimi i kërkon ofruesit të shërbimit formatin XML që nevojitet për autentifikimin e përdoruesit. Ky informacion përmban të dhëna si, formatin e identitetit të sigurisë që pranon ofruesi i shërbimit dhe egzaktësisht pohimet e nevojshme për të siguruar identitetin e përdoruesit.

Së dyti, aplikimi ia kalon informacionin e marrë mbi formatin XML, CardSpace, duke i kërkuar këtij të fundit formën e plotë të plotësuar të identitetit të sigurisë. CardSpace kontakton një ofrues të përshtatshëm identitetesh bazuar në formatin e mëparshëm XML dhe shkarkon gjithë formën e plotësuar me pohimet e sigurisë.

Së fundmi CardSpace ia kalon këtë informacion aplikimit të përdoruesit dhe ky i fundit ia transmeton ofruesit të shërbimit, i cili nga ana e tij mund të kontaktojë një ofrues tjetër shërbimesh ose të identifikojë përdoruesin duke lejuar ose jo akses në burimet e tij.



Figurë 6.2 Bashkëveprimi midis përdoruesit, aplikimit, shërbimit dhe CardSpace

Një nga disavantazhet e CardSpace është se përdoruesve u duhet edhe një burimi i tretë i besueshëm identitetesh dhe në rastin e humbjes së besimit të burimit të tretë, identiteti i përdoruesve është i rrezikuar [43].

Një studim pë rritjen e sigurisë të CardSpace mund të gjendet tek [36].

6.2. OpenID

OpenID është një protokoll autentikimi i decentralizuar që u vjen në ndihmë përdoruesve të resë kompjuterike në menaxhimin e identiteteve dixhitalë me një kontroll më të madh në ekspozimin e të dhënave personale. Një përdoruesi i duhet të mbajë mend vetëm një emër përdoruesi dhe një fjalëkalim të quajtur me një emër të vetëm OpenID [26].

Përdoruesi i resë kompjuterike akseson një shërbim të caktuar duke përdorur si autentikim OpenId të krijuar më parë. Në momentin që një shërbim në “re” zbulon se përdoruesi përdor OpenId, i ofron atij mundësinë të identifikohet duke përdorur OpenID. Ofruesi i shërbimit OpenId pyet përdoruesin nëse ofruesi i shërbimit në renë kompjuterike është i besueshëm ose jo. Nëse përdoruesi e pranon shërbimin si të besueshëm, kredencialet e tij i kalohen shërbimit, i cili vendos ose jo t’i ofrojë përdoruesit shërbimin e kërkuar. Mbas verifikimit të OpenId, autentikimi konsiderohet i suksesshëm dhe përdoruesi konsiderohet i loguar në sistem me kredencialet e OpenID.

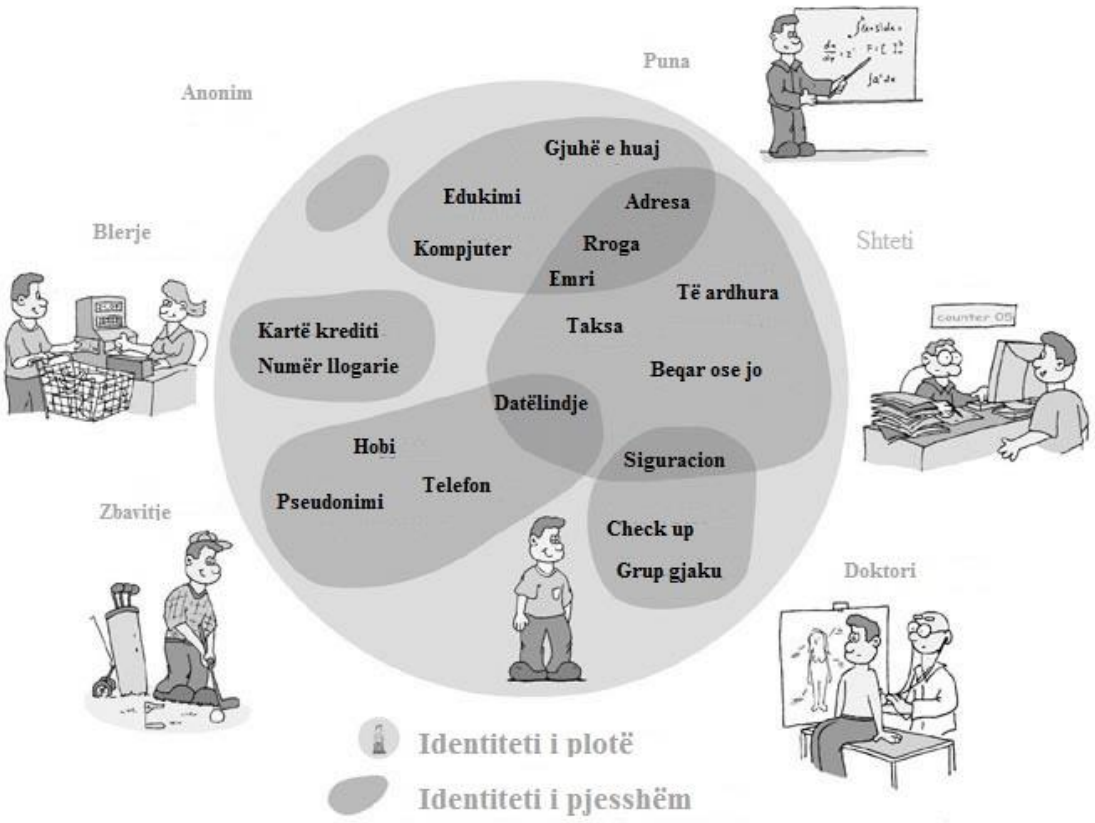
OpenId ka disavantazh, ashtu si edhe CardSpace, faktin se i lihet në dorë përdoruesit të gjykojë nëse shërbimi në re është i besueshëm apo jo. Një sulm mund të ndërtohet lehtë duke “joshur” përdoruesit në transmetimin e kredencialeve në një website të ngjashëm me një ofrues legjitim OpenID [37, 41].

6.3. Prime – Menaxhimi i identiteteve dhe privatësisë për Evropën

PRIME adreson çështjet thelbësore të privatësisë në Internet dhe bazohet në dy rregullat bazë të mbrojtjes në retë kompjuterike:

1. Ndarja e kontekstit, në mënyrë që një vëzhgues të mos arrijë të mbledhë të dhëna sensitive.

2. Të qenit i kujdesshëm kur kërkohen të dhëna personale dhe ruajtja e historikut të informacionit të ekspozuar më parë.



Figurë 6.3 Identitetet e pjesshme të një entiteti

Këto rregulla janë parimet bazë të koncepteve dhe prototipeve të zhvilluara nga projekti PRIME. Që në 2004, shumë partnerë nga industria, akademia, qendrat kërkimore dhe autoritet e mbrojtjes së informacionit kanë punuar në projektin PRIME mbi menaxhimin e identitetit dhe privatësisë [38].

Entitetet zakonisht në mënyrë intuitive vendosin të tregojnë informacione private në varësi të situatës specifike. Për shembull të dhënat në jetën profesionale janë të ndryshme nga ato në jetën private. Në një librari është i nevojshëm një informacion tjetër, krahasuar me atë në një qendër sportive. Asnjë nuk arrin të krijojë identitetin personal të një entiteti. Vetëm identitete të pjesshme mund të vëzhgohen. Identiteti i një entiteti përbëhet nga shumë identitete të pjesshme, ku secili nga identitetet përfaqëson entitetin në një kontekst apo rol të caktuar. Menaxhimi i identiteteve nënkupton zgjedhjen dhe krijimin e identiteteve të pjesshme bazuar në kërkesat specifike të aplikimit. Sisteme menaxhimi të identiteteve të kontrolluara nga entiteti mund të përdoren për të mirëmbajtur fjalëkalimet dhe pseudonimet e ndryshme.

Një nga metodat e veçanta të përdorura nga Prime, është përdorimi i "kredencialeve private", të cilat provojnë veti të caktuara të një individi (p.sh mosha mbi 18 vjeç) pa zbuluar informacione që mund të gjejnë identitetin e tij. Këto kredenciale private

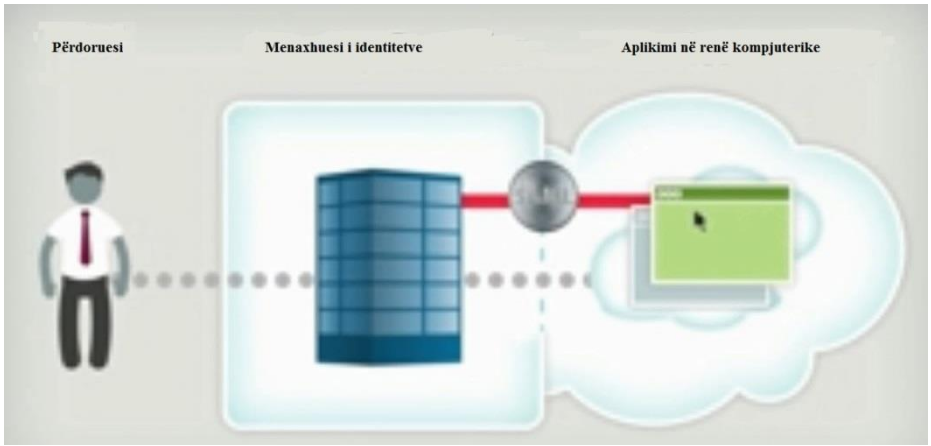
derivohen nga certifikatat lëshuar një entiteti të caktuar me pseudonime të ndryshme. Nga një certifikatë e vetme mund të krijohen disa kredenciale private, nga ku është e pamundur të gjendet lidhja e këtyre të fundit me njëra-tjetrën si edhe me certifikatën master. Kredencialet private sigurojnë anonimitetin e një entiteti, për sa kohë nuk ka ndonjë keqpërdorin të tyre nga vetë entiteti [38].

Entitetet që përdorin aplikime të ndryshme në retë kompjuterike, përdorin një protokoll miks që u lejon atyre të zgjedhin disa nga atributet e ofruara nga një sistem identifikues identitetesh të jashtme, pa zbuluar të dhënat e tyre personale. Këto kredenciale më pas nënshkruhen duke përdorur infrastrukturën e çelësave publikë.

Një nga kufizimet e Prime, është fakti që shërbimet në retë kompjuterike duhet të instalojnë PRIME si shtresë të mesme në aplikimet e tyre, gjë që krijon pengesa në standardizimet e menaxhimit të identiteteve.

6.4. SAML (Security Assertion Markup Language)

SAML është një protokoll i standardizuar i përdorur për shkëmbim të dhënash të autentikuara dhe autorizuara. SAML është një standard i bazuar në mekanizmin e komunikimit XML duke shkëmbyer në mënyrë të sigurt identitete dixhitalë midis aplikimeve dhe organizatave të ndryshme. Nga përparësitë kryesore të SAML, janë aftësia për të eliminuar fjalëkalimet e shumta që duhet të mbajë mend një përdorues dhe hyrja në sistem vetëm një herë dhe më pas aksesi në aplikime dhe shërbime pa përdorur kredenciale të tjera. Vetia e dytë e njohur si *Single Sign On (SSO)*, është shumë e dëshirueshme në një sistem të shpërndarë me aplikime dhe shërbime.



Figurë 6.4 Koncepti i SAML

Në vend të fjalëkalimeve, aplikimet që përdorin SAML pranojnë identifikues sigurie të cilët përmbajnë vetëm çka është e nevojshme për të pasur akses tek aplikimi. Meqë nuk transmetohen fjalëkalimet, nuk ka asgjë për t'u shqetësuar për klientët, partnerët ose punonjësit në rast se ata harrojnë, humbasin ose u vidhen fjalëkalimet.

Një përdorues hyn në rrjetin e brendshëm të kompanisë së tij me kredencialet e krijuara nga administratori i kompanisë dhe kur përdoruesi klikon një link të caktuar për akses tek aplikimi i dëshiruar, menaxhuesi i identiteteve krijon një XML dhe ia dërgon aplikimit në re. Është XML që i jep akses përdoruesit në aplikimin e kërkuar,

por XML nuk përmban asnjë lloj informacioni që mund të përdoret nga ndërhyrës për akses të paautorizuar në aplikacion [40].

6.5. Shërbimi SSO për Google Apps

Menaxhimi i identiteteve në Google është një model i bazuar rreth entitetit dhe u jep kompanive partnere një kontroll më të madh mbi autorizimin dhe identifikimin e përdoruesve të hostuar në shërbimet web të aplikimeve Google.

Modeli SAML u ofron partnerëve të Google mundësinë të jenë ata menaxhues të identiteteve duke kontrolluar emrat e përdoruesve, fjalëkalimet dhe informacione të tjera të përdorura për të identifikuar, autentifikuar dhe autorizuar përdoruesit për aplikimet e hostuara në Google [34].

SAML funksion në këtë mënyrë:

1. Përdoruesi tenton të aksesojë një aplikim ose servis të hostuar në Google.

2. Google krijon një kërkesë për autentifikim në formatin e kërkuar nga SAML. Kërkesa SAML kodohet dhe i bashkëngjitet URL-s së shërbimit SSO të hostuar në Google.

3. Google i dërgon përdoruesit një link automatik që përmban kërkesën e koduar SAML për t'u postuar tek ndërfaqja SSO e aplikimit.

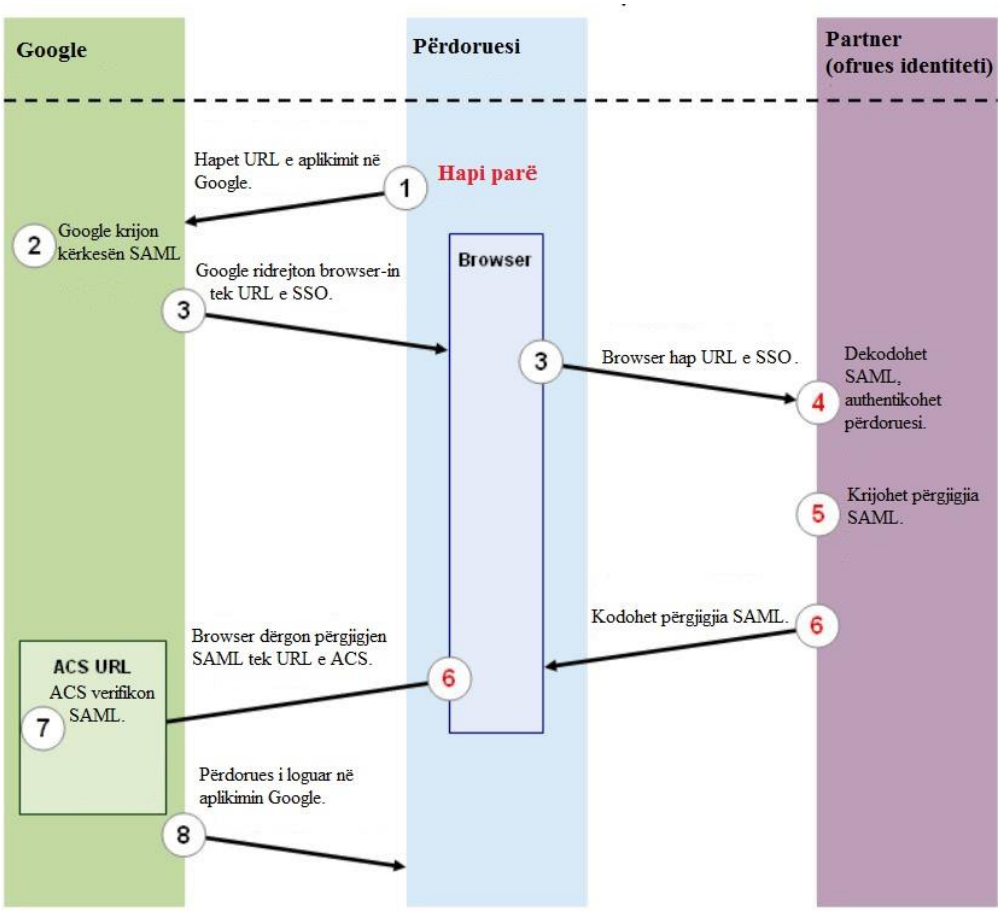
4. Aplikimi dekodon kërkesën për autentifikim SAML të postuar nga browser i përdoruesit, duke lexuar URL-n e Google, ACS (Assertion Consumer Service), së bashku me URL-n finale të përdoruesit. Aplikimi më pas identifikon përdoruesit, ose duke u kërkuar atyre kredencialet e nevojshme, ose duke kontrolluar për sesione të vlefshme të bazuara në "cookies".

5. Shërbimi partner i Google krijon një përgjigje SAML që përmban emrin e përdoruesit të identifikuar. Kjo përgjigje më pas nënshkruhet me një firmë dixhitale me çelësat publikë dhe privatë DSA/RSA të partnerit.

6. Shërbimi partner kodon përgjigjen SAML dhe ia dërgon përdoruesit në browser-in e tij. Partneri i Google përdor një mekanizëm me anë të cilit, përdoruesi ia rinis përgjigjen SAML shërbimit ACS të Google, p.sh me anë të një forme HTML, ku përdoruesi ka një buton me anë të të cilit mund të postojë formën që përmban përgjigjen SAML.

7. ACS verifikon përgjigjen SAML duke përdorur çelësin publik të shërbimit partner. Nëse verifikimi është i suksesshëm, ACS e ridrejton përdoruesin në destinacionin final.

8. Përdoruesi quhet tashmë i loguar në shërbimin e Google Apps.



Figurë 6.5 Hapat e transaksioneve SAML

6.6. Force.com

Dy janë mekanizmat bazë që kontrollojnë aksesin e përdoruesve në platformën e Force.com: profilet dhe rregullat e ndarjes.

Një profil është një template që përmban disa rregulla të paracaktuara që vendosin se çfarë mund të aksesojë një përdorues me platformën. Profilet janë rregulla të detajuara me anë të cilave një përdorues lejohet të aksesojë ose jo një aplikim të caktuar apo pjesë të veçanta të një aplikimi.

Përdoruesit e Force.com duhet të autentikohen me anë të një emri dhe fjalëkalimi të cilat ruhen në databazat e Salesforce. Përdoruesi me anë të formës së log-in, vendos kredencialet vetëm një herë e më pas akseson nëpërmjet profilit të vet, aplikimet e lejuara si Salesforce CRM, Portals etj, pa rivendosje të kredencialeve.

Kur një përdorues përdor një aplikim të hostuar jashtë platformës SaleForce, krijohet një sesion për llogari të përdoruesit me anë të cilit mbahet komunikimi me platformën. Për krijimin e sesionit, zakonisht kërkohen dhe ruhen më pas kredencialet e përdoruesit. Platforma e Force.com gjithashtu kërkon që aplikimet e jashtme që lidhen me platformën, të dërgojnë një identifikues sigurie për llogari të përdoruesit. Për të kontrolluar dhe ulur rrezikun e ekspozimit të fjalëkalimeve, Force.com ofron dy alternativa për SSO [32, 56].

1. Autentifikim i deleguar ku një organizatë krijon një servis web të quajtur autoritet i deleguar (AD) që zëvendëson mekanizmin për të gjitha hyrjet në platformë. Përdoruesit fillimisht duhet të identifikohen në kompaninë e tyre dhe më pas kompania duhet të krijojë një sesion drejt SalesForce duke dërguar në URL emrin e përdoruesit së bashku me një identifikues sigurie për verifikim nga AD. Pas kësaj, përdoruesi mund të "lëvizë" midis shërbimeve të resë dhe kompanisë së tij pa vendosur kredencialet.

2. Autentifikim i federuar. Platforma e Force.com është në gjendje të verifikojë pohimet SAML dhe të krijojë një sesion për përdoruesit sipas rastit. Krahasuar me autentikimin e deleguar, që kërkon nga organizata ose kompania e përdoruesit të ngrejë një shërbim që bën thirrjet e nevojshme API, SAML mund të dërgojë në mënyrë të sigurt të dhëna personale pa shkruar programe shtesë.

   Autentikimi i deleguar përdor si verifikues identitetesh shërbimin e brendshëm të kompanisë, si p.sh Active Directory, bazuar në protokolle autentikimi si NTML apo Kerberos, kurse në rastin e autentikimit të federuar, kompania duhet të ndërtojë një menaxhues të besueshëm identitetesh bazuar në SAML përpara se të përdorë shërbimet në re.

6.7. Federimi në Amazon Web Services (AWS)

AWS suporton SAML, gjë që bën të mundur një SSO të federuar dhe u lejon përdoruesve të hyjnë në ambientin e AWS ose të përdorin API nga një sistem menaxhues identitetesh si Active Directory Federation Services (ADFS).

Duke përdorur rolin AWS IAM, në vend të krijimit të llogarive për çdo përdorues të korporatës, mund të krijohet një rol AWS dhe më pas të lidhet me një rol në Active Directory. P.sh një përdorues mund të jetë pjesë e disa grupeve të sigurisë në Active Directory dhe këto grupe reflektojnë edhe të drejtat që përdoruesi ka në shërbimet e Amazon si p.sh EC2 apo S3. Në përgjithësi, shërbimet e Amazon me anë të politikave të kompanisë, mund të lidhen me një menaxhues identitetesh të besueshme çfarëdo.

Procesi i identifikimit të përdoruesit është transparent për përdoruesin, meqë, SSO është krijuar së bashku me rolin IAM [33, 56].

6.8. Konkluzione

Menaxhimi i identiteteve mund të shikohet në tre aspekte. I pari do ishte ai nga një IDM drejt një reje kompjuterike, pra transferimi nga një klient drejt një reje. I dyti do ishte transferimi i informacionit nga një re drejt një IDM-je dhe i treti do ishte menaxhimi i identiteteve nga një re kompjuterike drejt një tjetre.

Nga autorë dhe studiues të ndryshëm arrihet në përfundimin se nuk ka një përgjigje të saktë në atë që një IDM është i duhur në të gjitha kontekstet. Menaxhimi i identiteteve shikohet si një sfidë më vete në problemet e reve kompjuterike, saqë shumë ofrues të SaaS kanë ndërtuar dhe krijuar funksionet IAM si për shembull duke aplikuar API për sisteme të federuar e duke ndërtuar diçka që i ngjason SSO.

Trendi tjetër ka të bëjë me lulëzimin e tregjeve IAMaaS, ose IAM si një shërbim, ku ofrues të ndryshëm kanë ndërtuar funksionet IAM nga ose drejt reve kompjuterike.

Në aspektin e autentikimit, SAML ka rezultuar si "fituesi" në garën e federimit të identiteteve për shkak se ofron funksionet SSO. OpenID bazuar në protokollin Oauth 2.0, rezulton të jetë i suksesshëm.

Literatura

[1] Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. “Above the Clouds” A Berkeley View of Cloud Computing. Technical Report. Uni-versity of California at Berkeley 2009.

[2] Cloud Security Alliance. (2009). “Security Guidance for Critical Areas of Focus in Cloud Computing”.

[3] Foster I, Kesselman, C, Tuecke S (2001) “The Anatomy of the Grid: Enabling Scalable Virtual Organization”. International Journal of High Performance Computing Applications 15(3):200-222

[4] Gens, F., (2010). “IDC on ‘the Cloud’: Get Ready for Expanded Research”, hapur mars 2014, gjendet tek:

http://blogs.idc.com/ie/?p=189

[5] Gartner (2008). “Gartner Says Cloud Computing Will Be As Influential As E-business”. Gartner press re-lease, 26 June 2008”.

[6] A. Stewart Fotheringham, Peter A. Rogerson “GIS and spatial analytical problem”, INT. J. GEOGRAPHICAL INFORMATION SYSTEMS, 1.993,VOL.7, NO. 1, 3-19.

[7] Shahab Fazal “GIS Basic” ISBN : 978-81-224-2376-1 Publication Year : May, 2008 Edition.

[8] Bill Kropla "Beginning MapServer-Open Source GIS Development" ISBN (pbk): 1-59059-490-8, 2005 Edition.

[9] Philip O'Doherty. “Cloud computing: Future belongs to 'GIS as a Service’” Geospatial World: October 2010, available: http://www.geospatialworld.net/Paper/Technology/ArticleView.aspx?aid=18700

[10] David W. S. Wong and C. Victor Wu, 1996, “Spatial Metadata and GIS for Decision Support, “Proceedings of the 29th Annual Hawaii International Conference on System Sciences - I996 IEEE.

[11] W.K. Chan, Lijun Mei, and Zhenyu Zhang, “Modelling and testing of cloud applications,” In: Proceedings of 2009 IEEE Asia-Pacific Services Computing Conference (APSCC 2009), (Singapore, December 7-11, 2009), IEEE Computer Society Press, Los Alamitos, CA, USA, 2009.

[12] B.P. Rimal, E. Choi, I. Lumb, A taxonomy and survey of cloud computing systems, Fifth International Joint Conference on INC, IMS and IDC, (2009).

[13] G. Huerta-Canepa, D. Lee, A virtual cloud computing provider for mobile devices, Proceedings of the 1st ACM Workshop on Mobile Cloud Computing & Services Social Networks and Beyond -MCS ’10, No.6 (2010).

[14] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, A view of cloud computing, Communications of the ACM, 53, No.4 (2010).

[15] J. Kilian, Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, Proceedings, 2139, (2001), 213-229.

[16] Harold C. Lim, Shivnath Babu, Jeffrey S. Chase, Sujay S. Parekh, Automated Control in Cloud Computing: Opportunities and Challenges, ACDC '09 Proceedings of the 1st workshop on Automated control for datacenters and clouds, (2009), 13-18.

[17] R. Maggiani, Cloud Computing is Changing How we Communicate, Professional Communication Conference, 2009. IPCC 2009. IEEE International, (2009), 1-4.

[18] M. Blaze, G. Bleumer, M. Strauss, Divertible protocols and atomic proxy cryptography, In Proceedings of Eurocrypt '98, 1403, (1998), 127-144.

[19] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou, Ensuring data storage security in Cloud Computing, Quality of Service, 2009. IWQoS. 17th International Workshop on, (2009), 1-9.

[20] X. Zhang, Ensure Data Security in Cloud Storage, International Conference on Network Computing and Information Security, (2011).

[21] K. Krauter, R. Buyya, M. Maheswaran, A taxonomy and survey of grid re- source management systems for distributed computing, Software: Practice and Experience, 32, No.2 (2002), 135-164.

[22] D. Anand, V. Khemchandani, R. K. Sharma, Identity-Based Cryptography Techniques and Applications (A Review) 5th International Conference on Com- putational Intelligence and Communication Networks, (2013).

[23] G. Ateniese, K. Fu, M. Green, S. Hohenberger. Improved Proxy Re-encryption Schemes with Applications to Secure Distributed Storage, ACM Transactions on Information and System Security (TISSEC), 9, No.1 (2006), 1-30.

[24] J. Katz, J.Lindel, Introduction to Modern Cryptography, Chapman & Hall/CRC, USA (2008).

[25] A. Ivan, Y.Dodis, Proxy Cryptography Revisited, Proceedings of the Network and Distributed System Security Symposium, NDSS , (2003).

[26] D. Nunez, I. Agudo, J. Lopez, Integrating OpenID with proxy re-encryption to enhance privacy in cloud-based identity services, 4th IEEE International Conference on Cloud Computing Technology and Science Proceedings, (2012).

[27] H. Tianfield, Security Issues in Cloud Computing, IEEE International Conference on Systems, Man, and Cybernetics (SMC), (2012).

[28] C. Paar, J. PELZ Understanding Cryptography, Springer, USA (2010).

[29] Chan, L. Mei, Z.Zhang, Modeling and testing of cloud applications, Services Computing Conference, IEEE Asia-Pacific, (2009).

[30] W. Liu, Research on cloud computing security problem and strategy, 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), (2012).

[31] P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Ben Othmane, L. Lilien, M. Linderman, An Entity-Centric Approach for Privacy and Identity Management in Cloud Computing, 29th IEEE Symposium on Reliable Distributed Systems, (2010).

[32] P. Harding, P. Dingle, An Overview of Force.com User Management and Sign-on, SalesForce Developers Technical Library, (2014).
https://developer.salesforce.com/page/An_Overview_of_Force.com_User_Management_and_Sign-on

[33] AWS Identity and Access Management, Amazon Web Services, Inc. or its affiliates, (2014). http://aws.amazon.com/iam/

[34] Google Apps Platform, Google Developers, hapur tetor 2013, gjendet tek:

https://developers.google.com/google-apps/sso/saml_reference_implementation

[35] S. Clauß, M. Köhntopp, Identity management and its support of multilateral security, Computer Security, 37 (2011).

[36] W. Alrodhan, C. Mitchell, Improving the Security of CardSpace, EURASIP Journal on Information Security, (2009).

[37] D. Recordon, D. Reed, OpenID 2.0: A platform for user-centric identity management, Proc. of the second ACM workshop on Digital identity management, (2006), 11-16.

[38] R. Leenes, J. Schallaböck, M. Hansen, PRIME white paper, (2008), www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf

[39] M. Hansen, A. Schwartz, A. Cooper, Privacy and Identity Management, Security & Privacy IEEE, 6 (2008).

[40] J. Hughes, E. Maler, Security Assertion Markup Language (SAML) V2.0 Technical Overview, (2005), hapur nëntor 2013, gjendet tek:
http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

[41] S. Sun, K. Hawkey, K. Beznosov, Systematically breaking and fixing OpenID security: Formal analysis, semi-automated empirical evaluation, and practical countermeasures, Computers & Security, 31 [2012].

[42] S. Pearson, Taking account of privacy when designing cloud computing services, Proc. CLOUD '09 of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing, IEEE Computer Society, (2009).

[43] V. Bertocci, G.Serack, C. Baker Understanding Windows CardSpace: An Introduction to the Concepts and Challenges of Digital Identities, Addison-Wesley, US, 2007.

[44] S. Rieger, User-Centric Identity Management in Heterogeneous Federations, Fourth International Conference on Internet and Web Applications and Services. (2009).

[45] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, You, Get Off My Cloud: Exploring Information Leakage in Third Party Compute Clouds, Y Proc. 6th ACM conference on Computer and Communications Security, Chicago, IL, Nov. 2009, pp. 199-212.

[46] R. Gellman, "Privacy in the clouds: Risks to privacy and confidentiality from cloud computing", The World Privacy Forum, 2009, hapur nëntor 2013, gjendet tek:
http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

[47] Jessica T., "Connecting Data Centres over Public Networks", IPEXPO.ONLINE, April 20, 2011.

[48] C. Roman, "Sony Data Breach Highlights Importance of Cloud Security", Cloud Times, May 9, 2011.

[49] F. Lombardi, R. Di Pietro, "Secure Virtualization for Cloud Computing", Journal of Network and Computer Applications, vol. 34, issue 4, pp. 1113- 1122, July 2011, Academic Press Ltd. London, UK.

[50] A. Bakshi, Y. B. Dujodwala, “Securing cloud from DDoS Attacks using Intrusion Detection System in Virtual Machine”, ICCSN ’10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.

[51] Eucalyptus web site, hapur dhjetor 2013, gjendet tek:

http://www.eucalyptus.com/

[52] W. Jansen, T. Grance, “NIST Guidelines on Security and Privacy in Public Cloud Computing”, Draft Special Publication 800-144, 2011.

[53] J. Karlin, S. Forrest, J. Rexford, “Autonomous Security for Autonomous Systems”, Proc. Of Complex Computer and Communication Networks; vol. 52, issue. 15, pp. 2908- 2923, Elsevier, NY, USA, 2008.

[54] Z. Brakerski and V. Vaikuntanathan, Efficient Fully Homomorphic Encryption from (Standard) LWE, FOCS 2011, IEEE 52nd Annual Symposium on Foundations of Computer Science, IEEE (2011), 97–106.

[55] A.Benusi, D.Hyka, A FRAMEWORK FOR SECURE DATA EXCHANGE IN MOBILE CLOUD COMPUTING, International Journal of Computing and Optimization, Vol.1, no,1-4, 2014. ISSN 2367-5594.

[56] A.Benusi, An Identity Management Survey on Cloud Computing, Int. Journal of Computing and Optimization, Vol. 1, 2014, no. 2, 63-71.

[57] A.Benusi, A.Golemi, “Usage of Cloud Computing platforms in Geographical Information Systems (GIS)”, Proc. of 4-th international conference; Information Systems and Technology towards a digital Economy, Tirana, June 15-16, 2013.