



**UNIVERZITET SINGIDUNUM  
DEPARTMAN ZA POSLE DIPLOMSKE STUDIJE**

**-MASTER STUDIJSKI PROGRAM-  
SAVREMENE INFORMACIONE TEHNOLOGIJE**

**Jelena Vujošević**

**Virtuelne platforme, bezbednosni problemi i  
njihova tehnička rešenja**

**-Master rad-**

**Mentor:  
Prof. dr Mladen Veinović**

**Student:  
Jelena Vujošević  
Br. indeksa: 410104/2010**

## **Virtuelne platforme, bezbednosni problemi i njihova tehnička rešenja**

### **Sažetak**

U ovom radu opisan su pojam virtualizacije, tipovi virtualizacije, njena softverska rešenja i arhitektura, kao i prednosti koje pruža. Pojam virtualizacije se prvi put pojavljuje 60-tih godina prošlog veka. Ona predstavlja novu revoluciju na polju informatičkih tehnologija. U ovom radu opisan je pojam Cloud computing-a, kao poslednji korak u razvoju virtuelizacije, njegove karakteristike, modeli servisa, arhitektura kao i prednosti, mane i problemi koje cloud computing kao model sa sobom nosi. Virtuelizacija i Cloud computing su sadašnjost i budućnost savremenih informacionih tehnologija. Njihova primena je svestrana kako u aktivnostima organizacija i poslovnim procesima tako i u aktivnostima fizičkih lica-običnih korisnika. Takođe u radu je stavljen akcenat na sigurnosne rizike i probleme bezbednosti koje ovi inoformatički modeli nose sa sobom i tehnike zaštite kojima se one nastoje rešiti.

Ključne reči: virtualizacija, softverska rešenja, arhitektura, VMM, supervisor, VPN, Cloud computing, servisni modeli, SaaS, IaaS, PaaS, bezbednost, arhitektura, IPsec protokol, SSL protokol, Cloud Security Alliance (CSA)

### **Abstract**

In this paper are described a virtualization phenomenon and its advantages, types of virtualization, its architecture and relating softwer solutions. The concept of virtualization in the IT world appears for the first time during the 1960s. It represents a new revolution in the IT field. In this paper is described a phenomenon of cloud computing, as the latest step in the development of virtualization, it's characteristics, service models, architecture, as well as advantages, disadvantages and problems of it's application. Virtualization and Cloud computing are one of the key foundations of modern IT development in the future. It's application is versatile and it encompasses the fields of public, bussines and private informatic technologies. Also, this paper deals with security risks and problems related with the implementation of virtualization and cloud computining and with the security techniques developed in order to sovre them.

Key words: virtualization, software solutions, architecture, VMM, supervisor, VPN, Cloud computing, service models, SaaS, IaaS, PaaS, security, architecture, IPsec protocol, SSL protocol, Cloud Security Alliance (CSA)

## Sadržaj

|        |                                                                                                          |    |
|--------|----------------------------------------------------------------------------------------------------------|----|
| 1.     | Metodologija istraživačkog projekta.....                                                                 | 5  |
| 1.1.   | Uvodne napomene i obrazloženje rada .....                                                                | 5  |
| 1.2.   | Predmet istraživanja.....                                                                                | 5  |
| 1.3.   | Cilj i zadaci istraživanja.....                                                                          | 5  |
| 1.4.   | Istraživačke hipoteze.....                                                                               | 5  |
| 1.5.   | Struktura rada.....                                                                                      | 6  |
| 1.6.   | Metodi istraživanja i tok istraživačkog procesa.....                                                     | 7  |
| 2.     | Pojam i istorijat virtuelizacije .....                                                                   | 7  |
| 3.     | Tipovi virtuelizacije i softverska rešenja .....                                                         | 8  |
| 3.1.   | Tipovi virtuelizacije .....                                                                              | 8  |
| 3.1.1. | Hardverska virtuelizacija .....                                                                          | 9  |
| 3.1.2. | Softverska virtuelizacija.....                                                                           | 11 |
| 3.1.3. | Virtuelizacija memorije .....                                                                            | 13 |
| 3.1.4. | Storage virtuelizacija .....                                                                             | 13 |
| 3.1.5. | Mrežna virtuelizacija .....                                                                              | 14 |
| 3.2.   | Softverska rešenja .....                                                                                 | 17 |
| 3.2.1. | Vmware.....                                                                                              | 17 |
| 3.2.2. | Citrix Systems Xen .....                                                                                 | 18 |
| 3.2.3. | Oracle VM VirtualBox (Sun Microsystems Virtualbox).....                                                  | 19 |
| 3.2.4. | Microsoft virtuelizaciona rešenja.....                                                                   | 20 |
| 4.     | Prednosti virtuelizacije.....                                                                            | 22 |
| 5.     | Arhitektura virtuelizacije .....                                                                         | 24 |
| 6.     | Cloud computing – poslednji korak u razvoju virtuelizacije .....                                         | 26 |
| 6.1.   | Pojam i definicija cloud computing-a .....                                                               | 26 |
| 6.2.   | Karakteristike cloud computing-a.....                                                                    | 27 |
| 6.3.   | Servisni modeli cloud computing-a .....                                                                  | 28 |
| 6.4.   | Modeli cloud computing-a prema klasifikaciji .....                                                       | 29 |
| 6.5.   | Prednosti i mane cloud computing-a.....                                                                  | 30 |
| 6.6.   | Cloud computing arhitektura .....                                                                        | 33 |
| 6.7.   | Cloud computing provajderi i uslovi pružanja usluga .....                                                | 33 |
| 7.     | VPN kao najčešće primenjivani oblik Desktop virtualizacije, bezbednosni problemi i njihova rešenja ..... | 37 |
| 7.1.   | Bezbednost.....                                                                                          | 38 |
| 7.2.   | IPsec bezbednosni protokol .....                                                                         | 39 |
| 7.2.1. | Tunelovanje.....                                                                                         | 39 |
| 7.2.2. | Transport mode .....                                                                                     | 40 |
| 7.2.3. | Tunnel mode .....                                                                                        | 40 |
| 7.3.   | SSL protokol za zaštitu VPN .....                                                                        | 40 |
| 7.3.1. | Slabosti i ranjivosti SSL protokola .....                                                                | 44 |
| 7.3.2. | Komunikacija na bezbedan način .....                                                                     | 47 |
| 8.     | Bezbednost u cloud computing-u.....                                                                      | 50 |
| 9.     | Cloud Security Alliance (CSA) .....                                                                      | 51 |
| 9.1.   | Zloupotreba cloud computing-a.....                                                                       | 52 |
| 9.2.   | Nesigurni interfejs i API .....                                                                          | 53 |
| 9.3.   | Zlonamerni korisnici koji napade izvode "iznutra".....                                                   | 53 |
| 9.4.   | Zajednički tehnološki problemi .....                                                                     | 54 |
| 9.5.   | Gubitak i neovlašćeno otkrivanje podataka.....                                                           | 54 |

|                                    |    |
|------------------------------------|----|
| 9.6. Krađa korisničkih imena ..... | 55 |
| 9.7. Nepoznati profil rizika ..... | 56 |
| Zaključak.....                     | 57 |
| Literatura.....                    | 59 |

## **1. Metodologija istraživačkog projekta**

### **1.1. Uvodne napomene i obrazloženje rada**

Projektni zadatak ima za cilj da definiše pojam virtualizacije, tipove i arhitekturu, kao i softverska rešenja koja ih prate, pojam cloud computing-a kao poslednjeg koraka u razvoju virtualizacije, kao i bezbednosne probleme koje virtualizacija i cloud computing donose i njihova tehnička rešenja. Težište rada je na značaju koji virtualizacija ima u savremenom poslovanju kao i na prednostima ali i bezbednosnim rizicima koje nosi sa sobom. Projektni zadatak je izrađen korišćenjem teoretskih i praktičnih znanja iz oblasti virtualizacije i cloud computing-a, kao i oblasti koje se bave nedostacima i performansama ovih fenomena.

### **1.2. Predmet istraživanja**

Predmet istraživanja je fenomen virtualizacije kao revolucionarni pomak u IT svetu. Takođe, težište rada je na bezbednosnim problemima virtuelnih platformi i njihovim tehničkim rešenjima prilikom implementacije u poslovni svet.

Ključna pitanja na koja su se tražili odgovori prilikom istraživanja su:

- Šta je virtualizacija?
- Koji su tipovi virtualizacije?
- Sta je VPN?
- Bezbednost u VPN i tehnička rešenja?
- Koja su softverska rešenja virtualizacije?
- Arhitektura virtualizacije
- Značaj virtualizacije
- Sta je Cloud computing?
- Koji su bezbednosni problem Cloud computing-a?
- Šta je Cloud Security Alliance(CSA)?
- Ko su provajderi Cloud computing usluga i kako obezbeđuju sigurnost korisnicima?
- Arhitektura Cloud computing-a
- Značaj cloud computing-a

### **1.3. Cilj i zadaci istraživanja**

Cilj istraživanja je da se istakne značaj primene virtualizacije u poslovnom svetu. Zadaci istraživanja su bili da se sagledaju svi oblici i aspekti virtualizacije kao i mane, prednosti i bezbednosni rizici koje oni sa sobom nose, kao i tehnička rešenja u borbi protiv bezbednosnih problema.

### **1.4. Istraživačke hipoteze**

- Na pojavu virtualizacije uticala je potreba za efikasnijom organizacijom poslovnih procesa i organizacija. Virtualizacija je doprinela: smanjenju

troškova električne energije, oslobađanju fizičkog prostora, konsolidaciji servera, lakšoj implementaciji aplikacija u organizacije, testiranju softvera itd.

- Virtualizacija je danas prisutna gotovo na svim poljima IT tehnologije. U skladu sa tim ona je poprimila različite pojavne oblike: hardverska, softverska, memoriska, storage virtualizacija, virtualizacija podataka, virtualizacija mrežnih resursa.
- U vreme kada Internet zauzima značajno mesto u privatnoj i poslovnoj komunikaciji, VPN i sa njim povezani bezbednosni rizici dobijaju sve važniju ulogu u razvoju IT.
- Kao poslednji korak u razvoju virtualizacije, pojam Cloud computing-a, javlja se poslenjih decenija, a njegov značajniji razvoj, prihvatanje i implementacija desio se tek u poslednjih 4-5 godina.
- Sa pojavom virtualizacije i Cloud computing-a, javljaju se bezbednosni problemi komunikacije, razmene podataka, čuvanja podataka, zaštite podataka, pouzdanosti, a samim tim se javlja potreba za razvojem različitih tehničkih rešenja kako bi se na odgovarajući način izašlo u susret ovim potrebama.
- Virtualizacija će u budućnosti težiti da postane standard u IT svetu, a njena primena će biti svestrana kako u aktivnostima organizacija tako i u aktivnostima fizičkih lica.

## 1.5. Struktura rada

Rad je podeljen u deset celina.

- U okviru prve celine obrađeni su pojam i istorijski razvitak virtualizacije.
- Druga celina rada bavi se tipovima virtualizacije. U okviru ove celine prikazani su: virtualizacija hardvera, softvera, memorije, storage-a, podataka i mrežnih resursa.
- Treća celina posvećena je softverskim rešenjima na koje se oslanja virtualizacija. Detaljnije su obrađeni različiti softveri za virtualizaciju: VMware, Xen, VirtualBox, Microsoft virtualizaciona rešenja.
- Četvrta celina rada bavi se prednostima koje virtualizacija nosi sa sobom. Analizirani su: konsolidacija, pouzdanost, sigurnost i efikasnost.
- Peta celina posvećena je arhitekturi virtualizacije. Objašnjeni su radni i zaštićeni mod arhitekture u virtualizaciji kao i prstenasta struktura.
- U okviru šeste celine opisana je pojava Cloud computing-a kao poslednjeg koraka u razvoju virtualizacije. Takođe, opisani su pojam, karakteristike, servisni modeli kao i modeli klasifikacije Cloud computing-a, njegova arhitektura i prednosti i mane koje Cloud computing kao model donosi.
- U sedmoj celini opisan je VPN kao najčešće primenjivani oblik desktop virtuelizacije u vremenu kada je Internet zauzima značajno mesto u privatnoj i poslovnoj komunikaciji. Takođe, sedma celina se bavi bezbednosnim problemima i rizicima u VPN-u, kao i IPsec i SSL bezbednosnim protokolima.
- Osma celina rada posvećena je bezbednosnim problemima u Cloud computing-u.
- Deveta celina objašnjava nastanak Cloud Security Alliance organizacije i koja je njihova uloga.

- Poslednja celina posvećena je provajderima Cloud computing usluga, njihovim uslovima pružanja usluga i sistemima zaštite korisničkih podataka.

## 1.6. Metodi istraživanja i tok istraživačkog procesa

U toku izrade rada primenjeni su sledeći metodološki procesi: prikupljanje raspoložive dokumentacije i relevantnih podataka, deskriptivna metoda, komparativne metode, kvalitativne metode i metoda prikaza.

## 2. Pojam i istorijat virtuelizacije<sup>1</sup>

Pojam virtualizacija prvi put se pojavljuje tokom 60-ih godina prošlog veka. Virtualizacija je tehnologija koja predstavlja kombinaciju hardvera i softvera. Ona omogućava da se na jednom fizičkom računaru pokrene više međusobno nezavisnih i različitih operativnih sistema (Microsoft, Linux, Unix...). Sta to zapravo znači? Nezavisnost se ogleda u tome da aplikacije ili programi pokrenuti na jednom sistemu ne mogu uticati na rad drugog, pa pri recimo padu jednog virtuelnog operativnog sistema, posledice po druge virtuelne ili host OS ne bi postojale. Dakle stvar je ista kao kada bi postojalo 5 računara na kojima bi funkcionisalo 5 nezavisnih operativnih sistema. Naravno da stvar nije potpuno ista, jer u slučaju virtuelizacije računar deli resurse (memoriju, skladište podataka, itd.) među virtuelnim računarima.

Pojam virtuelna mašina, kao termin, prvi put je upotrebila firma IBM. To je bio projekat M44/44X. Glavna mašina je bila IBM 7044 (M44) i nekoliko simuliranih 7044 virtuelnih mašina koje su zajedno koristile hardvere i softvere, kao i virtuelnu memoriju u službi multi programiranja. Takav centralni sistem podržavao je istovremeno izvršavanje većeg broja programa. Obzirom na to da je hardverska oprema tada bila veoma skupa, virtuelizacija kao rešenje je donosila značajno smanjenje finansijskih troškova. IBM je jedna od firmi koja je dala najveći doprinos u razvoju tehnologija virtualizacije. Prvi CTSS (engl. *Compatible Time Sharing System*) sistemi razvijeni su upravo na njihovim računarima. Pošto je ovaj sistem omogućio deljenje hardvera računarskog sistema među različitim korisnicima (ljudi ili programa), više različitih zadataka moglo se obavljati istovremeno. To je predstavljalo značajan pomak u pogledu funkcionalnosti. IBM dalje razvija računare čiji je hardver podržavao virtualne sisteme kao i odgovarajuće virtualne platforme. Neki od tih sistema bili su CP-40 sistem za IBM 360/40 računare, CP-67 sistem za IBM 360/67 računare... . IBM-ove virtualne mašine simulirale su IBM-ov hardver, identičan onom na kakvom su se pokretale dok se *Virtual Machine Monitor* interfejs izvršavao direktno na hardveru. IBMov VM/370 sa kraja 60-ih godina najsličniji je

---

<sup>1</sup> Videti detaljnije Lian Proven, [A Brief History of Virtualisation](#) (Kindle Edition), The Register, 2011

savremenoj virtuelizaciji. Osnovna ideja je bila da na jednom računarskom sistemu istovremeno rade različite instance operativnih sistemima. Savremena virtualizacija dovela je do toga da skupe mainframe sisteme zamene računarski sistemi. Svaka OS instanca deli raspoložive resurse dostupne na fizičkom hardware-u.

Tokom 80-ih i 90-ih godina prisutnost virtualizacije opada. Osnovni razlog ovome bila je pojava i razvoj 32-bitne arhitekture koja je sa sobom nosila ekspanziju i složenost programa koji će biti zastupljeni. Samim tim raste i fizička iskorišćenost računara pa će se distribuirano programiranje i klijent-server arhitektura na više umreženih računara pokazati kao bolje rešenje od virtualizacije.

Međutim, sa pojavom x86-bitne arhitekture virtualizacija se opet javlja kao idealno rešenje. U poslednjih desetak godina beleži se stalni rast razvoja virtualizacije. Smatra se da će do kraja druge decenije XXI-og veka virtualizacija biti standard u IT svetu i težiti da bude zastupljena u svim oblicima poslovanja.

Virtuelizacija predstavlja jedan od ključnih instrumenata kojima se služi Cloud computing. Pojavljivanje cloud computing-a kao poslovnog koncepta i samog termina vezuje se za poslednju deceniju, a njegov značajniji razvoj i prihvatanje od strane šire informatičke zajednice desio se tek u poslednjih 4-5 godina. Cloud computing se smatra poslednjim korakom u razvoju virtualizacije.

### **3. Tipovi virtuelizacije i softverska rešenja**

#### **3.1. Tipovi virtuelizacije**

Virtualizacija, u računarstvu, predstavlja stvaranje virtuelne verzije nečega, kao što su hardverska platforma, operativni sistem, hard disk ili mrežni resursi. S toga razlikujemo šest vrsta virtualizacije.

Virtualizacija:

- Hardvera
- Softvera
- Memorije
- Hard diska ili storage-a
- Podataka
- Mrežnih resursa

### 3.1.1. Hardverska virtualizacija

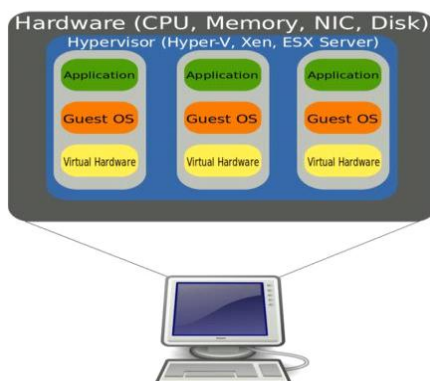
Hardverska virtualizacija ili platformska virtualizacija odnosi se na stvaranje virtualnih mašina koje rade kao pravi računari sa operativnim sistemom. Izvršni softver na ovim virtualnim mašinama je odvojen od osnovnih hardverskih resursa. Kod hardverske virtualizacije srećemo dva pojma *host* mašina i *guest* mašina. Termin *host*(domaćin) mašina odnosi se na stvarnu mašinu na kojoj se odvija virtualizacija. Termin *guest*(gost) mašina odnosi se na virtualnu mašinu. Pridevi *domaćin* i *gost* se takođe koriste za razlikovanje softvera koji je pokrenut na stvarnoj mašini i softvera koji je pokrenut na virtualnoj mašini. Hipervizor ili Virtual Machine Monitor je softver koji virtualna mašina kreira na hostu ili domaćinu.

Različiti tipovi hardverske virtualizacije uključuju:

- Potpunu virtualizaciju
  - Hardverski - potpomognuta virtualizacija
- Delimičnu virtualizaciju
- Para – virtualizaciju

#### *Potpuna virtualizacija*

Virtualne mašine su zasnovane na domaćin/gost paradigmi. Svaki gost se pokreće ili podiže na virtualnoj imitaciji hardverskog sloja. Ovo omogućava da se operativni sistem gosta izvršava bez ikakvih modifikacija. To takođe omogućava administratoru da kreira goste koji koriste različite vrste operativnih sistema. Gost nije svestan operativnog sistema domaćina jer nije pokrenut na stvarnom hardveru. To međutim zahteva prave resurse računara; Hipervizor se koristi za koordinaciju instrukcija sa CPU(*central processor unit*). On vrši validaciju svih CPU instrukcija izdatih od strane gosta i upravlja izvršnim kodom koji zahteva dodatne privilegije. Puna virtualizacija zahteva da se svaka istaknuta hardverska karakteristika reflektuje odnosno prenese na jednu ili više virtualnih mašina. To uključuje pun set instrukcija, input/output operacije, prekide, pristup memoriji, kao i sve druge elemente koje koristi softver pokrenut na host mašini, a koje su namenjene da se izvršavaju na virtualnoj mašini. Ne sme se dozvoliti da bilo koja virtualna operacija menja stanje bilo koje druge virtualne mašine, programa za kontrolu ili hardvera. Loša strana ovakve vrste virtualizacije jeste brzina izvršavanja virtualizovanih operativnih sistema i programa. Centralni procesor mora da simulira i dodatan hardver i to značajno utiče na performance ovakve konfiguracije. VMware i Microsoft Virtual Server koriste ovakav vid virtualizacije.



Slika 1. Potpuna virtualizacija

*Hardverski - potpomognuta virtualizacija* zapravo predstavlja način poboljšavanja efikasnosti hardverske virtualizacije. To uključuje uvođenje specijalno dizajniranih procesora i hardverskih komponenti u svrhu poboljšanja performansi okruženja gosta. Primeri ovih tehnologija za x86 arhitekture procesora su Intel VT (engl. *Virtualization Technology*) i AMD-V (engl. *AMD Virtualization*). Virtualna okruženja koja koriste hardversku podršku su VMware Workstation, Xen 3.x, Linux KVM i Microsoft Hyper-V. Problem kod ove vrste virtualizacije jeste potreba za posebnom hardverskom platformom kako bi se obezbedila i povećala efikasnost rada u virtualnim okruženjima.

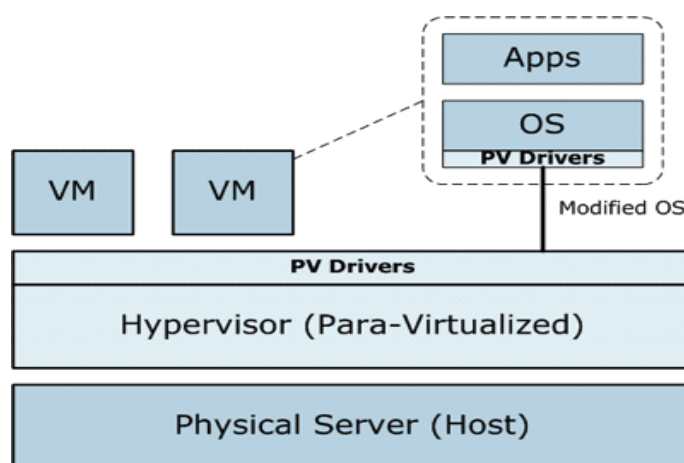
### *Delimična virtualizacija*

U slučaju delimične virtualizacije na virtualnoj mašini se ne može pokretati ceo operativni sistem kao što je to slučaj kod pune virtualizacije. Delimična virtualizacija međutim omogućava pokretanje velikog broja programa. Odvajanje adresnih prostora za virtualne mašine jedna je od osnovnih karakteristika ovog tipa virtualizacije. Svakoj virtualnoj mašini dodeljuje se poseban virtualni adresni prostor. Delimična virtualizacija predstavljala je važan istorijski korak na putu do ostvarivanja pune virtualizacije. Na primer on je korišćen u prvoj generaciji time-sharing sistema CTSS, kao i u IBM M44/44X eksperimentalnom (pejdžing) sistemu. Ova vrsta virtualizacije nije loše rešenje ukoliko je osnovni cilj deljenje memorijskih resursa između klijenata odnosno korisnika.

### *Para – virtualizacija*

Kod ovog tipa virtualizacije gostujući operativni sistem komunicira sa matičnim operativnim sistemom preko hipervizora takođe. Gostujući operativni sistem podatke o hardveru dobija direktno od matičnog operativnog sistema. Hipervizor zapravo izmeni kod operativnog sistema gosta. Ove modifikacije nazivaju se porting (portovanje). U tom slučaju drajveri gostujućeg operativnog sistema i drajveri

hipervozora se međusobno integrišu da bi efikasnije omogućili i delili pristup fizičkom uređaju. Na taj način simulacija kompletnog hardvera nije potrebna, pa su performanse drastično veće. Kako operativni sistem mora biti izmenjen (tako da može da komunicira sa matičnim operativnim sistemom) fleksibilnost takvog rešenja znatno je manja. Kao i kod pune virtualizacije i paravirtualne mašine takođe mogu koristiti više različitih operativnih sistema. Xen i UML koriste model para-virtualnih mašina.



Slika 2. Paravirtualizacija

### 3.1.2. Softverska virtualizacija

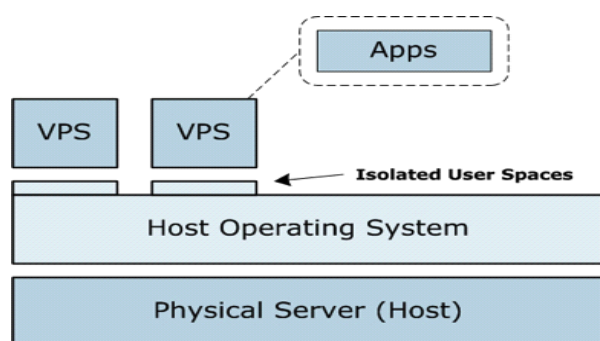
Postoje dva tipa softverske virtualizacije:

- Virtualizacija na nivou operativnog sistema
- Virtualizacija aplikacija

#### *Virtualizacija na nivou operativnog sistema*

Virtualizacija na nivou operativnog sistema funkcioniše malo drugačije. Ona se ne zasniva na domaćin/gost paradigmi. Domaćin pokreće jedan jedini OS kao osnovu i njegove funkcionalnosti prosleđuje i deli sa svim gostima. To dalje implicira da operativni sistem gosta mora biti isti onaj koji koristi domaćin. Ova vrsta virtualizacionog rešenja omogućava postojanje više izolovanih i sigurnih virtuelnih server koji rade kao zasebni serveri posmatrajući sa strane korisnika. Isto jezgro operativnog sistema se koristi za implementaciju okruženja gosta. Aplikacije koje su pokrenute u okruženju gosta posmatraju se kao samostalni sistemi. Problem kod ove vrste virtualizacije je taj što se ne mogu koristiti virtualni serveri s različitim operativnim sistemima. Neka od rešenja koja primenjuju virtualizaciju na nivou operativnog sistema su: Linux VServer, OpenVZFreeBSD Jail itd. Virtualne mašina

direktno koristi stvarni operativni sistem bez hardverskog ili programskog prevođenja virtualnih komandi u stvarne. Ovakav sistem rada omogućava neneraušavanje efikasnosti rada samih virtualnih mašina.



Slika 3. Virtualizacija na nivou OS

### *Virtualizacija aplikacija*

Virtualizacija aplikacija je relativno nov pojam u svetu virtualizacije. Virtualizacija aplikacija omogućava korisnicima da dobiju jednu ili više aplikacija koje nisu instalirane na glavnom operativnom sistemu računara koji koriste. Te aplikacije mogu biti specijalno spakovane i hostovane ili lokalno ili prenosno tako da izgleda kao da su zapravo instalirane i pokrenute normalno.

Ova vrsta virtualizacije ima sledeće prednosti:

- Aplikacijama koje su virtualizovane se dodeljuju posebna file-registry setovanja, čime se onemogućuje interferencija sa ostalim aplikacijama. Ovim se eliminiše problem koji može postojati između aplikacija. Primenom ovakvog virtualizacionog rešenja moguće je da se aplikacije različitih verzija pronađu na jednom operativnom sistemu.
- Često se primenjuje u slučaju testiranja aplikacija.
- Instalacija aplikacija u velikim računarskim okruženjima može biti komplikovana i dugo trajati. Primena i instalacija ovih aplikacija je maksimalno olakšana i ubrzana upotrebom virtualizacije aplikacija.
- Poboljšava se bezbednost, jer su aplikacije izolovane od operativnog sistema itd.

Ali i mane:

- Ne mogu se svi softveri virtualizovati. Jedan od tih primera su aplikacije koje zahtevaju drajvere.
- Neke vrste softvera kao što su anti-virus paketi teško je virtualizovati itd.

### 3.1.3. Virtuelizacija memorije

U informatici, virtualna memorija podrazumeva proces kojim se resursi RAM memorije u okviru jednog sistema baze podataka dele, a sa ciljem da se smeste u skladište virtualne memorije, odakle postaju dostupni svakom računaru sa klastera. Skladištu virtualne memorije pristupa se putem operativnog sistema ili aplikacija koje funkcionišu pod neposrednim okriljem operativnog sistema.

Memorijska virtualizacija omogućava mrežnim serverima da prevaziđu ograničenja koja im nameće fizička memorija, deleći zajedničko virtuelno memorijsko skladište. Memorijska virtualizacija omogućava bolje funkcionisanje aplikacija, jer stavlja na raspolaganje veliku količinu memorije za poboljšanje njihovih performansi, povećava efikasnost korišćenja raspoložive memorije, iskorišćenosti sistema itd.

Prednosti:

- Poboljšava iskorišćenost memorije kreiranjem zajedničkog virtualnog memoriskog skladišta
- Povećava efikasnost i skraćuje vreme operisanja složenih I/O aplikacija
- Omogućava aplikacijama na različitim serverima da dele podatke bez dodatnog opterećenja fizičke memorije

### 3.1.4. Storage virtuelizacija

Virtualizacijom serverskih i desktop sistema, podaci kojima oni operišu su uskladišteni lokalno na tim sistemima. Ovakav tip skladištenja podataka poznatiji je kao DAS – Direct Attached Storage sistem. Ovakav tip skladištenja podataka može biti vrlo problematičan u virtualizovanim sistemima.

Upravljanje lokalnim skladištenjem podataka na većem broju virtualizovanih sistema može biti pravi izazov i izvor problema. Bolji pristup ovom segmentu virtualizacije može se pronaći u centralizovanim virtualnim skladištima podataka što je forma virtualizovanih storage sistema.

Izdvajaju se sledeće prednosti virtualnih storage sistema:

- Bolja iskorišćenost storage resursa - na centralnoj lokaciji storage virtualizacija dodeljuje potreban prostor za podatke virtualnim mašinama i time se otklanjaju problemi sa neujednačenim korišćenjem kapaciteta.
- Laka proširivost storage kapaciteta – povećanje skladištenog prostora se vrši samo na jednoj centralnoj lokaciji .
- Efiaksnije upravljanje resursima storage sistema - organizacijama je lakše da upravljaju podacima, viši je nivo njihove bezbednosti od gubitka i lakše je uraditi proces bekapovanja kada su podaci skoncentrisani na jednoj centralnoj lokaciji.

### 3.1.5. Mrežna virtualizacija

Mrežna virtualizacija je metod koji se koristi za kombinovanje resursa računarske mreže u jedinstvenu platformu, poznatu kao virtualnu mrežu. To se postiže softverom i uslugama koji omogućavaju deljenje storage-a, propusnog opsega, aplikacija i drugih mrežnih resursa. Virtualna mreža tretira sve hardvere i softvere u mreži kao jedan skup resursa kojima se može pristupiti bez obzira na fizičke granice. Jednostavno rečeno virtualizacija mreže omogućava svakom ovlašćenom korisniku da deli resurse mreže sa jednog računara.

Mrežna virtualizacija razlikuje dva osnovna oblika:

- Platformska ili "serverska virtualizacija"
- Desktop virtualizacija

#### *Platformska ili „serverska” virtualizacija*

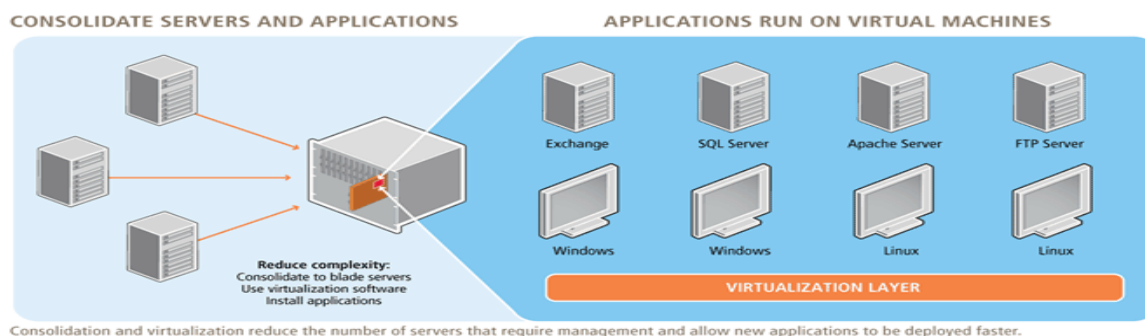
Serverska virtualizacija je zapravo maskiranje serverskih resursa, uključujući broj i identitet individualnih fizičkih servera, procesora, operativnih sistema od korisnika servera. Administrator servera koristi softversku aplikaciju kako bi podelio jedan fizički server na više izolovanih virtualnih okruženja. Virtualna okruženja se ponekad nazivaju virtualni privatni serveri, ali se najčešće nazivaju "gosti", instance, kontejneri ili emulacije.

Postoje tri popularna tipa pristupa virtualizaciji servera:

- Model virtualnih mašina ili takozvani model pune virtualizacije
- Model para- virtualizacije
- Model virtualizacije na nivou operativnog sistema

Sva tri tipa virtualizacije su detaljno objašnjena u okviru hardverske virtualizacije.

Serverska virtualizacija se može posmatrati kao deo sveukupnog trenda virtualizacije u IT preduzećima koja uključuju storage virtualizaciju, mrežnu virtualizaciju i menadžment upravljanja poslom. Ovaj trend je jedna od najbitnijih karika u razvoju autonomnog računarstva. Korisnost serverske virtualizacije je višestruka. Ona se može koristiti da bi se eliminisale potrebe za većim brojem fizičkih servera, da bi se obezbedila bolja iskorišćenost serverskih resursa, da se poboljša dostupnost servera, da se centralizuje administracija servera itd.



Slika 4. Platformska ili „serverska“ virtualizacija

### Desktop virtualizacija

Desktop virtualizacija (ponekada se naziva *klijentska virtualizacija*) kao koncept razdvaja desktop okruženje personalnih računara od fizičkih mašina korišćenjem klijent-server modela. Model čuva virtualizovani desktop na udaljenom centralnom serveru umesto na lokalnom hard disku udaljenog klijenta. Stoga kada korisnici rade na svojim udaljenim desktop-ovima, svi programi, aplikacije, procesi i podaci su pokrenuti i zadržani centralno. Ovakav tip virtualizacije omogućava klijentima da pristupe svojim desktopovima sa bilo kojeg uređaja, bilo da su u pitanju tradicionalni personalni računari, laptop računari, smartphon-ovi ili tin klijenati. Jednostavno rečeno, virtualne mašine rade na serveru (za svakog klijenta) i klijenti se mogu povezati na svoje "kompjutere" korišćenjem remote desktop softvera.

Time Desktop virtualizacija obezbeđuje da veći broj korisnika putem mreže i nezavisno od geografske lokacije pristupa svojim zasebnim virtuelnim okruženjima koja su pri tome locirana na jednoj centralizovanoj lokaciji kao što su veliki data centri. Danas se sve veći broj poslovnih organizacija okreće desktop virtualizaciji. Korisnici pristupaju svojim podacima i aplikacijama na bezbedan način i bez rizika od gubitka podataka.

Slika 5. Desktop virtualizacija<sup>2</sup>

<sup>2</sup> Preuzeto sa <http://www.chriswolf.com/?cat=9&paged=2>

Najčešće korišćeni tipovi virtualizacije mreže su:

- Virtual LAN (VLAN) – Dodavanje novih računara u mrežu, kao i uvođenje u rad klijent-server aplikacija i multimedije povećava opterećenje mreže, što može dovesti i do ozbiljnih zastoja u radu. Suština rada Ethernet-a je u detekciji i izbegavanju kolizija paketa sa informacijama, pri čemu sa povećanjem mrežnog saobraćaja istovremeno raste i broj kolizija i pada efikasnosti mreže. VLAN koncept je smišljen da razreši ovaj problem, tj. da mreža ostane fizički povezana, ali da se smanji broj kolizija i nivo Broadcast i Multicast saobraćaja – “virtuelnom” podelom na manje delove. IEEE standard 802.1Q je razvijen da reši problem podele većih mreža na manje delove, tako da Broadcast i Multicast saobraćaj ne uzmu više propusnog opsega nego što je neophodno. Standard takođe obezbeđuje i dodatni nivo sigurnosti između segmenata mreže. Administratori najčešće primenjuju VLAN-ove, da bi kontrolisali broadcast domene, kao i da bi kontrolisali interakciju između uređaja na različitim mrežnim segmentima. VLAN je danas standard u primeni Ethernet mreža. Svaki VLAN segment koristi određeni deo fizičke strukture switch-a (memorija, bandwidth....)
- Virtual IP (VIP) – Virtuelna IP adresa predstavlja IP adresu koja nije dodeljena konkretnom uređaju ili mrežnom interfejsu. VIP se obično dodeljuje mrežnom uređaju koji se nalazi na putu protoka određenog mrežnog saobraćaja. Dolazni paketi se šalju na VIP adresu, ali se paketi redirektuju na IP adresu pravog interfejsa uređaja. VIP se najčešće koristi u slučajevima kada je potrebno obezbediti visoku dostupnost i redundantnost.
- Virtual Private Network (VPN) - Virtualna privatna mreža obezbeđuje mehanizme za bezbednu komunikaciju i prenos podataka i drugih informacija kroz javnu mrežu kao što je Internet, osiguravajući da se kroz takvu sredinu prenose visoko poverljive i osetljive informacije. Takođe predstavlja i jeftinu alternativu za iznajmljene telekomunikacione linije između kompanija i njihovih udaljenih organizacionih jedinica. Pored velikog broja pogodnosti koje pruža, VPN omogućava zaposlenima da mogu sa bilo koje tačke na svetu da bezbedno pristupaju podacima na kompanijskim serverima na isti način kao što to čine iz svoje kancelarije. Kada se veza VPN uspostavi, krajnji korisnik ima utisak kao da se nalazi u korporativnoj mreži.

### 3.2. Softverska rešenja

Na tržištu postoji mnogo softvera, za sve operativne sisteme, čija je namena virtualizacija. U zavisnosti za koju se vrstu virtualizacije, gore navedene, opredelimo primenjuje se odgovarajući softver za njenu implementaciju. Može se Linux pokrenuti kao matični operativni sistem, a onda u virtualnim okruženjima pokretati razne verzije Windows-a, DOS-a, BSD operativnih sistema itd. Takođe može se pokrenuti Windows kao matični operativni sistem, a onda na njemu pokretati razne distribucije Linux-a. Ovaj pristup omogućava susret sa novim operativnim sistemom bez straha od rizika i komplikovanih instalacija na hardveru. Druga opciju uključuje pokretanje istog operativnog sistema, kao što je pokretanje još jedne ili dve kopije Windows-a na matičnom Windows-u. Jedan od aspekata zaštite je u ovako organizovanom sistemu obezbeđen time što se internet veza odvija isključivo u virtualnoj mašini. Svi potencijalni virusi ostaju na virtualnoj mašini, dok je matična mašina zaštićena od istih. U slučaju da se virtualna mašina potpuno zarazi, matični hard disk je siguran od zaraze. Kompletan hard disk virtuelne mašine je najčešće samo jedan fajl na matičnom hard disku, pa je u slučaju potpune zaraze virtualne mašine dovoljno obrisati taj fajl ili kopirati novu kopiju sveže instaliranog operativnog sistema i nastaviti sa radom.

Najpoznatiji programi za virtualizaciju su: VMware, Xen, VirtualBox, Microsoft virtualizaciona rešenja itd.

#### 3.2.1. VMware<sup>3</sup>

Kada se prvi put pojavio VMware na sceni 1998 godine, imao je samo jedan proizvod VMware Workstation. On je omogućavao desktop računarima da pokreću više instanci operativnog sistema u isto vreme. U to vreme ovo se smatralo revolucionarnim. Kasnije će ova firma izbaciti veliki asortiman svojih proizvoda. VMware se smatra jednim od najvećih proizvođača softvera za virtualizaciju. VMware proizvodi mogu se pokretati gotovo na svim operativnim sistemima: Windows, Linux i Mac OS X. Izlaskom VMware GSX i VMware ESX ova kompanije se okreće razvoju serverskih okruženja. Korporativni VMware ESX server se izvršava direktno na hardveru čime se značajno poboljšavaju performanse. Kako je broj konkurentskih firmi vremenom rastao, da bi se održao na tržištu VMware lansirala dve verzije svojih rešenja, besplatne edicije VMWare Server i VMware ESXi.

Virtualizacija emulira celokupni hardver, tj. mrežne uređaje, video kartice, USB priključke itd.. VMware Workstation, Server i ESX proizvodi ne prevode mašinske naredbe, odnosno koriste isti skup mašinskih instrukcija koji koristi stvarni hardver. To značajno poboljšava performanse sistema, ali može stvarati probleme kod prenošenja virtualnih mašina na druge fizičke arhitekture (virtualna mašina se mora zaustaviti pre nego se prebaci na drugi procesor).

---

<sup>3</sup> Videti Ron Oglesby, Scott Herold, VMware ESX Server, Advanced Technical Design Guide, Tech Target, 2005

Neki od VMware proizvoda i njihovi kratki opisi:

- *VMware Workstation* – omogućuje emulaciju više različitih x64-x86 sistema na jednom računaru.
- *VMware Fusion* – ima istu funkcionalnost kao prethodni alat, ali namenjen je Intel Mac sistemima.
- *VMware Player* – besplatna verzija VMware virtualne mašine koja je dostupna za ličnu upotrebu.
- *VMware ESX* – već spomenuti komercijalni sistem koji se izvodi direktno na hardveru čime se bitno poboljšavaju njegove performanse. Podržava širok spektar standardnog hardvera, od Intel i AMD procesora, do SAN, iSCSI i NAS podsistema diskova (fajlova) itd.
- *VMware Server* – je program koji se izvodi iznad operativnog sistema i omogućuje stvaranje više virtualnih sistema, a dostupan je besplatno kao i *VMware Player*.
- *VMotion* - tehnologija koja omogućava migraciju servisa (virtualnih mašina) u radnom stanju i bez prekida u radu sa jednog na drugi fizički *host*.
- *VMware ThinApp* - alat za virtualizaciju aplikacija (programa)
- *VMware Infrastructure* - alat za upravljanje okolinom kod ESX/ESXi
- VMware vSphere - alat za virtualizaciju složenih hardverskih i programskih infrastruktura itd.

### 3.2.2. Citrix Systems Xen

Xen je potpuno besplatni VMM (engl. *Virtual Machine Monitor*) program koji omogućuje virtualizaciju na x86, x86-x64, Itanium i PowerPC 970 arhitekturama. Na Univerzitetu Cambridge 2003. godine rodio se projekat pod nazivom „XenSource“, koji iste godine postati javno objavljen. 2007. godine dolazi u vlasništvo kompanije Citrix System. Od 2009. godine dostupan je kao besplatan alat.

Xen sistemi imaju takvu strukturu gde hipervizor radi na najnižem odnosno naprivilegovanim sloju tzv domain0. Xen radi kao hipervizora iznad hardvera. Prvi operativni sistem (tzv. domain 0) koji se direktno pokreće kod podizanja sistema, ima prava pristupa hardveru i preko njega se može upravljati svim drugim virtualnim operativnim sistemima (u tzv. *domain U* domenu). Kao domain 0 sistem mogu se pokretati prilagođene verzije Solaris, Linux i NetBSD sistema. Prilagođene verzije nekih UNIX sistema takođe se mogu izvoditi i u domain U domenu. Novije verzije Xena omogućuju virtualno pokretanje izvornih Windows sistema u slučaju da hardver podržava x86 virtualizaciju. Takav hardver uključuje Intel VT i AMD-V arhitekture. U zavisnosti od hardverskih arhitektura Xen sistemi oslanjaju se kako na para virtualizaciju, tako u pojedinim slučajevima i na potpunu virtualizaciju.

Lansiran je veliki broj alata za upravljanje Xen sistemima preko korisničkog interfejsa. Neki od najpoznatijih i najviše korišćenih su:

- *XenExpress* - je najjednostavnija varijanta. Potupuno je besplatna i podržava pokretanje do četiri virtualne mašine.
- *XenServer* - malo naprednija verzija prethodnog, omogućava pokretanje do osam virtualnih mašina.
- *XenEnterprise* - napredni softver namenjen najzahtevnijim korisnicima. Uz godišnju pretplatu za dva snažnija rešenja, *XenSource* obezbeđuje i tehničku podršku za rešavanje svih zahteva korisnika Xen virtualizacije. U slučaju *XenEnterprise* rešenja omogućeno je kreiranje neograničenog broja virtualnih mašina – jedino realno ograničenje su hardverski kapaciteti računara na kojem se ovaj sistem pokreće. I proizvođačima procesora, koji stalno dodaju jezgra i nove kapacitete, jasno je da sve to nije lako iskoristiti u potpunosti, pa razvijaju i sopstvene tehnologije vezane za virtualizaciju, kakve su *Intel VT* i *AMD Virtualization (AMD-V)*.
- *Xen Tools* – perl alati za Debian GNU/Linux,
- *Ganeti* – orijentisani na upravljanje grozdovima računara i paralelizaciju,
- web orijentisani *HyperVM* – polu-komercijalni (engl. *proprietary*) alat namenjen Linux sistemima.

### 3.2.3. Oracle VM VirtualBox (Sun Microsystems Virtualbox)

Oracle VM VirtualBox je x86 softverski paket za virtualizaciju. On je originalno kreiran od strane Innoteka GmbH, kompanije za razvoj softvera. 2008. godine kompanija Sun Microsystems kupuje Innotek. Oracle Korporacija je januara 2010. godine kupila Sun, i tada se zvanično tržišna marka promenila iz Sun Microsystems VirtualBox u Oracle VM VirtualBox. Danas se ovaj softver razvija od strane Oracle korporacije kao jedan od proizvoda linije softvera za virtualizaciju.

VirtualBox Open Source verzija pojavila se u januaru 2007. godine i bila je potpuno besplatna. Potpuni VirtualBox paket bio je licenciran kao tzv. polu-komercijalni alat. To znači da se njegova upotreba naplaćivala. Takođe, postojala je zaštita autorskih prava i izvornog koda te ograničenja na način na koji ih korisnici mogu koristiti (kopirati, distribuirati). On je danas dostupan kao besplatan alat slobodan za neograničenu upotrebu.

VirtualBox omogućava virtualizaciju x86 hardvera na operativnim sistemima:

- Windows
- Solaris
- Linux
- Mac OS X
- FreeBSD

Virtualni operativni sistemi koji se mogu pokrenuti na ovom alatu su:

- FreeBSD
- Windows
- Linux
- Solaris
- OpenBSD, DragonflyBSD, SkyOS i drugi.

Na VirtualBox-u može istovremeno nezavisno raditi nekoliko operativnih sistema. Svi međusobno, uključujući i operativni sistem domaćina mogu komunicirati preko zajedničkog bafera ili koristeći mrežne veze. Virtualizacije hardvera čuvaju se u VDI (engl. *Virtual Disk Images*) formatu. Moguće je čitati i pisati VMware-ove VMDF (engl. *Virtual Machine Disk Format*) i Microsoftove VHD (engl. *Virtual Hard Disk*) datoteke.

Virtual Box podržava i Intelovu hardversku virtualizaciju VT-x i AMD-ovu AMD-V. Virtualno okruženje uključuje emulaciju mrežnih, grafičkih i zvučnih kartica pa se veliki deo sistema može pokretati i bez instalacije upravljačkih programa (drajvera).

#### 3.2.4. Microsoft virtuelizaciona rešenja

Connectix korporacija je osnovan 1998. godine i jedan je od ranih nosioca razvoja virtuelizacionih tehnologija. Jedan od proizvoda je Virtual PC, koji je obezbeđivao Macintosh sistemima da rade pod Windows platformom. Microsoft je preuzeo od Connectix-a nerealizovani Virtual Server u februaru 2003. godine. Tada je nastavljeno sa razvojem Virtual PC proizvoda. Microsoft je napravio nekoliko bitnih promena u dizajnu. Ubrzo nakon toga su lansirani proizvodi poput Virtual Server 2005, i Virtual PC 2007. Najnoviji proizvod iz ove familije proizvoda koje je Microsoft lansirao je Tip1 hipervizora, koji se zove **Hyper-V**.

Kada govorimo o serverskoj virtualizaciji postoje 3 osnovna tipa Microsoft proizvoda:

1. Microsoft Virtual Server 2005 (hosted hibridna virtualizacija),

i Microsoftove Hyper-V tehnologije:

2. Microsoft Windows Server 2008 Hyper-V (hipervizor)
3. Microsoft Hyper-V Server 2008 (hipervizor)

##### *Microsoft Virtual Server 2005*

Microsoft Virtual Server 2005 predstavlja servis koji radi pod Windows operativnim sistemom. Ovo je prvi Microsoft-ov proizvod namenjen za menadžmentu virtualnih

serverskih mašina. Virtual Server radi i pod 32-bitnim i 64-bitnim verzijama Windows operativnih sistema. Gostujući operativni sistemi moraju biti 32-bitni. Iako Virtual Server 2005 R2 radi na domaćinu sa x86 i x64 procesorima gosti ne mogu biti 64-bitni. Virtual Server 2005 dostupan je u dve edicije: Standar i Enterprise edicija. Enterprise edicija podržava rad sa više procesorskih jedinica.

### *Microsoft Hyper-V tehnologije*

Microsoft Hyper-V, pod komandnim imenom Viridian, a opšte poznat kao Windows Server Virtualizacija, predstavlja virtualizaciju zasnovanu na hipervizorima kod x86-64 sistema. Beta verzija je isporučena za neke od x86-64 edicije Windows Servera 2008, a finalna verzija je objavljena 26. juna 2008. godine. Hyper-V je prvo realizovan kao stand-alone verzija i kasnije nadograđen u R2 (Release2) verziju. Hyper-V je zastupljen u dve varijante. Prva varijanta uključuje samostalnu, verziju poznatu pod nazivom Microsoft Hyper-V Server 2008. Druga verzija podrazumeva da se Hyper-V rola (uloga) instalira na operativni sistem Windows Server 2008R2 ili Windows Server 2008.

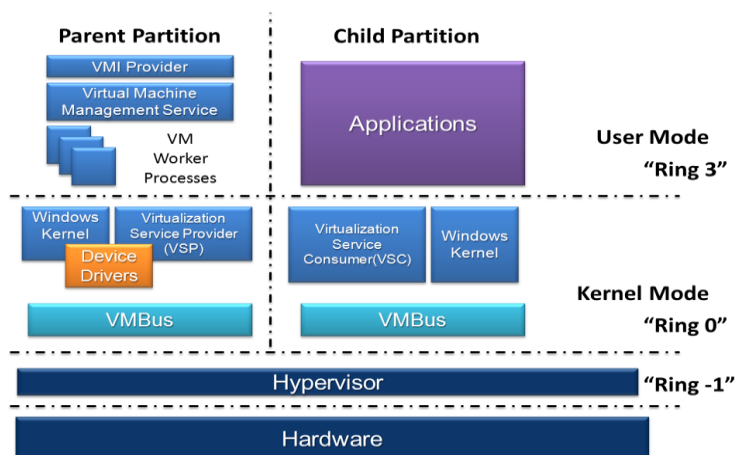
### *Microsoft Hyper-V Server 2008*

Predstavlja samostalnu verziju Hyper-V. Objavljen je 1. oktobra 2008. godine. On je zapravo varijanta core instalacije Windows Server 2008 koji uključuje potpune Hyper-V funkcionalnosti, ali su ostale Windows Server 2008 uloge isključene. Takođe Windows servisi su ograničeni. Iz toga sledi da Hyper-V Server 2008 nije Windows Server 2008 okruženje, ali jeste izgrađen na core-u Windows tehnologija. Besplatna Hyper-V Server 2008 varijanta je ograničena na interfejs komandnih linija (CLI), gde se konfiguracija "Hosta" i "Parent" operativnih sistema, fizičkog hardvera i softvera vrši pomoću shel komandi. Novi meni vođen CLI interfejsom znatno pojednostavljuje početnu konfiguraciju. Pojedini skript fajovi koji se mogu besplatno daunlodovati proširuju ovaj koncept. Administracija i konfiguracija "Host" operativnog sistema, koji je naravno Hyper-V Server 2008, i "guest" ili virtualnih operativnih sistema, se generalno izvršava uz pomoć daunlodovanih proširenih Microsoft Menagement konzola koje se instaliraju na Windows Server 2008 (x32-64) ili na System Center Virtual Machine.

### *Microsoft Windows Server 2008 Hyper-V*

Predstavlja drugu varijantu Hyper-V. U ovom slučaju Hyper-V je zapravo rola u okviru Windows Server 2008 operativnog sistema. Da bi se instalirala Hyper-V rola u okviru Windows Servera 2008, potrebno je da hardver bude 64 bitni. Kada se Hyper-V rola instalira na Windows Serveru 2008 ubacuje se hipervizor binarni kod između operativnog sistema i fizičkog hardver u okviru but procesa. Kako hipervizor radi direktno na hardverskoj platformi, on spada u Tip1 hipervizora. Za ovakvu vrstu Hyper-V rešenja potrebna je posebna arhitektura. Ona zahteva hardverski -

potpomognutu virtualizaciju sa Intel VT ili AMD V procesorima. Arhitektura Windows Server 2008 Hyper-V je potpuno ista kao i ona kod Hyper-V Servera 2008.



Slika 6. Hyper-V arhitektura<sup>4</sup>

## 4. Prednosti virtuelizacije

Nakon upoznavanja sa pojmom virtualizacije, njenim nastankom, oblicima i vrstama virtualizacionih rešenja pitanje do kojeg se neminovno dolazi jeste: Koja je svrha postojanja virtualizacije i šta nam ona korisno donosi?

Ključni pokretači razvoja virtualizacije su:

- Konsolidacija
- Pouzdanost
- Sigurnost
- Efikasnost

### Konsolidacija

Kada se pomisli na virtualizaciju obično se prvo pomisli na smanjenje troškova. Za kompanije virtualizacija konkretno znači da imaju smanjene količine hardvera koji je potreban za pokretanje radnih procesa koji su neophodni za posao.<sup>5</sup> Cilj je da se iskoristi pun potencijal serverskih sistema. Virtualizacija pomaže u migraciji starih operativnih sistema. Na taj način se rešava problem nekompatibilnosti starih operativnih sistema i aplikacija sa novim hardverom. Ranije su operativni sistemi bili fizički vezani za hardversku odnosno fizičku platformu i to je stvaralo velike probleme kada bi kompanije imala potrebu da nadgrade postojeće sisteme koje su koristile. Virtualizacija predstavlja savršeno rešenje za ovakve probleme jer se softver odvaja od fizičke platforme. Virtualina okruženja pomažu razvoj i testiranje kako aplikacija tako i operativnih sistema, koji zahtevaju relativno skupe resurse i mnogo

<sup>4</sup> Preuzeto sa <http://en.wikipedia.org/wiki/Hyper-V>

<sup>5</sup> Videti Virtualizacija i njene glavne prednosti, str.1 (Dušan Abadžin, 2010)

vremena. Alati virtualizacije omogućavaju softveru da brzo i lako postavlja i održava testirano okruženje, kao i da brzo povрати okruženje u svoje prvobitno stanje kada je to potrebno. Na taj način se period pripreme za implementaciju u produkciono okruženje smanjuje, uz minimalno korišćenje fizičkih resursa, čime je cena testiranja svedena na minimum.

### *Pouzdanost*

Jedan od ključnih aspekata uspešnosti poslovanja kompanije meri se kroz stepen pouzdanosti poslovnih sistema i aplikacija koji se u okviru nje primenjuju. Velike kompanije ne smeju dozvoliti da poslovni procesi ijednog trenutka stanu, a da bi to obezbedile neophodno je da osiguraju neprekidan rad poslovnih sistema i aplikacija koji se oslanjaju na IT resurse. Da bi se sistem održavao pouzdanim, redundantnost sistema mora postojati, a da bi se redundantnost obezbedila potrebno je dodatno investirati u opremu i softver. Kompanije su spremne da investiraju značajna sredstava u pouzdanost kako bi obezbedile maksimalnu dostupnost svog poslovnog sistema. Virtualizacija daje elegantan odgovor na to kako je moguće napraviti uštedu u troškovima opreme i održavanja. Virtualizacione tehnologije daju mogućnost da se određeni procesi izoluju. Njenom primenom se može na primer pokrenuti sistem za nekoliko kompanija na jednom serveru, zadržavajući aplikacije bezbedno odvojene jedne od drugih. Naime, virtualne mašine u toku svog rada ne moraju da ugoržavaju ostale virtualne mašine, time virtualizacija daje određni nivo abstrakcije koji omogućava viši nivo pouzdanosti.

### *Sigurnost*

Virtualizacija je najbolje rešenje kada je oporavak od neželjenog pada sistema u pitanju. Postoji stara izreka da je nemoguće obezbediti „disaster recovery“, a da to rešenje bude pri tome brzo, jeftino i pouzdano. Ali ova izreka jeste stara, jer virtualizacija odgovara na sva tri zahteva. Oporavak virtualnih mašina je brz koliko i startovanje mašina, a o pouzdanosti ne treba posebno govoriti, jer same fizičke mašine nemaju fizički hardver koji je podložan padu. Danas postoji mnogo alata za menadžment virtualnih mašina, koje omogućavaju P2V „physical to virtual“, pomoću kojih je moguće uraditi snapshot čitavog servera, napraviti sliku, i to bez da se isti fizički-produkcion server restartuje. Možemo slobodno da kažemo da virtualizacija jeste brzo, jeftino i pouzdano rešenje za oporavak od neželjenog pada sistema. Tehnologija koja štiti aplikacije time što ih izoluje od ostatka aplikativnog okruženja takođe može da obezbedi zaštitu i sigurnost od propusta u čitavom sistemu koji je virtualizovan. Ako se desi da je određeni deo sistema kompromitovan, on neće uticati na ostale partije u sistemu.

### *Efikasnost*

Kao što je pokazano virtualizacija ima različite oblike, i kao takva može se primeniti na mrežnim resursima i na procesima u okviru servera. Primenom virtualizacije moguće je napraviti odličan „load balancing“, jer svaka virtualna mašina može imati svoju jedinstvenu IP adresu i može biti vezana za određeni segment mreže. Ovo obezbeđuje fleksibilnost da tokovima upravlja na način koji će najmanje opteretiti protok i saobraćaj na mreži. Virtualizacija računarskih resursa je revolucionarni korak u administraciji računarskih sistema, zato što je njenom primenom omogućeno

centralizovano nadgledanj i kontrolisanje svih procesa jednog sistema na jednom mestu. Nikada nije bilo lakše upravljati udaljenim serverima, njihovom migracijom, ažuriranjem novih verzija i patch-eva, izolacijom određenih servisa i pružanjem maksimalnog odziva na neke nepravilnosti u radu sistema. Primenom virtualizacije ne smao da se smanjuje broj hardverskih instanci, njihovo napajanje, hlađenje, nego se zauzima i manji prostor više nego ikada.

## 5. Arhitektura virtuelizacije

Cilj virtualizacije jeste da obezbedi operativnim sistemima da rade u izolovanim režimima. Da bi se to postiglo koristi se hipervizori ili VMM-ovi koji predstavljaju programski mehanizme. Oni obezbeđuju lakšu komunikaciju sa hardverom. Zbog toga je jezgro CPU arhitekture dovedeno bliže programskom nivou arhitekture. Na taj način će svakoj mašini biti posebno posvećeno okruženje.

Pod idealnom računarskom arhitekturom se smatra ona arhitektura u kojoj je procesor direktno usaglasen sa operativnim sistemom. Kada su CPU i operativni sistem pravljeni da rade zajedno obezbeđuje se veći nivo stabilnosti i zaštite.

Najčešće korišćena arhitektura u modernim računarskim sistemima je x86 kompatibilna. Kod familije proizvoda ove arhitekture postojala su dva načina pristupa memoriji:

1. Realni mod
2. Zaštićeni mod

### *Realni mod*

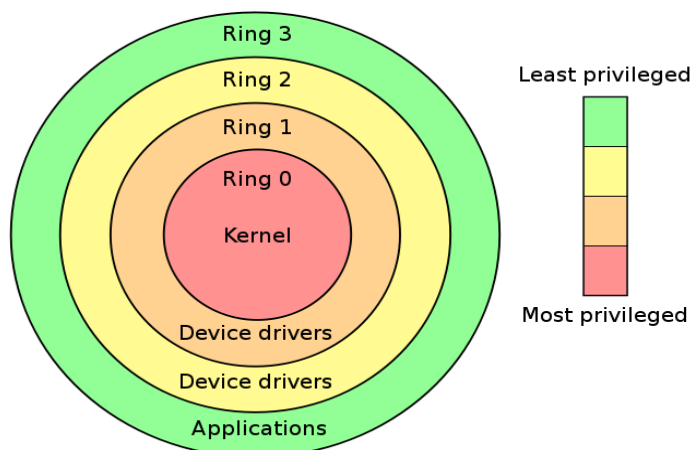
Realni mod koji dozvoljava limit od 1MB memorije vrlo brzo je prevaziđen. Virtualni mod je maksimalno mogao da izvršava 16-bitne operacije, pa je brzo prevaziđen sa pojavom 32-bitnih operativnih sistema u x86 arhitekturi.

### *Zaštićeni mod*

U x86 arhitekturi zaštićeni mod koristi 4 nivoa privilegije. Ovo se najčešće u praksi nazivaju prstenovi. Prstenovi su numerisani brojevima od 0 do 3. Sistemska memorija je podeljena u segmente i svakom segmentu je dodeljen određeni prsten. Procesor koristi pretenove da bi odredio šta može, a šta ne može biti urađeno sa kodom ili podacima u okviru segmenta. Termin prsten preuzet je iz Multics sistema (Multiplexed Information and Computing Service), gde se nivo privilegija određuju koncentričnim prstenovima. Unutrašnji prsten ili prsten 0 ima totalnu kontrolu nad procesorom.

Operativni sistemi Windows, Linux, Unix prstenastu arhitekturu. Kod njih je četvoroslojna arhitektura svedena na dvoslojnu, prsten 0 i 3. Prsten 0 predstavlja Supervisor mod, a prsten 3 se naziva User mod ili korisnički mod. Mehanizmi sigurnosti u hardveru primenjuju restrikcije na prstenu 3 limitirajući na taj način pristup segmentima. To bi značilo na primer da ukoliko korisnički program koji radi

na prstenu 3 pokušava da adresira memoriju van svog opsega automatski dolazi do zaustavljanja izvršavanja koda.



Slika 7. Struktura prstenova kod x86 arhitekture<sup>6</sup>

### Hipervizor – Virtual Monitor Mašina

On predstavlja izvršni mod na x86 procesorima. Zadužen je za izvršavanje instrukcija kao što su privilegovane I/O i memorijske upravljačke operacije. Operativni sistemi bi trebalo da rade na prstenu 0 ili supervizor modu. Kako je prsten 3 zasnovan na prstenu 0 modu, svaka nestabilnost ili nepravilnost u prstenu 0 direktno utiče na korisnički mod u prstenu 3. Da bi se izolovao prsten 0 za svakog virtualnog gosta, neophodno je uraditi pomeranje prstena 0 bliže gostujućim operativnim sistemima. Time se postiže da pad jednog virtualnog sistema gosta, odnosno pad prstena 0 neće uticati na prsten 0 ili prsten 3 bilo kog drugog gosta. Taj virtuelni prsten 0 za korisnika, može da bude postavljen na prstenu 1,2,3 za x86 arhitekturu. Naravno što je virtuelni prsten 0 dalji od pravog 0 prstena, to je više udaljen od izvršavanja direktnih hardverskih operacija. Naravno, ovo direktno utiče na smanjenje performansi.

Pomeranje 0-og prstena u privilegovane prstenove radi se tako što virtualizacija pomera hipervizora odnosno VMM u jedan od prstena koji za uzvrat predstavlja prsten 0. Na tom prezentovanom prstenu 0 se pokreću virtualne mašine.

Razlikuju se dva osnovna tipa VMM-a:

1. Tip 1 VMM
2. Tip 2 VMM

#### Tip 1 VMM

U ovom slučaju softver radi na prvom 0-om prstenu, odnosno na vrhu hardverske platforme bez dodatnih intervencija operativnog sistema.

<sup>6</sup> Preuzeto sa [http://en.wikipedia.org/wiki/Ring\\_%28computer\\_security%29](http://en.wikipedia.org/wiki/Ring_%28computer_security%29)

Izolovanost svake pojedinačne virtualne mašine postiže se time što se gostujući operativni sistemi podižu na višem nivou hardvera.

### *Tip 2 VMM*

Softver radi na 3 prstenu u okviru operativnog sistema. Virtualne mašine se pokreću na prstenovanom prstenu 0 koji je najudaljeniji od hardvera koliko je to moguće. Procesi i komande se izvršavaju bez obzira na operativni sistem koji je ispod. Ova arhitektura je više zastupljena kod procesne nego kod serverske virtualizacije.

Hipervizori:

Postoje dve vrste hipervizora:

1. monolitni
2. mikrokernelizovani

### *Monolitni*

Monolitni hipervizori se odlikuju time što njih sačinjavaju različiti drajveri za uređaje kao i mnoge druge komponente. Monolitni hipervizori zaista predstavljaju jedan operativni sistem.

### *Mikrokernelizovani*

Mikrokernelizovani hipervizori sadrže veoma mali set funkcija koje omogućavaju izvršavanje operacija nad hardverom na najvišem nivou privilegija. Prstenovi sa nižim brojem obezbeđuju veći nivo sistemskih privilegija i pristupa hardverskim resursima.

## **6. Cloud computing – poslednji korak u razvoju virtuelizacije**

### **6.1. Pojam i definicija cloud computing-a**

Pojavljivanje cloud computing-a kao poslovnog koncepta i samog termina vezuje se za poslednju deceniju, a njegov značajniji razvoj i prihvatanje od strane šire informatičke zajednice desio se tek u poslednjih 4-5 godina. U samom začetku, bilo je dosta nedoumica u vezi ovog novog IT koncepta, kako o samom načinu funkcionisanja i arhitekturi, tako i o osnovnim definicijama cloud computing-a. Danas svi govore o “cloud computing-u“, ali čini se da svako koristi drugačiju, iako sličnu definiciju, u zavisnosti od svoje pozicije. Na primer, oni koji rade u oblasti usluga imaće drugačiju definiciju “cloud computing-a“ od nekoga ko radi na sistemskoj arhitekturi.

### Definicija cloud computing-a:

Cloud computing je model koji omogućava jednostavan mrežni pristup, na zahtev korisnika, deljenom skupu resursa (npr. mrežni resursi, serveri, prostor na hard diskovima, aplikacije i servisi) koji mogu biti brzo omogućeni za upotrebu ili ugašeni, a sa minimalnim intervencijama ili akcijama od strane pružaoca usluga.

„Oblast računarstva u kojoj se veoma skalabilni informatički kapaciteti obezbeđuju u vidu usluge isporučene putem interneta brojnim eksternim potrošačima.“

Daryl Plummer, Gartner

„Apstrahovana, visoko skalabilna i kontrolisana kompjuterska infrastruktura koja hostuje aplikacije namenjene krajnjim korisnicima i čije se usluge naplaćuju na bazi ostvarene potrošnje.“

Forrester

Cloud je već uveliko prisutan u oblicima koje mnogi poznaju kao DropBox, SkyDrive, Gmail, YouTube, Facebook i mnogi drugi. Cloud je usluga koja nam nudi neograničene količine svega (hard disk, procesor, memorija i ostalo) onda kada nam je potrebno i koliko nam je potrebno i to na način da samostalno sve to kontrolišemo, kroz neku aplikaciju ili web portal. Ideja se zasniva na tome da su svi podaci koji su korisniku potrebni, dostupni u svakom trenutku putem Interneta. Cloud je usluga dostavljanja servisa umesto samog proizvoda. Cloud pruža aplikacije, pristup podacima, servise za skladištenje podataka i ne traži od korisnika poznavanje fizičke lokacije sistema koji nam obezbeđuje uslugu, broj servera koji se koriste za tu uslugu takođe korisniku nije poznat, njihova infrastruktura takođe nije poznata, mogu biti u istoj zgradi ili na različitim kontinentima.

S obzirom da korisnik nije vlasnik infrastrukture samim tim nije dužan ni da je održava, on u stvari plaća iznajmljivanje usluge i onih resursa koji su mu u određenom trenutku potrebni. Znači, potrebna mu je neka poslovna aplikacija, iznajmi je, završi posao i plati. Nema potrebe za kupovinom aplikacija, promenama hardvera i ostalo, sada mu je potreban samo pristup nekom cloud servisu gde plaća ono što koristi i koliko koristi. Kada više ne želi neke usluge, nema više potrebe za njima, jednostavno se isključi i ne plaća više za njih.

## 6.2. Karakteristike cloud computing-a

Cloud computing odlikuje pet osnovnih karakteristika:

- Samostalnost u korišćenju zahteva
- Širok spektar mogućnosti mrežnog pristupa
- Alokacija resursa
- Fleksibilnost sistema
- Merljivost usluge

Samostalno korišćenje na zahtev - Korisnik može koristiti resurse kada on to želi, sa bilo kojeg mesta i u bilo koje vreme. Ovi resursi podrazumevaju serversko vreme ili mrežni prostor (fizički prostor na storage uređajima, kao što je hard disk) kojima se

pristupa bez potrebe za ljudskom intervencijom bilo kod klijenta ili kod provajdera usluga.

Širok spektar mogućnosti mrežnog pristupa - Mogućnosti sistema su dostupne klijentima putem mreže i može im se pristupiti sa različitih uređaja, kao npr. desktop računara, mobilnih telefona, smartphone uređaja, PDA računara i slično.

Alokacija resursa - Kompjuterski resursi provajdera su grupisani kako bi opslužili veliki broj istovremenih korisnika. Mehanizam raspodele procesorske snage ili, na primer, količine memorije funkcioniše tako što sistem dinamički vrši raspodelu ovih parametara prema zahtevima korisnika. Sami korisnici nemaju kontrolu nad fizičkim parametrima, odnosno lokaciji resursa, ali na nekim višim nivoima podešavanja svog sistema u okviru cloud-a mogu da izaberu gde će njihovi podaci biti smešteni i procesirani (npr. određena država ili određeni data centar).

Elastičnost sistema - Mogućnosti cloud-a mogu biti veoma brzo i elastično pružene korisniku sistema, ukoliko isti ima potrebe za tim. Pretpostavimo da se naš web sajt nalazi u oblaku i da nam je promet u smislu broja posetilaca sličan svakoga dana. Zatim pretpostavimo da jednog dana, iz nekog razloga, posećenost naše web prezentacije skoči za 1200%. Ukoliko je sajt hostovan na našem, privatnom serveru, postoji velika mogućnost da se on jednostavno sruši i prestane sa radom, što zbog softverskih, što zbog hardverskih ograničenja. U takvim slučajevima, cloud automatski i dinamički dodeljuje potrebne resurse kako bi podržao novonastalu situaciju, a kada promet ponovo opadne, resursi se isto tako brzo povlače i vraćaju u prvobitno stanje. Korisnik može kupovati dodatne resurse i mogućnosti u bilo kojim količinama i bilo kada.

Merljivost usluga - Cloud sistemi automatski kontrolišu i optimizuju neophodne resurse u zavisnosti od potreba korisnika i tipa usluge koja se traži (prostor na disku, procesorska snaga, količina RAM memorije i slično). Sve ove usluge su merljive i njihovo korišćenje je transparentno, kako za provajdera, tako i za klijente, što je veoma važno jer finansijski momenat igra veliku ulogu kad je u pitanju ova nova tehnologija, naročito za velike, enterprajs sisteme i kompanije.

### 6.3. Servisni modeli cloud computing-a

Cloud computing se temelji na tri osnovna modela servisa:

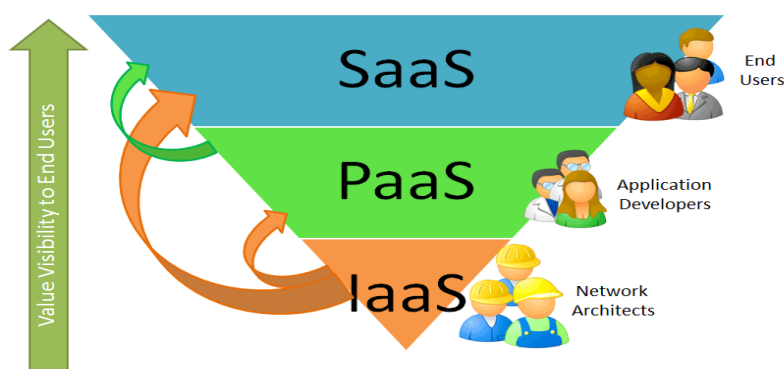
- Software as a Service(SaaS)
- Infrastructure as a Service(IaaS)
- Platform as a Service(PaaS)

*Softver kao servis (Software as a Service, SaaS)* odnosi se na softverske usluge u cloud-u. SaaS znači da određeni softver/aplikacija koju želite da koristite nije instaliran kod vas već na nekom drugom mestu. Treba napomenuti da SaaS

predstavlja opšti naziv za model isporučivanja softvera kao servisa i ne koristi se samo u cloud computing-u već se može sresti i kod drugih tehnologija. Primeri toga su Facebook, Gmail i sve web aplikacije.

*Infrastruktura kao servis (Infrastructure as a Service, IaaS)* odnosi se na isporučivanje infrastrukture kao servisa. Tačnije, radi se o virtuelnom serveru uz koji se vežu sve relevantne usluge kao što su procesorska snaga, memorija, prostor na disku i ostalo. Ovo u prevodu znači da se korisnik brine za sve od operacionog sistema, aplikacije, antivirus softvera pa do samih podatak. Ono što se može smatrati lošim kod ove usluge jeste to što je to u stvari vaša virtuelna mašina i vi ste u potpunosti odgovorni za nju.

*Platforma kao servis (Platform as a Service, PaaS)* usluga je model isporučivanja operativnih sistema kao servisa zajedno sa ostalim servisima, putem Interneta bez potrebe za download-om i instalacijom. PaaS usluga preuzima odgovornost za sve što se tiče platforme, uključujući i skalabilnost zavisno o potrebnom kapacitetu. PaaS nudi različite kombinacije usluga u cloud-u za podršku svim fazama razvojnog ciklusa aplikacije među kojima su integrisano razvojno okruženje (IDE), kontrola izvornog koda, kontrola verzija, praćenje izmena koda, interaktivni testovi za više korisnika i ostale. PaaS rešenja su razvojne platforme u kojima su razvojni alati smešteni u cloud-u i kojima se pristupa pomoću web browser-a.



Slika 8. Nivo vidljivosti servisa

7

#### 6.4. Modeli cloud computing-a prema klasifikaciji

U cloud computing-u razlikujemo 4 različita modela prema klasifikaciji:

- Private Cloud
- Community Cloud
- Public Cloud
- Hybrid Cloud

*Privatni cloud (Private Cloud)* Privatna cloud infrastruktura je u vlasništvu organizacije i njome upravlja sama organizacija (kompanija) ili treća lica koja to rade

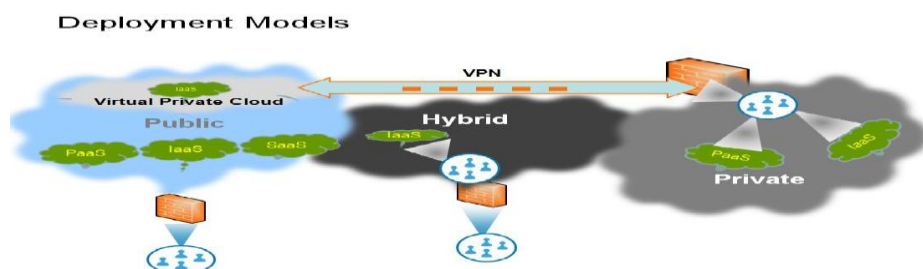
<sup>7</sup> Skila preuzeta sa sajta <http://argowiki.com/index.php?title=SaS>

za njih (outsourcing). Ovakav model može fizički biti u okviru prostorija organizacije ili fizički dislociran.

*Community cloud* Kod ovog modela, infrastruktura je podeljena između nekoliko organizacija i pruža podršku grupi organizacija (ili kompanija) koje dele iste interese, kao što su misija i vizija, sigurnosna politika, i slično. Kao i u prethodnom slučaju, njime može biti upravljano od strane interno zaposlenog osoblja, ili kroz outsourcing.

*Javni cloud (Public Cloud)* U ovom slučaju sistem je u posedu kompanije koja se bavi prodajom cloud usluga i dostupan je svim pojedincima i poslovnim subjektima.

*Hibridni cloud (Hybrid Cloud)* Model koji je sastavljen od dva ili više prethodno navedenih (Private, Community, Public) u kome svaki od njih ostaje nezavisan, ali su međusobno povezani prateći definisane standarde i procedure kako bi se obezbedila mobilnost podataka između njih. Tako na primer, velika kompanija može svoj sistem držati većinom u privatnom oblaku, dok neke poslovne funkcije može prebaciti u javni oblak (slanje velikog broja email-ova ili slično) kako bi rasporedila opterećenje sistema prema svojim potrebama.



Slika 9. Šematski prikaz modela prema klasifikaciji

## 6.5. Prednosti i mane cloud computing-a

### Koje su prednosti "cloud computing-a" za obične korisnike?

Prednosti koje donosi novi poslovni model su sledeće:

- Niža cena programske podrške: plaća se usluga, tj. onoliko koliko se koristi (troši).
- Korisniku je uvek dostupna zadnja, najnovija verzija programske podrške.
- Programska podrška i podaci su dostupni sa svake lokacije gde korisnik ima pristup Internetu.
- Manji troškovi održavanja i nadogradnje programske podrške.
- Nema troškova direktno vezanih za kupovinu hardvera, licenci za serverske operative sisteme, baze podataka, servere za elektronsku poštu.
- Nema troškova njihovih instalacija i konfiguracija samim time kasnije održavanja.

- U uslugu je uključena profesionalna antivirusna zaštita i backup podataka.

### **Koji su nedostaci "cloud computing-a" za obične korisnike?**

"Cloud computing" podrazumeva i neke nedostatke:

- Problem dostupnosti – nije moguće koristiti uslugu ukoliko je internet veza slaba ili u prekidu.
- Problem sigurnosti
  - Poverenje da provajder usluga neće ukrasti, prodati ili zloupotребiti: naše podatke, dokumenta, baze podataka, podatke o našem ponašanju i korišćenju aplikacija
  - Mogućnost "prisluškivanja" komunikacije između nas kao korisnika i naših klijentskih uređaja i računskih centara.
- Problem zavisnosti o jednom provajderu programske podrške, tj. usluga (zbog nedostatka standarda o zapisu podataka i njihovoj razmeni između različitih platformi).

### **Šta je "cloud computing" za profesionalne informatičare?**

On predstavlja novu tehnološku platformu koja omogućava da se inženjeri i programeri koncentrišu i usmere na implementaciju poslovne logike, umesto da implementiraju infrastrukturu za izvršavanje i podršku rada aplikacija. Takođe sistemski inženjeri imaju manje posla pri održavanju platformi za izvršavanje aplikacija.

### **Koje su prednosti "cloud computing-a" za profesionalne informatičare?**

Postoji niz prednosti:

- **Dostupnost aplikacija:**
  - Sa svake lokacije koja ima pristup Internetu i putem njega računskom centru
  - Velik broj računara omogućava povećanje dostupnosti aplikacija zbog:
    - velikog broja računskih centara koji su distribuirani geografski
    - svaki računski centar ima redundantnu infrastrukturu počevši od servera, komunikacionih veza, sistem napajanja, klimatizacije, automatskog nadgledanja i profesionalnog informatičkog osoblja za podršku.
- **Skalabilnost aplikacija** (mogućnost opsluživanja velikog broja korisnika):
  - Cloud computing platforme omogućavaju iskorišćavanje velikog broja servera i računskih centara na različitim mestima

- Nova paradigma razvoja aplikacija omogućava jednostavniji razvojni proces – programska podrška se razvija kao da se planira da opslužuje jednog korisnika, a infrastruktura računskog centra i platforme omogućava da se takva aplikacija "klonira" i opslužuje veliki broj korisnika u isto vreme
- U konfiguraciji cloud computing platforme moguće je podesiti kada će se koristiti dodatni resursi, čime se optimizuje cena korišćenja infrastrukture sa stvarnim potrebama da bi se efikasno mogao opslužiti veći ili manji broj korisnika.
- **Fleksibilnost u menjanju i prilagođavanju aplikacija:**
  - Aplikacija se ažurira samo na jednom mestu, korisnici dobijaju novu verziju prilikom sledećeg pristupa
  - Parametrima konfiguracije aplikacija se može prilagoditi svakoj grupi korisnika.
- **Stalno praćenje rada i održavanje infrastrukture:**
  - Veliki deo troškova za informatiku i osiguranje rada programskih rešenja odnosi se upravo na osiguranje infrastrukture za njihov rad, sigurnost, čuvanje podataka i konfiguraciju sistema kao i stalni nadzor performansi rada
  - Smeštanje aplikacija u "oblak", ovi troškovi su višestruko manji, a kvalitet usluga i performansi se često povećava.

### **Koji su nedostaci "cloud computinga" za profesionalne informatičare?**

Naravno postoje i nedostaci koje treba uzeti u obzir kada se razmišlja o razvoju aplikacija koje će se smestiti u "oblak":

- Mora da se usvoji nov način razvoja aplikacija: platforme koje danas nude različiti proizvođači ili provajderi poput Microsoft-a i Amazon-a vrlo su različite i zahtevaju poseban način projektovanja arhitekture takvih aplikacija.
- Nije moguće jednostavno premeštati postojeće aplikacije.
- Ne postoje standardi za:
  - Povezivanje aplikacija (servisa) u "oblacima" različitih proizvođača (ili čak istog proizvođača)
  - Razmenu podataka
  - Premeštanje podataka i programske podrške iz "oblaka" jednog proizvođača u "oblak" drugog proizvođača
- Problem sigurnosti, poverenja da "vlasnik oblaka" neće preuzeti korisnike, aplikacije, ukrasti podatke ili samu aplikaciju

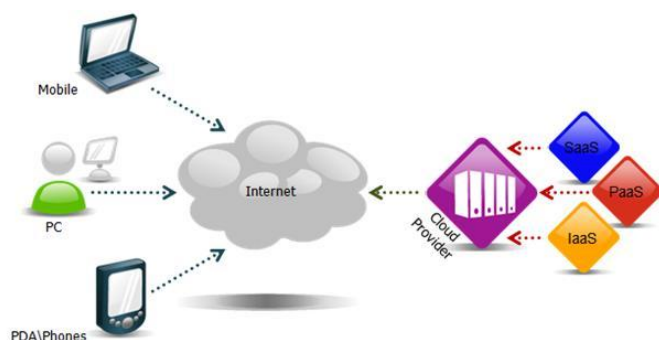
## 6.6. Cloud computing arhitektura

Arhitektura cloud computing-a se raslojava na:

- Front end
- Back end

Front end je strana korisnika odnosno klijenta. Front end podrazumeva računar korisnika ili računarsku mrežu i aplikaciju neophodnu za pristupanje cloud computing sistemu. Različiti computing sistemi koriste različite interfejse. Neki od njih koriste postojeće web browsere (Internet Explorer, Mozilla Firefox), dok drugi imaju jedinstvene aplikacije koje omogućavaju mrežni pristup klijentu. Klijenti pristupaju svojim aplikacijama i podacima u bilo kom trenutku i sa bilo kog mesta koristeći bilo koji uređaj povezan na Internet (računar, mobilni telefon, iPad i sl.).

Na back end strani nalaze se razni serveri, sistemi i računari za skladištenje podataka koji kreiraju cloud računarski servis. Centralni server nadgleda saobraćaj i klijentske zahteve. On je zadužen za upravljanje sistemom a sa ciljem da obezbedi stabilno funkcionisanje istog. Centralni server koristi posebnu vrstu softvera zvanog Middleware. Ovaj softver omogućuje mrežnim računarima da međusobno komuniciraju.



Slika 10. Front end i Back end

## 6.7. Cloud computing provajderi i uslovi pružanja usluga

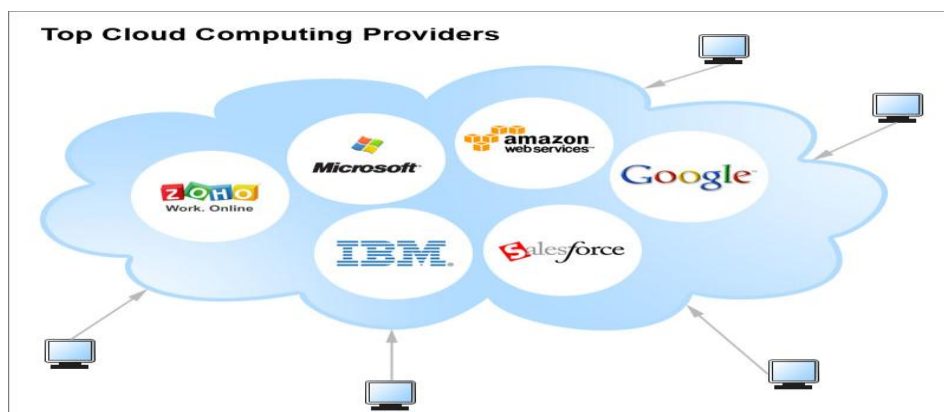
Od trenutka pojave cloud computing-a, na tržištu se pojavilo mnoštvo novih pružaoaca usluga, a taj trend se i dalje održava. Svaki od njih ima neke prednosti i nedostatke. Korisnici se odlučuju za one provajdere usluga koji najbolje zadovoljavaju njihove potrebe. Svaki korisnik ima drugačije potrebe i drugačije stvari su mu bitne. U prilog korisniku ide činjenica da svaki pružalac usluga ima drugačije osobine, čime se stvara pozitivna konkurentna atmosfera. Konkurencija prisiljava pružaoce usluga na neprekidnu potrebu za usavršavanjem i na snižavanje cena. Organizacije koje nude cloud computing usluge se moraju neprekidno razvijati i usavršavati, kako bi zadržale postojeće i pridobile nove korisnike njihovih usluga, ali isto tako i ostali konkurentni na tržištu.

Iznenadjujuće je podatak, da su pružaoci usluga međusobno dosta različiti. Dok su mnogi delovi usluge web hostinga prilično standardni (čuvanje podataka, obrada velike količine podataka, pristup različitim aplikacijama, nije potrebno kupovati hardver), definicija cloud computing-a jako varira. Amazonov Elastic Compute Cloud nudi Linux servere s administratorskim pristupom i mogućnost pokretanja bilo koje aplikacije. Google-ov App Engine takođe omogućava pokretanje bilo kojeg programa napisanog u Pythonu koji koristi Google-ovu bazu podataka. Cloud computing daje mogućnost korišćenja više procesora kad god se pojavi potreba za tim, ali oni ne mogu rešiti probleme ravnomernog raspoređivanja i čuvanja podataka. Najveći izazovi i problemi se javljaju na nivou arhitekture tako da jednostavno pokretanje više procesora neće rešiti problem osnovnih grešaka u dizajnu.

Oblaci su jedna od mogućnosti čuvanja podataka koja poseduje veliki potencijal, ali tradicionalni web hosting i dalje ima značajne prednosti nad njima. Korišćenje oblaka pojednostavljuje neke stvari, ali i dalje ne zadovoljava u potpunosti želje korisnika.

Neki od provajdera koji nude cloud computing usluge su:

- Amazon
- Google
- GoGreed
- AppNexus...



Slika 11.  
Cloud computing provajderi

### *Amazon Elastic Compute Cloud*

Amazon i dalje važi za jednog od provajdera koji klijentima nudi najširi diapazon usluga. Amazon je bio jedna od prvih organizacija koja je lansirala rešenje namenjeno široj javnosti. Ako je korisniku potrebno više procesora, on može ubrzati virtualne mašine sa EC2 (Elastic Compute Cloud) web uslugom. Ako korisnik ima potrebu za čuvanjem podataka, on može sačuvati do 5 GB podataka u S3 sistemu (Simple Storage Service). Amazon je izgradio i novi sistem korišćenja baze podataka, međutim on je i dalje u test verziji. Da bi se dobilo na brzini i efikasnosti,

<sup>8</sup> Slikovni prikaz najpoznatijih provajdera Cloud computing usluga

korisnikov računar može direktno da komunicira sa Amazonovom SQS uslugom (Simple Queue Service) i API-em (Application Programming Interface) za slanje poruka.

Korisnik šalje naredbe vlastitom setu servera u “oblaku” tako što se služi sigurnosnim alatima i upisivanjem naredbi u linije za upisivanje podataka. Svi virtualni serveri koriste neki od Linux operativnih sistema. Korisnik bira sopstveni virtualni server na koji želi da instalira sopstvene programe i korisničke instalacije. Ako korisnik rezerviše dovoljno prostora na oblaku, učitavanje operativnog sistema zajedno sa željenim aplikacijama se odvija jako brzo.

### *Google App Engine*

Google App Engine nudi potpuno druge mogućnosti u odnosu na Amazon. Dok kod Amazona korisnik dobija administratorska ovlašćenja, na App Engine-u Google je iz sigurnosnih razloga zabranio korisniku upisivanje podataka izvan sopstvene baze. Ako korisnik želi da sačuva podatke mora da koristi Google-ovu bazu podataka.

Rezultat svih tih ograničenja nije nužno loša stvar. Web aplikacije su ogoljene do samog osnovnog skupa osobina i sagrađeno je prilično dobro okruženje za njihovu dostavu. Google nudi neke dobre alate za pronalaženje grešaka u aplikacijama na korisnikovom računaru. Interesantna stvar je što Google insistira na povezivanju korisnikovog broja mobilnog telefona i Gmail korisničkog imena.

App Engine najčešće koriste grupe ili individualni korisnici koji u Python-u žele da napišu deo interfejsa, koji se nalazi između korisnika i baze podataka. API je upravo namenjen ovoj grupi korisnika.

### *GoGrid*

GoGrid predstavlja svetski cloud computing servis sa više cloud servera. Sa funkcionalnog aspekta ponuda GoGrid-a ne razlikuje se mnogo od onoga što nudi Amazonov EC2. Za razliku od Amazonovog EC2, njegov web control panel korisnicima je ipak mnogo praktičniji za korišćenje od EC2-ove komandne linije u koju korisnici Amazona upisuju naredbe za upravljanje sopstvenim virtualnim mašinama. Nije potrebno upisivanje nikakvih naredbi u komandne linije već se sve akcije odvijaju putem jednostavnog grafičkog interfejsa. Za vreme korišćenja usluga korisnici svo vreme imaju uvid u dosadašnje troškove. To je jako bitno za praćenje materijalnih troškova vezanih uz usluge koje se koriste.

GoGrid nudi mnoštvo operativnih sistema spremnih za upotrebu. Ako je korisniku potreban neki od Windows operativnih sistema, uz adekvatnu naknadu, omogućeno mu je korišćenje Windows Server 2007 operativnog sistema sa Microsoft SQL server paketima. Postoji uobičajena zbirka CentOS/Fedora i LAMP rešenja. Amazonov SimpleDB nudi više cloud usluga za zajedničko skladištenje informacija. Jedan od ključnih problema koji se može javiti jeste nemogućnost prestanka plaćanja usluge, jer u slučaju prestanka plaćanja usluge dolazi do brisanja servera, a to znači potpuni gubitak podataka koji se u tom trenutku na njemu nalaze.

### *AppNexus*

AppNexus provajder je dobar izbor za korisnike kojima se sviđa ideja cloud computing-a, ali nisu sigurni da li žele da napuste korišćenje jezgra Unix operativnog sistema i pojedinih administratorskih alata. AppNexus koristi hiljade servera koji su raspoređeni u četiri data centra na dva kontinenta. AppNexu se služi najboljim alatima za zajedničko učitavanje i čuvanje podataka, takođe se bavi prodajom malih delova servera neposrednim korisnicima. AppNexus pruža nekoliko apstraktnih komandnih naredbi koje omogućavaju korisnicima uključivanje i isključivanje servera kao i mogućnost pristupa bazi podataka.

Osnovne funkcionalnosti AppNexus oblaka su slične Amazonovom EC2. Korisnik se prijavljuje preko komandne linije i pokreće pripremljenu distribuciju operativnog sistema Linux. U slučaju potrebe, AppNexus može ponovo da pokrene virtualni server iz drugih izvora (poput Amazonovog EC2). Korisnici na jednostavan način mogu da prate čuvanje i deljenje podataka unutar mreže servera (cluster).

AppNexus se služi CDN sistemom (Content Delivery Network). CDN predstavlja mrežu servera za čuvanje podataka koji poseduju ugrađen sopstveni skup HTTP servera. Podaci postaju dostupni odmah nakon što ih korisnik zapiše u “/cdn” mapu, a AppNexus raspodeljuje podatke u “oblaku” za čuvanje podataka kako bi stvorio više nezavisnih data centara.

Kada korisnik želi da koristit usluge cloud computing-a on mora da sa provajderom usluga sklopi ugovor. Ugovori koji se sklapaju su specifični i jasni. U njima su navedeni uslovi koje korisnik mora da poštuje kao i mogućnosti koje provajder usluga potpisivanjem ugovora dobija.

Na primer, GoGrid u ugovoru navodi vrednosti poput vremena čekanja, menjanja faze signala, gubitka paketa i dr. Ako sistem ne zadovoljava navedene vrednosti GoGrid obećava davanje svojih usluga u iznosu 100 puta većem od izgubljenog iznosa.

Amazon nakon potpisivanja ugovora sa korisnikom o korišćenju usluge cloud computing-a, ima pravo da ukine korisnički račun i obriše sačuvane podatke. Amazon pri tome nije u obavezi da navede korisniku nikakav poseban razlog brisanja korisničkih podataka.

Google korisnicima ipak nudi malo bolje uslove vezane za pravo brisanja korisničkih podataka. Google će ukinuti korisnički račun samo ako korisnik ne poštuje uslove ugovora ili učini nešto ilegalno. Potpisivanje ugovora između Google-a i korisnika podrazumeva da Google ima pravo skeniranja, pregledanja, obeležavanja, filtriranja, menjanja, odbijanja i/ili uklanjanja bilo kojeg dela ili kompletnog sadržaja sa servera.

Provajderi cloud computing usluga su jako fleksibilni pri izgradnji mreže uređaja. Veliki problem je mogućnost rušenja servera ili gubitka podataka sa diska za vreme obavljanja određenog posla.

Ako korisnik želi da na sigurnost podataka ne utiče problem s bilo kojim serverom unutar "oblaka", mora ih sačuvati u tzv. "memoriju oblaka", ali to je jako skupo. Cena je pri tome mnogo viša od uobičajene jer je nivo usluge viši.

Svaka od organizacija ima drugačije načine naplaćivanja svojih usluga. GoGrid ima Intel Xeon servere, koje smatraju jačim nego što su serveri drugih organizacija. Iz tih razloga GoGrid povećava cenu svojih usluga. Na primer, Google ne naplaćuje svoju uslugu po vremenu trajanja usluge, već po broju ciklusa CPU-a. Amazon EC2 ima mašine uobičajene veličine, ali i one koje imaju veći kapacitet od uobičajenih, pa ih zato i više naplaćuje. Kada se troškovi menjaju, organizacije često smanjuju cene, ali ih isto tako i povećavaju kada se ispostavi da je cena usluge bila viša od očekivane. U priloženim tabelama može se videti kolike su bile cene navedenih cloud computing usluga različitih provajdera.<sup>9</sup>

| RESURSI                         | JEDINICA      | CENA U \$ |
|---------------------------------|---------------|-----------|
| Premeštanje podataka na server  | GB            | 0,12      |
| Premeštanje podataka sa servera | GB            | 0.10      |
| Vreme CPU                       | sati rada CPU | 0.10      |
| Čuvanje podataka                | GB mesečno    | 0.15      |

Tabela 1. Cene Google-ovih cloud computing usluga

| RESURSI                         | JEDINICA      | CENA u \$ |
|---------------------------------|---------------|-----------|
| Premeštanje podataka na server  | GB            | 0.10      |
| Premeštanje podataka sa servera | GB            | 0.15      |
| Vreme CPU                       | sati rada CPU | 0.12      |
| Čuvanje podataka                | GB mesečno    | 0.15      |

Tablica 2. Cene Amazonovih cloud computing usluga

| RESURSI                         | JEDINICA      | CENA u \$ |
|---------------------------------|---------------|-----------|
| Premeštanje podataka na server  | G             | 0.10      |
| Premeštanje podataka sa servera | G             | 0.14      |
| Vreme CPU                       | sati rada CPU | 0.125     |
| Čuvanje podataka                | GB mesečno    | 0.15      |

Tabela 3. Cena Microsoft-ovih cloud computing usluga

## 7. VPN kao najčešće primenjivani oblik Desktop virtualizacije, bezbednosni problemi i njihova rešenja

Koncept virtuelnih privatnih mreža (VPN) sastavljen je iz dva dela: virtuelne mreže, koja leži na vrhu sveprisutne interkonekcije na Internetu, i privatne mreže za poverljivu komunikaciju i ekskluzivnu upotrebu. U frazi VPN ono "virtuelna" implicira da ne postoji izdvojena fizička mrežna infrastruktura. Umesto toga, imamo fizički jednu mrežnu infrastrukturu (Internet), koju deli veliki broj različitih logičkih

<sup>9</sup> Komparativni tabelarni prikaz cena Cloud computing usluga različitih provajdera

mreža (podmreža). Na primer, možete koristiti isti mrežni pristupni tok za pristup Internetu, za konekciju na različite korporativne sajtove, i za pristup drugim poslovnim mrežama. Ovakve virtuelne mreže omogućavaju konstrukciju dodatnih logičkih mreža samo izmenom konfiguracije različitih uređaja. VPN obezbeđuje brži razvoj i smanjenje troškova koji bi se utrošili na postavljanje fizičke infrastrukture. Međutim jedan od najbitnijih aspekata virtuelnih mreža je "privatnost". Osnovni cilj privatnih mreža je održavanje poverljivosti informacija (podataka), tako da oni mogu biti primljeni samo od strane onih kojima su i upućene. Kada se komunikacija odvija u nekom od javnih medija, Interneta, šifrovanje informacije je jedina solucija za zaštitu podataka.

### 7.1. Bezbednost

Virtuelna privatna mreža (VPN) predstavlja poseban način komunikacije računara preko Internet ili Intranet infrastrukture. Tri su osnovne primene VPN-a:

- Pristup udaljenom računaru
- Povezivanje lokalnih mreža preko Interneta
- Povezivanje lokalnih mreža preko Intraneta

Najvažniji razlog korišćenja virtualnih privatnih mreža je ekonomski, ali virtualne privatne mreže pružaju i sledeće sigurnosne prednosti:

Omogućena je sveukupna kriptografija podataka. Virtualne privatne mreže obuhvataju celi promet koji se koristi, odnosno svi mrežni podaci koji se prenose su kriptovani. Na taj se način osigurava mrežni promet, tako da neovlašćene osobe nisu u mogućnosti da dođu do informacije koje unutrašnji računar koristi, koji je korišćeni protokol itd.

Pojedine protokole je zbog svoje funkcionalnost vrlo teško koristiti u sigurnom okruženju koje se postiže korišćenjem pakalnog filtriranja i proxy servisa. Virtualne privatne mreže omogućavaju kriptovanjem podataka, siguran udaljen pristup, korišćenjem ovih protokola.

Bilo da se radi o povezivanju samo jednog računara na udaljenu mrežu (kao u prvoj primeni), ili da se putem VPN-a povezuju dve mreže na udaljenim lokacijama (druga primena), komunikacija između subjekata ove strukture zaštićena je enkripcijom čije parametre dogovaraju obe strane. Izbor enkripcijskog algoritma i dužine ključa je od suštinskog značaja za sigurnost uspostavljene komunikacije, i tek u slučaju treće primene, gde komunikacija između mreža nije javna, enkripcija igra nešto manju ulogu.

Bezbednost je integralni deo VPN usluge. Postoji veliki broj pretnji VPN mrežama:

- Neovlašćeni pristup VPN saobraćaju
- Izmena sadržaja VPN saobraćaja
- Ubacivanje neovlašćenog saobraćaja u VPN ( *spoofing*)
- Brisanje VPN saobraćaja
- DoS ( *denial of service*) napadi
- Napadi na infrastrukturu mreže preko softvera za upravljanje mrežom
- Izmene konfiguracije VPN mreže
- Napadi na VPN protokole

Odbrana od VPN napada realizuje se i na korisničkom i na nivou provajdera VPN usluga:

- Kriptozaštita paketa
- Kriptozaštita kontrolnog saobraćaja
- Filteri
- Firewall
- Kontrola pristupa
- Izolacija

Tipovi virtuelnih privatnih mreža se zasnivaju na implementaciji više različitih protokola od kojih su najzastupljeniji: *IPsec bezbednosni protokol* i *SSL Protocol za zaštitu VPN*.

## 7.2. IPsec bezbednosni protokol

IPSec (Internet Protocol Security) je definisan RFC-ovima 4301 i 4309. Protokol radi na mrežnom sloju i implementiran je u verziji IPv6 protokola. IETF je formirao IP Security(IPSEC) radnu grupu čiji je zadatak da definiše standarde za VPN oblast. Ova radna grupa definisala je sledeće standarde:

- definisana su dva protokola zaštićenog prenosa Authentication Header (AH) i Encapsulating Security Payload (EPS)
- definisan način komunikacije uvođenjem pojma Security Associations (SA)
- definisan je način razmene ključeva posredstvom Interneta, Internet Key Exchange (IKE)

Iako ovaj protokol sve više prepušta svoje mesto znatno fleksibilnijem SSL protokolu veliki broj kompanija još uvek ga koristi za obezbeđivanje sigurne komunikacije. On se najčešće koristi u klasičnim VPN mrežama gde se na dve lokacije nalaze specijalizovani mrežni uređaji između kojih se uspostavlja IPsec konekcija. IPsec protokol podržava dva načina rada:

- Transport mode
- Tunnel mode

### 7.2.1. Tunelovanje

Tunelovanje je najvažnija komponenta tehnologije virtuelnih privatnih mreža koje su zasnovane na IPsec protokolu i predstavlja prenos paketa podataka namenjenih privatnoj mreži preko javne mreže. Ruteri javne mreže nisu svesni da prenose pakete koji pripadaju privatnoj mreži i VPN pakete tretiraju kao deo normalnog saobraćaja.

Tunelovanje ili enkapsulacija je metod pri kome se koristi infrastruktura jednog protokola za prenos paketa podataka drugog protokola. Umesto da se šalju originalni paketi, oni su enkapsulirani dodatnim zaglavljem. Dodatno zaglavlje sadrži informacije potrebne za rutiranje, odnosno usmeravanje paketa kroz mrežu, tako da novodobijeni paket može slobodno putovati transportnom mrežom.

Tunel predstavlja logičku putanju paketa kojom se on rutira preko mreže. Enkapsulirani podaci su rutirani transportnom mrežom sa jednog kraja tunela na drugi. Pojam tunel uvodi se jer su podaci koju putuju tunelom razumljivi samo onima koji se nalaze na njegovom izvoru i odredištu. Ovi paketi se na mreži rutiraju kao svi ostali paketi.

Početak i kraj tunela nalaze se u VPN mrežama. Kada enkapsulirani paket stigne na odredište vrši se deenkapsulacija i prosleđivanje na konačno odredište. Ceo proces enkapsulacije, transporta i deenkapsulacije paketa naziva se tunelovanje. Tehnologija tunelovanja koristi tri vrste protokola:

- Protokol nosač - ovi protokoli služe za rutiranje paketa po mreži ka njihovom odredištu. Tunelovani paketi imaju enkapsulaciju ovih protokola. Za rutiranje paketa po Internetu koristi se IP protokol.
- Protokol za enkapsulaciju - ovi protokoli služe za enkapsulaciju originalnih podataka, i koriste se za stvaranje, održavanje i zatvaranje tunela. Najčešće korišćeni su PPTP i L2TP protokoli.
- Transportni protokol enkapsulira originalne podatke za transport kroz tunel. Najpoznatiji su PPP i SLIP protokol.

#### 7.2.2. Transport mode

Osnovne karakteristike transportnog moda su:

- šifruje se samo korisnički deo IP datagrama
- ne menja se dužina IP datagrama
- zadržava se originalno IP zaglavlje što omogućava da se vidi ko su partneri u komunikaciji

#### 7.2.3. Tunnel mode

Osnovne karakteristike tunelskog moda su:

- Zajedno sa korisničkim delom IP datagrama šifruje se i originalno IP zaglavlje
- Dodaje se novo spoljno IP zaglavlje sa adresom sledećeg uređaja u mreži gde paket treba da stigne

Što se tiče IPsec protokola treba još reći da je tunelski mod znatno bezbedniji od transportnog moda. IPsec protokol se i dalje veoma često koristi za prenos zaštićenih podataka tamo gde nije neophodno da se za prebacivanje podataka sa jedne lokacije na drugu koristi Web pretraživač.

### 7.3. SSL protokol za zaštitu VPN

Secure Sockets Layer (SSL) je protokol za sigurno slanje poruka (komuniciranje) putem Interneta, koji omogućuje slanje poverljivih podataka putem Interneta u šifrovanom i sigurnom obliku. SSL protokol ostvaruje poseban komunikacioni sloj, koji je smešten na pouzdan transportni sloj (npr. TCP/IP), dok se na SSL smešta aplikacijski sloj. Od aplikacijskog sloja prima poruku koju

treba poslati, rastavi je u manje delove prikladne za šifrovanje, dodaje kontrolni broj, šifruje, eventualno kompresuje, a zatim te delove pošalje. Primalac primi delove, dekompresuje, dešifruje, proveriti kontrolne brojeve, sastavi delove poruke, pa ih preda aplikacijskom sloju. Na taj način se putem SSL-a ostvaruje zaštićeni kanal prenosa kroz mrežu. Ukoliko su klijent i server neaktivni duže vreme ili razgovor sa istim atributima zaštite potraje predugo, atributi se menjaju. SSL omogućava razmenu informacija između klijenta i servera, na transparentan način.

SSL se sastoji od dva pod-nivoa: SSL Record i SSL Handshake, i koristi još 4 podprotokola. Svi nivoi SSL su:

- SSL Record,
- SSL Handshake,
- ChangeCipher Spec
- Alert

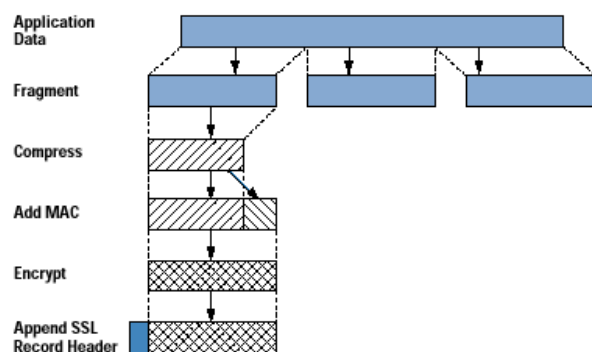
| SSL handshake protocol | SSL cipher change protocol | SSL alert protocol | Application Protocol (eg. HTTP) |
|------------------------|----------------------------|--------------------|---------------------------------|
| SSL Record Protocol    |                            |                    |                                 |
| TCP                    |                            |                    |                                 |
| IP                     |                            |                    |                                 |

Slika 13. Nivoi SSL protokola

*SSL Rekord protokol (Record Protocol)* se brine o šifrovanju–dešifrovanju informacija koje se prenose i tu uslugu pruža višim slojevima. U praksi to je obično HTTP (engl. Hypertext Transfer Protocol) preko koga Web čitači i serveri razmenjuju podatke. SSL Record sloj je odgovoran za prenos blokova informacija, između dva računara. SSL rekord protokol na predajnoj strani prihvata podatke od aplikacijskog sloja, vrši njihovu fragmentaciju u blokove, opciono komprimuje podatke, dodaje autentifikaciju (MAC - message authentication code), šifruje podatke, dodaje zaglavlje i predaje TCP sloju radi slanja. Na prijemnoj strani podaci se preuzimaju od TCP sloja, dešifruju, izračunava se i poredi MAC radi provere verodostojnosti, vrši dekompresija podataka, defragmentacija i na kraju podaci se predaju aplikacijskom nivou.

Aplikacijski podaci se dele na blokove ne veće od  $2^{14}$  (16384) bajtova. Kompresija se opciono sprovodi i mora biti bez gubitaka. Nad kombinacijom komprimovanih podataka, parametrima kompresije i simetričnog MAC ključa izračunava se sažetak poruke po algoritmu MD5 ili SHA-1 i tako osigurava autentičnost poruke.

Komprimovani podaci i MAC se zatim šifruju dogovorenim algoritmom za šifrovanje simetričnim ključem.



Slika 14. SSL Rekord protokol (Record Protocol)

### SSL Handshake protokol

Ovaj protokol upravlja razmenom ključeva, obaveštenja i promene lozinki. Ovi nivoi se nalaze na vrhu sloja za prenos podataka, koji je obično TCP sloj. Najsloženiji je deo SSL-a. Ovaj protokol omogućava: proveru identiteta klijenta i servera, pregovaranje oko upotrebe algoritma za šifrovanje i izračunavanje sažetka poruke i razmenu PreMasterSecret, koja se koristi za generisanje identifikacionih i šifrovanih ključeva kroz MasterSecret. Koristi se u fazi uspostavljanja konekcije pre bilo kakve razmene podataka iz sloja aplikacije.

Poruke koje se razmenjuju u okviru ovog protokola imaju sledeću strukturu:

| 1 bajt | 3 bajta | $\geq 1$ bajta |
|--------|---------|----------------|
| Tip    | Dužina  | Sadržaj        |

Polje "tip" je veličine 1 bajt, i označava jednu od deset vrsta poruka. Polje "dužina" sadrži dužinu poruke u bajtovima. Konačno, polje "sadržaj" ne može biti manje od 1 bajta, i sadrži parametre koji su vezani za poruku.

Razmena poruka može grupisati u četiri faze. Prva faza se koristi za pokretanje logičke veze i uspostavljanje sigurnosnih kapaciteta koji su povezani sa određenim razgovorom. Obično, ova razmena je pokrenuta od strane klijenta koji šalje ClientHello poruku. Druga faza se sastoji od serverove provere identiteta, tako što on šalje svoju potvrdu. Razmena ključa i zahtev za klijentovom potvrdom može biti deo ove faze. Server označava kraj ServerHello poruke, tako što šalje ServerHelloDone poruku. U trećoj fazi, klijent šalje svoju potvrdu (ako je zahtevana), potom razmenjuje PreMasterSecret sa serverom, i može poslati proveru potvrde. Poslednja faza završava proces podešavajući sigurnu vezu. Klijent šalje ChangeCipherSpec poruku i kopira sigurnosne parametre(Cipher Spec) u trenutne sigurnosne parametre, i govori klijentu da započne šifrovani režim rada. Posle toga, klijent šalje Finished poruku pod novom sigurnosnom šemom. Finished poruka proverava da li su procesi razmene ključeva i identifikacije bili uspešni. Bitno je napomenuti da ChangeCipherSpec poruka nije deo Handshake protokola. Kada je razgovor uspostavljen, može se desiti da je potrebno uspostaviti novu vezu, koja se sastoji od novih parametara Client\_Random i Server\_Random, sa ClientHello i ServerHello porukama, dok u isto vreme, čuva algoritme za šifrovanje i "hash" koji su već izabrani. Nova provera identiteta se izbegava i, suprotno nego kod uspostavljanja razgovora,

ClientHello i ServerHello poruke su šifrovane. Klijent i server potvrđuju njihovu razmenu šaljući ChangeCipherSpec poruku sa obe strane i završavajući skraćeni "handshake" sa Finished porukom.

### *SSL ChangeCipherSpec protocol*

Ovaj protokol je najjednostavniji od svih SSL protokola. Sastoji se od jedne poruke veličine 1 bajta koja nosi isto ime kao i protokol. On šalje poruku Record protokolu da šifrovanje može da počne sa sigurnosnim parametrima koji su usvojeni (razmenjeni). Svrha ove poruke je da izazove da se Cipher Spec stanje prekopira u trenutno Cipher Spec stanje, koje podešava cipher suite (niz parametara, kao što su: odabir algoritma, veličina ključa, i dr.) koji će biti korišćen u razgovoru ili vezi od strane Record sloja.

### *SSL Alert protocol*

Ovaj protokol, u osnovi šalje poruke obaveštenja kada se desi greška i prikazuje promenu stanja, kao što je kraj veze. U osnovi, postoje dve vrste poruka, u zavisnosti od ozbiljnosti napada. Svaka poruka sastoji se iz dva bajta. Prvi bajt može da ima vrednost warning (1) ili fatal (2), ako je vrednost fatal konekcija se trenutno raskida. Drugi bajt sadrži kod upozorenja. Poruka upozorenja je samo upozorenje i neće tražiti nikakvu akciju. Fatalna greška šalje određenoj strani poruku da odmah zatvori vezu, bez čekanja na potvrdu od prijemne strane. U trenutku slanja i primanja takve poruke, obe strane zatvaraju sesiju (vezu). Server i klijent su u tom slučaju dužni da zaborave bilo kakve podatke o sesiji, identifikatore sesije, ključeve i ostale tajne koje su vezane uz sesiju.

Ovaj protokol može biti pokrenut u zavisnosti od situacije: od strane aplikacijskog sloja, da inicira kraj veze, od strane Handshake protkola ako se desio problem, od strane Record protokola kada integritet poruke nije u redu. Sa druge strane, zato što fatalna poruka izaziva kraj razgovora, SSL je ranjiv na denial-ofservice (otkaz servisa) napade, ako napadač uspe da zameni originalne poruke sa novom porukom, koja će učiniti da razgovor bude prekinut.

### *Sesija(session)*

Razgovor (session) može sadržati više veza (connections). Identifikacija se utvrđuje za svaki od razgovora, i sledeći parametri ostaju konstantni tokom razgovora:

- 1) redni broj razgovora (ID),
- 2) potvrda,
- 3) algoritam za kompresiju,
- 4) algoritmi za šifrovanje i potpis, i
- 5) MasterSecret koji se razmenjuje između klijenta i server

Za svaku novu vezu u razgovoru, "handshake" postavlja sledeće parametre: dva slučajna broja, jedan za klijenta a drugi za server, parametre "hashing"

algoritma na klijentskoj strani i serverskoj strani, blok šifrovanih ključeva za klijenta i servera, inicijalni vektor za blok šifrovanja na obe strane. Niz brojeva je specifičan za svaku vezu, i on se inicijalizuje posle poruke ChangeCipherSpec. Kad god se klijent spoji na server, novi razgovor je pokrenut. Ako se isti klijent spoji na drugi server, novi razgovor će biti pokrenut bez prekida prethodnog. Ako se klijent kasnije vrati na prvi server, i poželi da sačuva izabrane sigurnosne parametre koji su već napravljeni, klijent će zatražiti od servera da nastavi stari razgovor umesto pokretanja novog. SSL dokumentacija sugerise da se dužina razgovora limitira na 24 sata, ali stvarna dužina razgovora je obično određena na serveru. Record protokol koristi parametre tokom procesa povezivanja ("handshake") da bi ih prosledio transportnom sloju. U suštini, ovaj protokol je odgovoran za deljenje podataka na blokove i njihovo slanje na strani pošiljaoca, kao i za deljenje na strani prijema. Druge funkcija uključuju kompresiju, kao i šifrovanje i dešifrovanje poruka.

### *Generisanje ključa*

Postoje dva glavna dela u okviru SSL-a, veza i razgovor. Proces generisanja ključeva je vezan za momenat stvaranja određenog ključa. Takođe, tu postoji proces za stvaranje MasterSecret (glavne šifre) na početku razgovora, i različit proces koji generiše inicijalizacione vektore, ključeve za šifrovanje i ključeve za "hash" algoritam, koji se koristi za generisanje MAC-a (kontrolnog broja).

#### 7.3.1. Slabosti i ranjivosti SSL protokola

Rast i popularnost SSL aplikacija upućuje na opasnost od otkrivanja i iskorišćavanja sigurnosnih "rupa" u protokolu, koji bi mogli ugroziti sigurnost podataka koji se štite. Popularnost Interneta, i njegovih korisnika je u rastu svaki dan, i broj korisnika koji koriste elektronske transakcije raste isto tako. SSL je vrlo jeftin za implementaciju, i razvijen je kao brza solucija za potrebe sigurnosti u web aplikacijama, koje rade sa poverljivim podacima. To objašnjava više implementacija ovog protokola na Internetu. Međutim, kao i svaki drugim sistem, SSL nije u potpunosti siguran. SSL je dizajniran da osigura sledeće: poverljivost, integritet i proveru identiteta. Deo koji se odnosi na poverljivost je takav, da zlonamerna osoba može presresti osetljive informacije, u trenutku dok se šalju, ali se ti podaci ne mogu dešifrovati. Deo sa proverom identiteta je dizajniran da osujeti mogući "čovek u sredini" napad, gde su poverljivi podaci preusmereni od strane zlonamerne osobe. Servis za proveru identiteta je dobro implementiran kroz potvrde, mada je moguće da postane žrtva napada.

### *Korisnička ubeđenja i pretpostavke*

Jedan deo problema sigurnosti u vezi SSL-a, je preveliko poverenje koje korisnici imaju u ovaj protokol. Dosta poverenja razvijeno od strane korisnika:

- da SSL protokol nema mana;
- da je protokol ispravno ugrađen u Internet Explorer;
- i da je identifikacija potvrda u potpunosti proverena na sajtovima pre primene istih.

U drugim slučajevima, korisnici možda nemaju dovoljno znanje i osećaj za sigurnost poverljivih podataka. Na primer, ako se uzme za primer da zlonamerni web sajt koristi samopotpisane potvrde, tj. potvrde koje ovlašćena organizacija za identifikaciju potvrda nije odobrila. Kada browser pokuša da uspostavi SSL vezu, on će proveriti da li je potvrda koja je prisutna na serveru ispravna. Browser će utvrditi da potvrda nije potvrđena ni od jedne od poverljivih institucija za proveru potvrda, pa će postaviti pitanje korisniku da li želi da prihvati potvrdu koja nije potvrđena, i nastaviti proces povezivanja ako korisnik odgovori potvrdno. Međutim, u Internet Exploreru i Netscape-u, način na koji je prikazano obaveštenje ne objašnjava da postoji sigurnosni rizik za prihvatanje potvrda. Većina korisnika koja je suočena sa tom porukom, koju ne razume baš najbolje, će odgovoriti potvrdno sa "OK".

#### *Lista organizacija za izdavanje potvrda*

Jedna od glavnih mana implementacije SSL protokola je nedostatak adekvatne zaštite liste organizacija za overu i izdavanje potvrda, koju web browser smatra poverljivom i sigurnom. Ova lista može biti izmenjena od strane nekog opasnog virusa, kao što je crv, trojanac, ili neka druga vrsta napada. Zlonamerni kod može promeniti listu, i dodati SSL potvrdu u niz proverenih. Ova mana ugrožava komponentu za identifikaciju SSL-a, i pravi od komunikacije između klijenta i servera, potencijalnu žrtvu napada koja se naziva "čovek u sredini".

#### *Napad ubacivanjem potvrda*

Ova vrsta napada je usmerena na ranjivost liste organizacija za izdavanje potvrda u Windowsu. Zlonamerna SSL potvrda može biti ubačena u browser-ovu listu poverljivih organizacija za proveru potvrda. Zbog toga je bitno ugraditi (update-ovati) sve aplikacije na najnovije verzije koje su moguće, jer se tako uklanjaju sigurnosne "rupe" u programima. Veličina ove pretnje je proporcionalna broju nezaštićenih i neobezbeđenih sistema, koji su još uvek ranjivi na ovu vrstu napada. U korporacijskim mrežama i serverima gde su sigurnosni sistemi pravilno održavani, opasnost je znatno manja. Međutim, kućni korisnici ne održavaju svoje računare u najsigurnijem stanju, pa su tako moguće velike izmene u njihovim sistemima. Drugi faktor koji omogućava ovu vrstu napada je operativni sistem. U korporacijskim mrežama moguće je koristiti datoteku i dozvole i registry bazu kroz listu pristupa za sprečavanje pristupa listi organizacija za proveru potvrda.

#### *Napad "Čovek u sredini"*

Ovaj napad se dešava kada korisnik pošalje zahtev serveru, misleći da je spojen na odgovarajući web sajt, dok se u stvari, ovaj zahtev šalje zlonamernom web serveru koji prosleđuje svoj sadržaj na pravi web sajt. Korisnik nepažljivo

otvara SSL vezu prema zlonamernom web serveru, čiju potvrdu prihvata browser. Korisnik vidi sličicu katanca u browseru, i videvši to šalje poverljive informacije kroz mrežu. Budući da je sa druge strane mreže zlonamerna strana, ona može odmah dešifrovati informacije, koje će kasnije proslediti na pravi sajt kroz drugu SSL vezu. I korisnik, i pravi web sajt neće primetiti zlonamernu stranu, budući da obojica šalju i primaju zahteve kroz "ispravnu" SSL vezu.

### *Cipher suite - povratni napad*

Jedan od glavnih propusta SSL protokola, odnosno njegove verzije 2.0, je cipher suite (niz parametara, kao što je algoritam za šifrovanje, itd.) povratni napad. Ovaj propust je ispravljen u verziji 3.0, ali još uvek postoji izvestan broj korisnika verzije 2.0. Ovaj napad se sastoji od toga da zlonamerna osoba neprimetno primorava korisnika da koristi slab algoritam za šifrovanje, iako postoje mnogo jači algoritmi. Ova vrsta napada se izvodi tako što se menja podržana lista cipher - suite parametara, koja se šalje tokom protokola povezivanja, i koja se šalje kao tekst kroz Hello poruku. Verzija 3.0 ovog protokola je rešila ovaj problem tako što obavlja identifikaciju svih poruka Handshake protokola kroz MasterSecret, tako da bi napadač mogao biti otkriven na kraju protokola i veza bi mogla biti prekinuta, ako je potrebno. Sve poruke Handshake protokola se šalju nešifrovane, ali umesto promene parametara koji se koriste, protokol razmene ključeva menja trenutno stranje veze. Pošto je povezivanje završeno, obe strane šalju poruku ChangeCipherSpec, koja obaveštava drugu stranu da izmeni svoje trenutno stanje veze na novo. Novo stanje veze se koristi od sledeće poruke. Posle ChangeCipherSpec poruke odmah se šalje Finished poruka, koja se sadrži MAC (kontrolni broj) na svim porukama Handshake protokola zaključanim od strane MasterSecreta. 48-bitni MasterSecret se nikad ne otkriva, umesto toga se ključevi veze generišu od njega. Finished poruka je zaštićena sa novo uspostavljenim parametrima veze (cipher suite). Ni jedna od strana u komunikaciji ne bi trebala prihvatiti podatke, sve dok se ne primi poruka Finished. Tok poruka ide na sledećim redosledom:

1.  $K \rightarrow S: [\text{ChangeCipherSpe}]$
2.  $K \rightarrow S: [\text{Finished:}] \{a\}_k$
3.  $S \rightarrow K: [\text{ChangeCipherSpc}]$
4.  $S \rightarrow K: [\text{Finished:}] \{a\}_k$
5.  $K \rightarrow S: \{m\}_k$

Gde  $\{*\}_k$  predstavlja zaključanu šifrovanu transformaciju koju koristi Record sloj,  $m$  označava tekstualnu poruku koja se šalje pošto je razmena ključeva završena, dok  $a$  predstavlja identifikacioni kod Finished poruke, koji je dobijen izračunavanjem simetričnog MAC-a na prethodnim "handshake" porukama.

### *Problem male dužine ključeva*

Sjedinjene Američke Države imaju dužu istoriju sprečavanja dužine ključeva za šifrovanje koji su namenjeni izvozu. Pre decembra 1998. godine, proizvodi za šifrovanje koji su izvoženi iz Sjedinjenih država nisu smeli imati više od 40-bitnog

simetričnog ključa za šifrovanje, ili 512-bitnog asimetričnog. Nekada je RSA<sup>10</sup> kao minimum u svojim algoritmima za enkripciju asimetričnim ključem upotrebljavao dužinu od 1024 bit-a, što odgovara 80-bitnom simetričnom ključu. RSA smatra da su asimetrični 1024-bitni ključevi, podložni razbijanju u velikoj meri već od 2010. godine i zato su u praksi već uveliko u upotrebi 2048-bitni ili 3072-bitni asimetrični ključevi, koji odgovaraju 112-bitnom odnosno 128-bitnom simetričnom ključu. Za informacije od najveće tajnosti preporučuje se upotreba 256-bitnog simetričnog ključa, što odgovara 15360-bitnom RSA asimetričnom ključu.

### 7.3.2. Komunikacija na bezbedan način

Uređaji koji su se ranije koristili za bezbednu komunikaciju zvali su se VPN koncentratori i oni su radili sa IPsec protokolom. Ovakvi uređaji se koriste i danas a komunikacija preko njih zahteva da na klijentskom računaru bude instaliran specifičan softver koji se zove VPN klijent. Za razliku od klasičnog VPN-a zasnovanog na IPsec protokolu, SSL VPN je konstruisan tako da nema potrebe za posebnim podešavanjem korisničkih računara. Bilo koji računar koji ima Web pretraživač može bez problema da pristupa SSL VPN mreži.

Korisnici mogu bezbedno da pristupaju kompanijskoj mreži sa bilo kog računara bilo da je to računar na javnom mestu, laptop računar ili čak mobilni telefon. SSL VPN je multifunkcionalni višenamenski uređaj<sup>11</sup>, a o nekim od njegovih mnogobrojnih funkcionalnosti biće više reči u ovom poglavlju. Jedna od funkcija je da bude gateway i da obezbedi korisnicima koji dolaze spolja pristup unutrašnjim servisima kao što je fajl server, e-mail server kao i Web orijentisanim aplikacijama koje su šifrovane korišćenjem SSL protokola. Mnoge poznate svetske kompanije prilagođavaju svoja rešenja zahtevima SSL VPN tehnologija koje se sve više razvijaju.

#### *SSL VPN uređaji*

Sve više poznatih proizvođača mrežne opreme nudi specijalizovane hardverske uređaje za SSL VPN mreže. Oni su različitih performansi i karakteristika ali je zanimljivo istaći da pored osnovne uloge da zatvaraju VPN konekcije odnosno da budu VPN koncentratori imaju i mnoge dodatne pogodnosti. Te pogodnosti koje nude usko su povezane sa sve dinamičnijim razvojem računarskih mreža, virtualnih privatnih mreža, a posebno sa razvojem Interneta koji nudi dosada nezamislive mogućnosti.

Kao što je već rečeno SSL VPN uređaj je višenamenski hardverski ili virtualni uređaj koji osigurava bezbednu kontrolu pristupa i bezbednu komunikaciju do lokalne mreže odnosno namenskog ili cloud servera. Ovi uređaji imaju sopstveni operativni sistem što im pruža mogućnost da se koriste bilo u Windows ili Linux okruženju. SSL VPN uređaj može da ima neke od sledećih funkcionalnosti:

---

<sup>10</sup> RSA(RSA Security LLC) je Amrička kompanija koja se bavi računarstvom i bezbednošću mreža. Njeni osnivači, su ujedno i tvorci čuvenog RSA algoritma za asimetričnu kriptografiju.

- Rad sa digitalnim sertifikatima (samopotpisanim ili sertifikatima drugih CA)
- Revers proxy
- Split tunneling
- Mrežni firewall
- Application firewall
- Intrusion prevention system
- Ddos protection
- Load balancing
- Rad sa grupnim polisama
- Kontrola radne stanice sa koje korisnik pristupa (verzija operativnog sistema, antivirus)

Za ostvarivanje bezbedne komunikacije između klijentskih radnih stanica i udaljenih server korišćenjem security servisa nisu potrebne sve navedene funkcionalnosti. Ono što je neophodno da bi security servis upšte mogao da funkcioniše jeste mogućnost SSL VPN uređaja da radi sa digitalnim sertifikatima. Kao što je poznato ovaj zahtev se prosleđuje sertifikacionom telu koje izdaje digitalni sertifikat koji se zatim prenosi na uređaj. Ova mogućnost pruža ozbiljnu prednost prilikom konfigurisanja virtualne privatne mreže, jer više nije potrebno da se request generiše na posebnom Web serveru već SSL VPN uređaj postaje uslovno rečeno Hardware Security Modul (HSM). To podrazumeva da se tajni ključ serverskog sertifikata čuva na specijalizovanom hardverskom uređaju u koga napadači veoma teško mogu da uđu. Što se tiče rada sa grupnim polisama one mogu da se čuvaju u samom uređaju mada postoji i varijanta da im se pristupa kroz LDAP, aktivni direktorijum ili preko RADIS servera.

Antivirus, antispam, anti phishing zaštita funkcioniše tako što je SSL VPN neprekidno povezan sa podrškom kompanije čiji je proizvod u pitanju i koja redovno prati i otkriva nove definicije zlonamernog koda i generiše mehanizme za zaštitu od njih. Web Application Firewall integrisan na ovaj uređaj obezbeđuje odbranu od najčešćih napada koji Web aplikacijama prete preko Interneta. Najčešće to podrazumeva zaštitu od DoS ili DDoS napada, SQL injection napada, CSS napada kao i mnogih drugih pretnji koje mogu da ugroze Web aplikacije. Web Application Firewall funkcioniše tako što je neprekidno povezan sa podrškom kompanije čiji je proizvod u pitanju i koja redovno prati i otkriva nove definicije zlonamernog koda i generiše mehanizme za zaštitu od njih.

Reverse proxy je proxy server koji radi u ime nekog mrežnog servera. Najčešće korišćenje reversnog proxy-ja je da se zaštiti Web server. Kada korisnik na Internetu zahteva podatke od Web servera koji je zaštićen reversnim proxy serverom, reverse proxy presreće zahtev i proverava da li su podatci sadržani u zahtevu prihvatljivi, i da ne sadrže neke ne-HTTP podatke ili neke maliciozne HTTP komande. Ovo obezbeđuje da korisnici na Internetu nikada ne pristupaju direktno Web serveru.

Postoji nekoliko tipova SSL VPN-a čije će karakteristike ovde biti detaljnije opisane.

Dva glavna tipa SSL VPN-a su:

- SSL portal VPN
- SSL tunnel VPN

Takođe, postoji i treći tip koji se zove SSL gateway-to-gateway VPN koji se primenjuje u pojedinim implementacijama. On se retko koristi jer ima slične karakteristike kao IPsec VPN ali je manje fleksibilan pa se zbog toga ovde neće detaljnije opisivati.

Oba glavna tipa SSL VPN mreža se koriste da bi se obezbedio pristup za udaljene korisnike brojnim servisima koje kontroliše i kojima upravlja SSL VPN uređaj. U zavisnosti od potreba korisnika treba obezbediti optimalno rešenja jer oba pristupa imaju svoje prednosti i nedostake.

### *SSL portal VPN*

SSL portal VPN dozvoljava korisnicima da koristeći standardnu SSL konekciju bezbedno pristupaju brojnim mrežnim servisima. Ovaj pristup se naziva SSL portal VPN zato što se preko jedne Web stranice pristupa svim ostalim resursima. Ova vrsta SSL VPN-a radi u transportnom sloju preko posebnog mrežnog porta čiji je pun naziv TCP port za SSL-protected HTTP (443). Udaljeni korisnici pristupaju na SSL VPN gateway koristeći bilo koji od postojećih Web pretraživača gde se autentifikuju metodom koju taj gateway podržava. Nakon toga prikazuje im se Web stranica koja predstavlja portal prema drugim servisima. Ovi servisi mogu da budu linkovi prema Web serverima, deljenim direktorijumima sa datotekama, Web-based email sistemima, aplikacijama koje su pokrenute na zaštićenim serverima kao i svemu ostalom čemu se može pristupati preko Web stranice.

Da bi pristupili SSL portal VPN-u korisnici unose u Web pretraživač URL portala na koji žele da se konektuju na isti način kao kada pristupaju bilo kom drugom Web sajtu. Ovaj URL najčešće koristi https šemu koja odmah startuje SSL konekciju, ali mnogi SSL VPN-ovi dozvoljavaju korisnicima da prvo pristupe portalu koristeći http URL, a da zatim budu redirektovani na bezbedan SSL port.

SSL portal VPN-ovi rade sa Web pretraživačima bez obzira na to da li Web pretraživač dozvoljava ili podržava aktivan sadržaj. Zbog toga je SSL portal VPN pogodniji za pristup većem broju korisnika nego što je to SSL tunnel VPN. Kada korisnik treba da pristupi nekoj Web aplikaciji gde se zahteva veća sigurnost SSL portal VPN nije preporučljiv.

### *SSL tunnel VPN*

SSL tunnel VPN dozvoljava korisnicima da koristeći običan Web pretraživač bezbedno pristupaju brojnim servisima kroz tunel koji je pokrenut preko SSL-a. On zahteva da Web pretraživač podržava specifične tipove aktivnog sadržaja (Java, JavaScript, Flash ili ActiveX) kojima korisnik može da upravlja. Većina Web pretraživača koji podržavaju ove aplikacije takođe dozvoljavaju korisnicima ili administratorima da blokiraju njihovo izvršenje.

Kada se govori o SSL tunnel VPN-u pojam „tunnel“ ima sličnosti ali i razlike sa istim pojmom u IPsec VPN-u. Sličnost je u tome što je ceo IP saobraćaj potpuno zaštićen tunelom i na taj način korisniku je omogućeno da na bezbedan način pristupa željenim mrežnim servisima. Razlika je u tome što je SSL VPN tunel kreiran preko SSL-a i ne koristi iste protokole za tunelovanje kao IPsec. Kada se koristi SSL tunnel VPN neophodno je da se na klijentskoj strani instalira plag-in koji omogućava uspostavljanje tunela između klijenta i SSL VPN gateway-a. Ovakav plag-in može da se instalira unapred ili prilikom povezivanja Web pretraživača sa SSL VPN uređajem. Najčešće se kao plag-in koristi ActiveX kontrola ali je problem u tome što ona može pouzdano da se koristi samo kroz Internet Explorer. Drugo rešenje predstavlja plag-in koji je napravljen kao Java Applet i koji može da radi na bilo kom Web pretraživču.

## 8. Bezbednost u cloud computing-u

Cloud computing obiluje sigurnosnim rizicima. Korisnik bi pre nego što odabere provajdera, čiju uslugu cloud computing-a će koristiti, trebao najpre da obavi procenu sigurnosti korišćenja ove tehnologije. Korisnici, takođe, treba da zahtevaju transparentnost podataka i da izbegavaju pružaoce usluga (provajdere) koji odbijaju da pruže detaljne informacije o sigurnosnim problemima.

Cloud computing poseduje jedinstvena obeležja koja zahtevaju procenu rizika na sledećim poljima: integritet, oporavak, privatnost, pravni problemi u područjima inovacije, revizije, nadzorne usklađenosti...

Specifični sigurnosni rizici:

*Privilegovani korisnički pristup* - Obrada osetljivih podataka izvan organizacije sa sobom nosi određeni nivo rizika. Spoljašnje usluge zaobilaze fizičke i logičke provere i nadzor osoblja. Korisnici bi trebalo da traže informacije o zapošljavanju i nadzoru privilegovanih administratora. Takođe bi korisnici trebalo da se raspitaju o ovlašćenjima koja administratori poseduju kada je u pitanju pristup njihovim podacima.

*Nadzorna usklađenost* – Korisnici su odgovorni za sigurnost i integritet ličnih podataka čak i kada su oni sačuvani kod pružaoca usluga. Provajderi svoju pouzdanost i prednost u odnosu na konkurenciju dokazuju na taj način što se podvrgavaju spoljnim revizijama i sistemu sigurnosne sertifikacije. Postoje provajderi koji se ne podvrgavaju ovakvim sigurnosnim sistemima zaštite. Klijentima se ne preporučuje da bitne podatke čuvaju korišćenjem usluga cloud computing-a koje nude ovakvi provajderi.

*Adresa podataka* - Korisnik nema jasan uvid gde su njegovi podaci sačuvani. Na primer, on ne mora da zna čak ni u kojoj su državi njegovi podaci sačuvani. Klijent može od pružaoca usluge (provajdera) da zahteva čuvanje podataka na tačno određenim adresama i davanje ugovorne obaveze o poštovanju zahteva privatnosti u interesu korisnika.

*Odvajanje podataka* – Podaci se u oblaku najčešće nalaze u zajedničkom okruženju sa podacima drugih kkorisnika. Zaštitno kodiranje pri tome može biti korisno, ali ne

rešava sve probleme. Provajderi bi trebalo da pruže dokaze da su osmišljene šeme zaštitnog kriptovanja ispitane. Greške u zaštitnom kriptovanju mogu učiniti podatke potpuno neupotrebljivim.

*Oporavljanje* – Iako klijent ne zna gde su njegovi podaci sačuvani, provajder bi trebalo da saopšti korisniku šta će se dogoditi sa podacima u slučaju neplaniranih nesreća. Svaka ponuda provajdera koja ne nudi redundanciju podataka i aplikacija na više različitih mesta je ranjiva i podložn trajnom gubitku podataka.

*Podrška istraživanja* – Istraživanje neprikladnih ili protivzakonitih aktivnosti mogu biti nemoguća ili jako složena korišćenjem cloud computing-a. Ako korisnik ne može da dobije pismenu potvrdu da cloud provajder podržava određeni oblik istraživanja može se zaključiti da zahtevi o istraživanju neće biti mogući. Pismena potvrda pružaoca usluge bi trebalo da sadrži podatke kojim on potvrđuje da je već uspešno sprovodio takve aktivnosti.

| CILJ          | OPIS                                                                                                                                                                               |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Poverljivost  | Sigurnost da se informacije ne otkriju ljudima koji nemaju prava pristupa                                                                                                          |
| Integritet    | Sigurnost da je informacija koja se čuva na sistemu prava reprezentacija informacije koja treba da se čuva od strane provajdera i da nije modifikovana od strane neovlašćene osobe |
| Dostupnost    | Sigurnost da resursi za obradu informacije nisu nedostupni zbog uticaja zlonamernih korisnika                                                                                      |
| Nepriznavanje | Sigurnost da se može dokazati da su sklopljeni dogovori između korisnika i provajdera zaista sprovedeni u delo                                                                     |

Tabela 4. Uobičajeni zahtevi sigurnosti<sup>11</sup>

## 9. Cloud Security Alliance (CSA)

Cloud Security Alliance (CSA) je neprofitna organizacija osnovana kako bi promovisala upotrebu najboljih načina na koje se korišćenje cloud computing-a može učiniti što sigurnijim. Takođe, Cloud Security Alliance se bavi edukacijom korisnika o načinima upotrebe cloud computing-a. CSA brinući o sigurnosti podataka u cloud computing-u ujedno pomaže osiguravanju svih drugih oblika računarstva: mobilnog računarstva, grid računarstva, klijent-server računarstva, peer-to-peer računarstva i dr.

Glavni zadaci Cloud Security Alliance su:

- Pomoć u međusobnom razumevanju između korisnika i provajdera koji pružaju cloud computing usluge, vezano za potrebne sigurnosne zahteve i potvrde osiguranja.
- Promocija nezavisnih istraživanja na području cloud computing sigurnosti.

<sup>11</sup> Prikaz tabele najčešćih zahteva sigurnosti u Cloud computing praksi

- Podizanje svesti o cloud computing-u i organizovanje edukativnih programa o prikladnom korišćenju cloud computing-a i mogućim sigurnosnim rešenjima.
- Pravljenje liste problema i smernica za rešavanje istih, utičući na taj način na povećanje bezbednosti u cloud computing-u.

"*Security Guidance for Critical Areas in Cloud Computing*" je vodič koji je CSA razvio za korisnike 2009. godine. Ovaj vodič je brzo postao industrijski vodič za sigurnost ove tehnologije i koriste ga mnoge organizacije širom sveta da bi upravljale svojim cloud computing resursima.

CSA je nakon toga objavio dokument, kao dodatak gore navedenom vodiču, pod nazivom "*Top Threats to Cloud Computing*" kako bi pružio potrebnu pomoć organizacijama pri donošenju odluka o upravljanju rizikom. Sa pojavom novih pretnji i rizika u oblasti sigurnosti i ovaj dokument se stalno nadograđuje. U njemu su se stručnjaci usmerili na jedinstvene ili jako raširene probleme cloud computing-a. U nastavku je opisano sedam osnovnih pretnji cloud computing arhitekturi.

### 9.1. Zloupotreba cloud computing-a

Korisnici cloud computing-a često imaju privid neograničenih mogućnosti upotrebe. Možda najveći takav privid imaju korisnici IaaS (Infrastructure as a Service, IaaS) modela. Navedeni model korisnicima daje neograničene mogućnosti upotrebe mrežnih resursa i čuvanja podataka.

Neki provajderi nude u određenom probnom periodu, besplatno, ali ograničeno, korišćenje cloud computing usluga. Zlonamerni korisnici relativno jednostavno i nekažnjeno iskorišćavaju sigurnosne propuste i na taj način razvijaju tehnologije koje će im omogućiti lakši pristup i iskorišćavanje podataka drugih korisnika, a pri tome neće ugroziti vlastiti identitet. Ove činjenice ukazuju na smanjenje nivoa sigurnosti korišćenja cloud computing-a.

Provajderi koji nude cloud computing usluge su neprekidna meta zlonamernih korisnika. Razlog tome je sa jedne strane slaba autentifikacija sistema, a sa druge nedovoljan nivo svesti o sigurnosnim rizicima krajnjih korisnika sistema.

PaaS (Platform as a Service) model se do sada pokazao kao najpodložniji napadima. Međutim poslednjih godina beleži se sve veći napad i na IaaS model pružanja usluga. U budućnosti će provajderi koji nude cloud computing usluge morati više pažnje da posvete sprečavanju probijanja lozinki i ključeva, DDoS napadima (Distributed Denial of Service), pokušaju izvođenja dinamičkih napada i sličnim napadačkim tehnikama.

Koje sisteme zaštite treba primeniti kako bi se, korisnik ili provajder, zaštitili od napada :

- Uvođenje složenije početne registracije i provera process registracije.

- Poboljšanje i usavršavanje u praćenju i koordinaciji prevara koje se izvode putem kreditnih kartica.
- Uvođenje sveobuhvatnog proveravanja mrežnog prometa korisnika.
- Uvođenje nadzora javnih crnih lista na kojima su navedeni zlonamerni korisnici odnosno adrese s kojih se oni prijavljuju kako bi se zaštitili vlastiti sistemi.

## 9.2. Nesigurni interfejs i API

Provajderi koji pružaju cloud computing usluge otkrivaju deo programskog interfejsa ili API-a (Application Programming Interface) koje korisnici koriste za upravljanje cloud uslugama. Korišćenjem tih interfejsa korisnici mogu vršiti raspodelu, upravljanje, nadzor i sinhronizaciju. Dostupnost i sigurnost API-a je u direktnoj sprezi sa sigurnošću i dostupnošću osnovnih cloud computing usluga. Ovi interfejsi moraju osigurati zaštitu korisnika od zlonamernih napada. Mnoge organizacije na postojeće interfejse nadograđuju dodatne usluge i tako dobijaju još složenije interfejse. Samim tim još više otežavaju sprečavanje raznih zlonamernih napada i zbog svoje složenosti su više izloženi riziku. Većina provajdera teži osiguravanju sopstvenih modela, ali korisnici pri upotrebi moraju da razumeju sigurnosne probleme vezane za upotrebu, upravljanje, sinhronizaciju i praćenje cloud usluga. Ako se organizacija prepusti korišćenju slabe grupe interfejsa, ona se izlaže velikim rizicima koji se odnose na sigurnost, integritet, dostupnost i odgovornost.

Za izvršavanje zlonamernih napada na korisnike, koristi se činjenica da se korisnici često susreću s anonimnim pristupom i/ili potrebom za ponovnom upotrebom lozinki, prijavom bez upisivanja teksta ili prenosa sadržaja, nefleksibilnom proverom pristupa ili neispravnom autentifikacijom, ograničenim praćenjem i beleženjem sposobnosti, nepoznatim uslugama ili zavisnosti interfejsa.

Pretnja se pojavljuje na svim modelima pružanja usluge - IaaS, SaaS i PaaS. Kako bi se korisnici i provajderi usluga zaštitili od napada potrebno je:

- Analizirati sigurnosne modele sistema provajdera cloud computing usluga.
- Prenositi šifrovani signal i osigurati odgovarajuću autentifikaciju i proveru pristupa.
- Razumeti da se preko interfejsa korisnik povezuje na druge sisteme koji mogu biti sigurnosno ugroženi, pa se tako mogu neplanirano i neoprezno i sami izložiti riziku.

## 9.3. Zlonamerni korisnici koji napade izvode "iznutra"

Provajderi cloud computing usluga ne otkrivaju način na koji svojim korisnicima daju pristup fizičkim i virtualnim sredstvima, kao ni način na koji prate korisnike, analiziraju i izveštavaju o saradnji. Ova situacija otvara mnoge mogućnosti zloupotrebe, koje zlonamerni korisnici rado koriste. Nivo odobrenog pristupa oblaku omogućava iskorišćavanje poverljivih podataka ili dobijanje potpunog nadzora nad uslugom s jako malom mogućnošću otkrivanja identiteta napadača. Uticaj koji

zlonamerni korisnici “iznutra” mogu imati na organizaciju definitivno se ne smeju zanemariti. Poseban rizik predstavlja nivo njihovog pristupa i mogućnost prodiranja u organizacije. Neki od načina na koji zlonamerni korisnici mogu uticati na organizaciju su povreda ugleda, finansijski uticaj i gubitak produktivnosti. Kada organizacija prihvati cloud okruženje ljudski uticaj postaje još veći. Od velikog je značaja upoznati korisnike cloud computing-a s postupcima koje reduzima provajder da bi sprečio napade iznutra.

Organizacije su uglavnom jako dobro upoznate s opasnostima koje im mogu doneti dobro upućeni zlonamerni korisnici. Ova pretnja ne predstavlja problem samo organizaciji već i korisnicima cloud usluga. Jedna od glavnih slabih karika jeste nedostatak transparentnosti procesa i procedura provajdera cloud computing usluga.

Da bi se korisnici i provajderi usluga zaštitili od napada treba:

- Sprovoditi strogi nadzor nad lancem nabavke i sprovoditi celokupne procene isporučioca.
- Odrediti zahteve za ljudskim resursima kao deo pravnog ugovora.
- Zahtevati transparentnost u pogledu sigurnosti informacija, praksi upravljanja, kao i usklađenost u izveštavanju.
- Odrediti proces obaveštavanja o sigurnosnim problemima.

#### 9.4. Zajednički tehnološki problemi

IaaS model pružanja usluge se temelji na deljenju infrastrukture. Često komponente koje čine infrastrukturu nude jaka izolaciona svojstva za arhitekturu podeljenu na više korisnika. Da bi se rešio ovaj nedostatak potreban je veći nadzor međusobnog posredovanja operativnih sistema korisnika i fizičkih računarskih resursa. Uprkos povećanom nadzoru zlonamerni korisnici ipak pronađu način dobijanja neodgovarajućeg nivoa nadzora ili uticaja na platformu. Kako bi se odbranili od ovakvih upada neophodno je obezbediti povećano praćenje korisničkih aktivnosti, akcije čitanja/čuvanja podataka i nadzor aktivnosti na mreži.

U poslednjih nekoliko godina, zlonamerni korisnici su uspeli da zloupotrebe zajedničku imovinu korisnika koja se nalazi u oblaku.

Da bi se korisnici i pružaoci usluga zaštitili od napada potrebno je:

- Implementirati najbolje sigurnosne postupke za instalaciju/konfiguraciju.
- Proučavati okruženje da bi se uočile neovlašćene promene/aktivnosti.
- Insistirati na jakim autentifikacionim mehanizmima i nadzoru pristupa za administrativne radnje.
- Insistirati na ugovorima koji sadrže klauzulu o nivou usluge kako bi se smanjio uticaj ranjivosti.

#### 9.5. Gubitak i neovlašćeno otkrivanje podataka

Postoje razni načini na koje zlonamerni korisnici mogu da ugroze važne podatke organizacije. Primer toga je brisanje ili promena podataka bez kopije originalnog

sadržaja. Raskidanje veze između dela podataka sačuvanih na nekom drugom delu servera i celokupnog izvornog podatka može podatak učiniti nepovratnim (isto kao što to može učiniti čuvanje podataka na nepouzdanom mediju za čuvanje). Gubitak ključa za kodiranje može dovesti do uništavanja bitnih podataka. Neovlašćenim stranama mora biti zabranjen pristup osetljivim podacima. Pretnja ugrožavanja podataka proizilazi iz mnoštva različitih međudelovanja između rizika i izazova koji su jedinstveni za oblak ali i zbog arhitekturnih i operacionih odlika oblaka, što je još opasnije.

Gubitak ili neovlašćeno otkrivanje podataka mogu imati poguban uticaj na poslovanje. Oni ugrožavaju ugled i reputaciju organizacije, mogu dovesti do prekida poslovne saradnje s organizacijama koje koriste oblak, poslovnim partnerima ili gubitka poverenja korisnika. Gubitak ključnog intelektualnog vlasništva može imati konkurentske i finansijske uticaje, jer će mnoge druge organizacije ili zlonamerni korisnici pokušati da dođu do tih podataka i iskoriste ih za ostvarenje sopstvenih ciljeva. Zavisno od toga koji su podaci izgubljeni ili su delimično procureli na tržište, može doći do kršenja ljudskih prava (npr. objavljivanja inkriminišućih podataka o nekom pojedincu, iskorišćavanje ukradenih informacija u želji da se smanji finansijska moć ili ugled pojedinca) i pravnih posledica (npr. pokretanje sudskih postupaka protiv pojedinaca ili organizacija zbog sadržaja pronađenih podataka). Do iskorišćavanja podataka organizacija ili pojedinačnih korisnika može da dođe zbog neodgovarajuće autentifikacije, autorizacije i provere kontrole, zatim nepravilnog korišćenja šifri i programskih ključeva, operacijskih neuspeha i dr.

Pretnja se pojavljuje na svim modelima pružanja usluge. Da bi se korisnici i pružaoci usluga zaštitili od napada potrebno je:

- Implementirati interfejs s dobrom kontrolom pristupa.
- Kriptovati podatke i zaštititi njihov integritet.
- Analizirati zaštitu podataka.
- Nakon što korisnici odluče da prestanu da koriste cloud computing usluge provajdera, provajder usluga bi trebalo trajno da ukloni podatke korisnika sa servera. Korisnici bi trebalo da sklope ugovor s provajderom usluga koji sadrži detalje oko postojanja sigurnosnih mera i strategije pridržavanja.

## 9.6. Krađa korisničkih imena

Krađom korisničkog imena napadači mogu da iskorišćavaju usluge koje korisnici plaćaju. Zlonamerni korisnici napadima poput krađe identiteta, prevara i iskorišćavanja programskih ranjivosti još uvek postižu uspehe u narušavanju sigurnosti korisnika. Korisnici često koriste iste akreditive i lozinke, što povećava broj ovakvih napada. Korišćenjem cloud computing-a pojavljuju se nove pretnje. Ako napadač dobije pristup nalogu, on može da posmatra aktivnosti i transakcije, upravlja podacima i na taj način da usmerava korisnike na zlonamerne stranice. Korisnički računi ili usluge postaju napadačima nova meta s kojom mogu iskorišćavati korisnikov identitet za izvođenje daljih napada.

Krađa korisničkih imena, obično u obliku krađe akreditiva (credentials), korisnicima predstavlja jednu od najvećih pretnji. S ukradenim akreditivima zlonamerni napadači

mogu da pristupe kritičnim podacima cloud computing usluga, i tako da ugroze poverljivost, integritet i dostupnost tih usluga. Organizacije bi trebalo da budu svesne ovih tehnika kao i uobičajenih načina zaštite od istih.

Pretnja se pojavljuje na svim modelima pružanja usluge cloud computing-a.

Da bi se korisnici i pružaoci usluga zaštitili od napada potrebno je:

- Zabraniti deljenje pristupnih akreditiva između korisnika i servera.
- Gde god je moguće koristiti snažne dvofaktorske tehnike autentifikacije.
- Izvoditi proaktivno praćenje za otkrivanje neovlašćenih aktivnosti.
- Razumeti sigurnosne politike i SLA (eng. Service Level Agreement) provajdera cloud computing usluga.

## 9.7. Nepoznati profil rizika

Jedna od karakteristika cloud computing-a je smanjivanje vlasništva nad mehanizmima i programima, pa samim tim i omogućavanje organizacijama da se usmere na njihove osnovne poslovne strategije. To dovodi do finansijskih i operativnih prednosti koje se moraju pažljivo odmeriti sa kontradiktornim sigurnosnim problemima. Verzije programa, dopune koda, sigurnosne prakse, profil ranjivosti kao i pokušaji neovlašćenih pristupa su jako važni faktori za procenu rizika organizacije. Za procenu rizika organizacijama su jako važne i informacije o tome ko sve deli zajedničku infrastrukturu. Sigurnost skrivanjem podataka (eng. security by obscurity) može se jednostavno postići, ali može isto tako da rezultira nepoznatom izloženošću. Ona takođe može da utiče i na dubinske analize koje zahtevaju visok stepen nadzora ili regulisanja operativnih područja.

Da bi se korisnici i pružaoci usluga zaštitili od napada trebalo bi se usmeriti na:

- Razotkrivanje primenjivih zapisa i podataka.
- Delimično i/ili potpuno otkrivanje detalja infrastrukture.
- Praćenje i upozoravanje na potrebne informacije kojima korisnici mogu smanjiti izloženost riziku.

## Zaključak

Pojava virtualizacije u informatici postavlja kako fizičku tako i logičku šemu poslovnih sistema na određeni stepen abstrakcije. Devedesetih godina prošloga veka krenula je nagla ekspanzija virtualizacionih tehnologija, da bismo danas virtualizaciju posmatrali kao ključnu tehnologiju u održavanju jednog savremenog datacentra.

Virtualizacija ima višestruke i raznolike primene u uređivanju poslovnih procesa kao i u rešavanju problema organizacije obzirom na različite oblike njenog postojanja kao i na različita rešenja virtualizacionih arhitektura. Ono što već sada virtualizaciju čini primamljivom je činjenica da je dostupna kako za mala-srednja tako i velika preduzeća.

Investicije u virtualizaciju bivaju isplative veoma brzo. Virtualizacija donosi veliki broj revolucionarnih rešenja u različitim aspektima: smanjenje potrošnje električne energije, konsolidacija servera, manja opterećenost fizičkog prostora, bolja povezanost računara u mreži, lakše rešavanje problema povezanih sa fenomenom disaster-recovery, lakši rad sa nekompatibilnim operativnim sistemima i lakša integracija različitih poslovnih aplikacija u kompanijama, velike prednosti u sigurnosti testiranja sistema pre implementacije istih u kompanijama itd.

Na tržištu postoje različita softverska rešenja za primenu virtualizacije koja sa sobom nose kako prednosti tako i mane. U zavisnosti od performansi koje kompanija želi da postigne zavisiće softversko rešenje za koje će se opredeliti.

Cloud computing model predstavlja poslednji korak u razvoju virtualizacije. Ovaj model omogućava jednostavan mrežni pristup, na zahtev korisnika, udeljenom skupu resursa (npr. mrežni resursi, serveri, prostor na hard diskovima, aplikacije i servisi) koji mogu biti brzo omogućeni za upotrebu ili ugašeni, a sa minimalnim intervencijama ili akcijama od strane pružaoca usluga (provajdera). Izmeštanje podataka i infrastrukture kod specijalizovanih provajdera pruža bolju dostupnost ovih resursa zaposlenima u kompaniji bez obzira na to gde se oni u određenom trenutku nalaze.

Ovaj oblik računarstva još uvek nije na svom vrhuncu, iako na tržištu postoji nekolicina provajdera koja nudi pružanje cloud computing usluga.

Danas korisnici sve više aktivnosti obavljaju preko web pretraživača, bilo da je to pregledanje elektronske pošte, gledanje video zapisa, slušanje muzičkih sadržaja, pisanje dokumenata i sl. Pri tome se izbegavaju lokalne instalacije programa, dok se sadržaj često prikazuje samo u toku rada i ne ostaje trajno zapisan. Kako je pristup svemu preko Interneta sve zastupljeniji, ideja oblaka na koje poslovni korisnici stavljaju svoje aplikacije sve je privlačnija. Umesto kupovine sopstvene opreme, Cloud computing omogućava pružanje raznih usluga uz relativno nisku cenu, a u današnjem svetu je raznim kompanijama sve važnije da deo svog poslovanja obavljaju na Internetu. Moguće je da će u budućnosti korisnici većinom da pređu na operativne sisteme koji uopšte ne instaliraju aplikacije lokalno nego svemu pristupaju preko Interneta. Jedan od primera ovakvih operativnih sistema je Google Chrome.

Takva budućnost zahteva tehnologije i modele poslovanja vezane za oblak, pa će samim tim cloud computing kao model postati neozabilazan većini kompanija.

Cloud computing će dosegnuti svoj potpuni razvojni potencijal tek kada se uklone dosadašnji problemi poput problema sigurnosti, dostupnosti, teškog prebacivanja podataka, zavisnosti o jednom provajderu i dr. Tek po nestanku tih problema značajno će se povećati broj korisnika. Cloud computing ima svetlu budućnost zato što teži povećavanju kapaciteta ili novih mogućnosti bez investiranja u nove infrastrukture, obuku novog osoblja ili kupovanje novih licenciranih programa. Sve su to velike prednosti Cloud computing-a u odnosu na dosadašnje načine čuvanja podataka, koje će organizacijama doneti velike finansijske uštede, a samim time i pružiti mogućnost bržeg i većeg razvoja, investiranja u nova istraživanja i nove projekte, pa tako i dalji razvoj IT sektora.

Tehnički obučeni korisnici, sve češća upotreba mobilnih uređaja kao što su mobilni telefoni ili laptop računari, pojava namenskih hardverskih uređaja, a pre svega virtualizacija i razvoj Cloud computing-a doveo je toga da je postalo neophdno da se preispita opravdanost sadašnje organizacije računarskih mreža, naročito manjih kompanija.

Neophodnosti izmeštanja podataka ili mrežne infrastrukture kod specijalizovanih provajdera uslovljena je sve povoljnijom ponudom namenskih servera kao i ekspanzijom virtualizacije koja predstavlja osnov za Cloud computing. Izmeštanje podataka i infrastrukture sa sobom nosi određene bezbednosne rizike, što je uslovalo razvoj različitih tehnika zaštite.

Najzastupljniji sigurnosni protokoli koji se koriste za bezbednu komunikaciju su IPsec protokol i SSL protokol. SSL protokol se sve više upotrebljava, pre svega zbog svoje fleksibilnosti koja se najviše ogleda u jednostavnosti korišćenja kroz Web pretraživač koji se sve više primenjuje ne samo za pretraživanje već i za pokretanje Web aplikacija kao i drugih Web servisa. Takođe, osnivaju se neprofitne organizacije koje za cilj imaju da promovišu upotrebu najboljih načina na koje se korišćenje cloud computing-a može učiniti što sigurnijim. Cloud Security Alliance (CSA) je jedno od takvih neprofitnih organizacija.

Virtuelizacija i Cloud computing su sadašnjost i budućnost savremenih informacionih tehnologija. Njihova primena će u budućnosti težiti da postane standard u svetu, a njihova primena će biti svestrana, kako u aktivnostima organizacija tako i u aktivnostima fizičkih lica.

## Literatura

1. „VMWare Virtualization Basics“, VMWare, 2009.,  
<http://www.vmware.com/virtualization>
2. „Virtualization“, Wikipedia, The free encyclopedia, 2010.
3. Strategies for Successfully Implementing a Virtualization Project: A Case with VMware, University of Southern Mississippi, USA, 2008.
4. Prof. dr Mladen Veinović, prof. Aleksandar Jevremović, Uvod u računarske mreže, Univerzitet Singidunum, Beograd, 2009.
5. Kenneth Hess, Amy Newman, Practical Virtualization Solutions: Virtualization from the Trenches, Prentice Hall, USA, 2009.
6. Dušan Abadžin, Virtualizacija i njene glavne prednosti, IT rešenja (online magazin), Beograd, 2010. <http://www.itresenja.com/resenja/virtualizacija-i-njene-glavne-prednost/1245358>
7. Rand Morimoto, Jeff Guillet, Windows Server 2008 Hyper-V Unleashed, Sams Publishing, USA, 2008.
8. Michael Slisinger, Virtualization Changes Everything: Storage Strategies for VMware vSphere & Cloud Computing, USA, 2012.
9. Dan Kusnetzky, Virtualization: A Manager's Guide, O'Reilly Media, USA, 2011.
10. „Cloud computing“, Wikipedia, The free encyclopedia, 2014.
11. Thomas Erl, Zaihgam Mahmood, Ricardo Puttini, Cloud Computing: Concepts, Technology & Architecture, Prentice Hall, 2013.
12. [Dan C. Marinescu](#), [Cloud Computing: Theory and Practice](#), Morgan Kaufman, USA, 2013.
13. [Barrie Sosinsky](#), [Cloud Computing Bible](#), Wiley Publishing, Inc., Indiana, 2011.
14. [Vic \(J.R.\) Winkler](#), Securing the Cloud: Cloud Computer Security Techniques and Tactics, Elsevier Inc., USA, 2011.
15. [Arshdeep Bahga](#), [Vijay Madisetti](#), [Cloud Computing: A Hands-On Approach](#), [Arshdeep Bahga](#) & [Vijay Madisetti](#), 2014.
16. Fred van der Molen, Get Ready for Cloud Computing: A Comprehensive, Van Haren Publishing, Rotterdam, 2010.