Факултет инжењерских наука Универзитета у Крагујевцу

Назив студијског програма: Машинско инжењерство
Ниво студија: Мастер академске студије
Модул: Информатика у инжењерству
Предмет: Пројектовање информационих система и база података
Број индекса: 378/2018

Никола З. Николић

Архитектура и безбедност cloud пословног софтвера

Мастер рад

Комисија за преглед и одбрану:

1. **Проф. др Милан Ерић - ментор**
2. _____
3. _____

Датум одбране:_____

Оцена:_____

Универзитет у Крагујевцу
Факултет инжењерских наука

Мастер студије: **Машинско инжењерство**

Студијско подручје (усмерење): **Информатика у инжењерству**

Име и презиме: **Никола Николић**

Број индекса: 378/2018

ПРИЈАВА МАСТЕР РАДА

Тема рада: ***Архитектура и безбедност cloud пословног софтвера***

Задатак: У оквиру мастер рада обухватити: Основе и карактеристике cloud рачунарства; Пословни софтвер као услуга и примена cloud рачунарсва у пословне сврхе; Архитектуру – cloud рачунарства; Примену технологија за пословни софтвер; Безбедност апликација у облаку; Безбедност базе података у облаку; Стандарде безбедности – примена. На крају рада дати закључна разматрања.

Ментор:

Крагујевац, 12.03.2020.

Проф. др Милан Д. Ерић

Изјава о самосталној изради рада

Изјављујем да сам овај мастер рад урадио самостално, служећи се стеченим знањем и искуством као и наведеном литературом.

Никола Николић 378/2018

_____

(потпис)

Садржај

1. Увод 1
2 Основе и карактеристике cloud рачунарства 2
2.1 Историја рачунарства у облаку 2
2.2 Дефиниција cloud рачунарства 2
2.3 Модели услуга (Cloud Service Model) 2
2.3.1 SaaS (Service as a Serve) 3
2.3.2 IaaS (Infrastructure as a service) 4
2.3.3 PaaS (Platform as a service) 4
2.3.4 Data-Storage-as-a-Service (dSaaS) 5
2.4 Модели примене у облаку (Cloud Deployment Model) 5
2.4.1 Јавни облак (Public cloud) 6
2.4.2 Приватни облак (Public cloud) 7
2.4.3 Хибридни облак (Hybrid Cloud) 7
2.4.4 Облак заједнице (Community Cloud) 8
2.5 Разлика између cloud рачунарства и cloud услуга 9
2.6 Карактеристике рачунарства у облаку 10
3. Архитектура cloud рачунарства 12
3.1 Дефиниција архитектуре рачунарства у облаку 12
3.2 Пословне предности архитектуре у облаку 12
3.3 Слојеви архитектуре облака 13
3.4 Екосистем cloud архитектуре 16
4. Пословни софтвер као услуга и примена cloud рачунарства у пословне сврхе 17
4.1 Лак приступ компанијама - cloud технологија 17
4.2 Рачунарство у облаку и бизнис 17
4.3 Cloud рачунарство и примена канцеларијских пакета 18
4.3.1 Google Apps for Work пакет 18
4.3.2 Microsoft Office 365 пакет 19
4.3.3 Zoho Office Suite пакет 19
4.4 Услуге складиштења у облаку 19
4.4.1 Dropbox 20
4.4.2 Box 20
4.4.3 Google Drive 20
4.4.4 OneDrive 20
4.5 Пословни информациони системи у облаку 21
4.5.1 Customer Relationship Management (CRM) 21

4.5.2 Enterprise Resource Planning (ERP) 22
5. Примена технологије за пословни софтвер у облаку 23
5.1 Методологија примене модела рачунарства у облаку 25
5.1.1 Стратегијска фаза 26
5.1.2 Фаза планирања 27
5.1.3 Фаза примене 28
5.2 Cloud рачунарство у развоју и тестирању 28
5.3 Виртуелизација 30
5.3.1 Виртуелизација предности и мане 31
5.4 Кластери високих перформанси засновани на облаку 31
6 Безбедност апликација у облаку 34
6.1 SOA безбедност и сигурносни стандарди 34
6.2 Веб услуге и сигурност 36
6.3 WS-Security и сродни стандарди 37
7. Безбедност Базе података у облаку 40
7.1 Безбедносни компромис између сервисних модела 40
7.2 Услуге базе података у облаку 41
7.3 Предности услуга базе података у облаку 43
7.4 Задатак Безбедности 44
7.4.1 Доступност 44
7.4.2 Проблеми са контролом приступа у јавном облаку 45
7.4.3 Питања ревизије и праћења 45
7.4.4 Санитизација података 45
7.5 Надгледање дистрибуиране базе података 46
7.6 Разматрање шифровања 48
8. Стандардне безбедности и примена 50
8.1 Безбедност и криптографија 50
8.2 AES (Advanced Encryption Standard) 51
8.3 DES (Data Encryption Standard) 54
8.4 Примена AES алгоритма за енкрипцију података 58
8.5 Подручје примене 58
8.6 Програм за Енкрипцију и Декрипцију 59
9 Закључак 61
10 Литература 63

Резиме

У раду је приказана архитектура пословног софтвера у облаку. Технологија, предности и мане рачунарства у облаку су присутне о раду као и конкретне предности преласка са класичног пословања на пословање на даљину. Најзначајније карактеристике cloud рачунарства су такође описане. Коришћење пословног софтвера као услуге, и примена cloud рачунарства у пословне сврхе. Посебна пажња се даје Безбедности апликације у облаку као и безбедност базе података у облаку. Дефинисане су и објашњене стандардне безбедности које се примењују за заштиту података.

Кључне речи: Cloud рачунарство, безбедност, пословни софтвер, архитектура

Summary

The paper presents the architecture of business software in the cloud. Technology, advantages and disadvantages of cloud computing are present in the work as well as the concrete advantages of the transition from traditional to cloud business. The most significant features of cloud computing are also described. Use of business software as a service, and application of cloud computing for business purposes. Special attention is paid to the security of the cloud application as well as the security of the cloud database. The security standards applied for data protection have been defined and explained.

Keywords: Cloud computing, security, business software, architecture

1. Увод

Модеран начин живота и пословања је укључио технологију у виду паметних телефона, таблета, лаптопова и осталих преносивих уређаја као средства за брз приступ подацима и обављању сложених задатака чији се софтвер налази изван конкретног уређаја. Овакав начин приступа информацијама и апликацији је омогућио приступ подацима брзо и свуда [1].

Први део рада бави се архитектуром cloud рачунарства са посебним освртом на примену ове технологије у пословне сврхе. Да би се реализовао брзи начин размене информација и приступ бази података мора се обезбедити адекватна безбедност која ће пратити ову технологију. Описане су стандардне безбедности рачунарства у облаку као и базе података у облаку.

Рачунарство у облаку је парадигма која се развија. Дефиниција NIST (National Institute of Standard and Tehnology) карактерише важне аспекте рачунарства у облаку и намењена му је да служи као средство за широко упоређивање услуга у облаку и стратегија примене, као и да пружи основу за расправу од тога шта је рачунарство у облаку до тога како најбоље користити рачунарство у облаку [3].

Рачунарство у облаку је модел који омогућава свеприсутан, погодан мрежни приступ на захтев дељеном скупу конфигурабилних рачунарских ресурса (нпр. мреже, сервери, складиште, апликације и услуге) који се могу брзо обезбедити и објавити уз минималан напор управљања или интеракција добављача услуга [3].

У раду се налазе карактеристике које описују рачунарство у облаку као и технологије и апликације као подршка. Дата је разлика између рачунарства у облаку и пружању услуга у облаку. Очигледна је све већа присутност cloud рачунарства, самим тим су се појавили и проблеми који су неизоставни, а који се односе првенствено на безбедност па и на архитектуру самих софтвера. Циљ оваквог начина пословања јесте да се корисник ослободи свих питања која се односе на саму компатибилност хардвера и софтвера. Практично то значи да код cloud апликација није потребна физичка присутност софтвера на конкретном уређају са којим се приступа апликацији, већ је довољно само регистровање и већ су доступне могућности које сам софтвер пружа.

Рачунарство у облаку је постало значајан тренд технологије и многи стручњаци очекују да ће cloud технологија преобликовати процесе информационе технологије (IT) и тржиште IT-а [1].

Због уштеде времена и простора, као и једноставности ове гране рачунарства, cloud апликације су нашле широку примену како малих тако и великих предузећа чији рад би данас био незамислив без оваквог вида технологије. Циљ је размотрити и идентификовати приступ рачунарству у облаку, а са тим размотрити и питања која се тичу безбедности и проблема у структури рачунарства у облаку и примени у пословне сврхе.

Рачунарство у облаку истовремено нуди бројне могућности и изазове. За изазов се сматра да је безбедност критична препрека рачунару у облаку на путу ка још већем успеху, а алокација података је пресудан фактор када је у питању сигурност рачунарства у облаку [4].

2 Основе и карактеристике cloud рачунарства

Како си се разматрала ова релативно нова грана IT света најпре се даје кратак осврт на сам настанак и услове који су довели до потребе за овим видом преноса и чувања податак. У овом одељку приказане су неке од многобројних дефиниција које се могу наћи у литератури. Дата је разлика између cloud услуга и рачунарства у облаку као и основни модели рачунарства у облаку.

2.1 Историја рачунарства у облаку

Први који је увео концепт рачунарства у облаку је Џон Мкарти (John McCarthy). Шездесетих година двадесетог века он је рекао да ће рачунарство једног дана бити организовано на тај начин да ће функционисати као једна служба. Даглас Паркхил (Douglas Parkhill) 1966. године у својој књизи „The Challenge of the Computer Utility“ први пут истражује карактеристике рачунарства у облаку.

Појам „Облак“ потиче из света телекомуникација. Настао када су теле-комуникационе компаније почеле да нуде услуге виртуелне приватне мреже или скраћено VPN (Virtual private network). Овакав вид технологије је био итекако конкурентан на тржишту у то време јер је пружао услуге по знатно нижим трошковима [5].

Пре проналаска VPN-а, обезбедили су наменске кругове података од тачке до тачке који нису ништа друго до расипање пропусног опсега. Коришћењем VPN услуга могли су да пребаце саобраћај у равнотежу употребом целокупне мреже. Cloud рачунарство сада то проширује тако да покрива сервере и мрежну инфраструктуру. Многи предузетници у индустрији прешли су у рачунарство у облаку и применили га за своје потребе. Amazon је имао важну улогу у развоју облака, покренуо је Amazon Web Service (AWS) 2006 године. Бројне предности оваквог начина пружања услуга увидели су и тимови из Google-а и IBM-а. Google и IBM су такође започели истраживачке пројекте у рачунарству у облаку. Прва платформа отвореног кода је Eucalyptus развијена од стране компаније Eucalyptus Systems и служила за постављање приватних облака [5].

2.2 Дефиниција cloud рачунарства

Да би се разумела ова релативно нова технологија у IT свету потребно је дефинисати је и дати основне информације. Свакодневни смо корисници cloud computing-а, али постоје често нејасноће око дефинисања овог појма. Област примене обухвата неколико грана па се дефиниције могу разликовати.

Рачунарство у облаку се може дефинисати као нови стил рачунарства у коме се динамички скалабилни и често виртуелизовани ресурси пружају као услуга [1].

Cloud начин реализације сложених процеса и операција је постао значајан технолошки тренд и многи стручњаци очекују да ће управо овакав концепт променити процесе IT-а. Помоћу ове технологије кориснику је доступан приступ апликацијама, складиштима и платформама, као и приступ услугама које нуде власници неких пословних софтвера у облаку. На тај начин се ствара уштеда пре свега у трошковима, а затим уштеда у времену због лаке доступности и флексибилности [1].

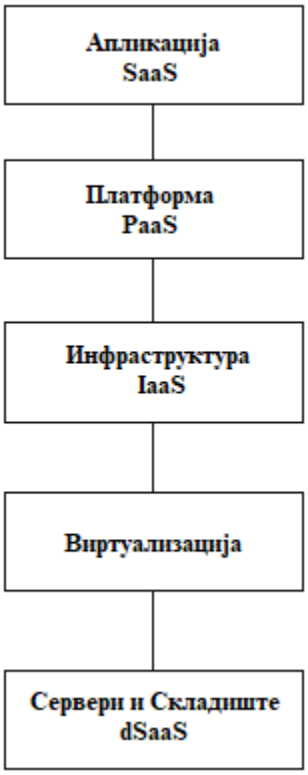
2.3 Модели услуга (Cloud Service Model)

Рачунарство у облаку можемо посматрати као свеукупност IT услуга које се нуде кориснику преко мреже на изнајмљеној основи и са могућношћу да повећају или смање њихове захтеве за услугама. Највећи број рачунарских услуга пружа независни провајдер

који је власник инфраструктуре. Разликујемо два основна модела облака у рачунарству и то су [5].:

- Cloud Service Model
- Cloud Deployment Model

Скуп услуга које нуди облак се могу представити као слојевита архитектура cloud рачунарства. На слици 1 је приказана слојевита архитектура рачунарства у облаку.



Слика 1 Слојевита архитектура cloud computing-a [1]

Слојеви који пружају услуге у облаку укључују инфраструктуру као основни слој, платформу као интерфејс између апликација и хардвера и на крају софтвер, слој који представља предњи крај са којим корисници комуницирају [6].

2.3.1 SaaS (Service as a Serve)

Услуге које се нуде путем рачунарства у облаку обично укључују IT услуге назване SaaS (Software as a Service). Софтвер као услуга налази се на самом врху слојевито приказане архитектуре cloud рачунарства (слика 1). Важна карактеристика технологије која је све заступљенија јесте да софтвер није физички присутан на уређају. То омогућава корисницима да покрећу апликације без присуства софтвера у складишту уређаја, већ се приступа покретању апликације из облака [1].

SaaS је лако доступан корисницима и купцима путем интернета. Кроз овај модел пружања услуга крајњи корисници користе услуге софтверске апликације преко мрежа према захтеву. На пример, gmail је SaaS где је google добављач, а ми потрошач [5].

Карактеристике SaaS модела [5] :

- Интернет приступ комерцијалном софтверу.
- Софтвером се управља из централне локација.

- Испорука софтвера према моделу „један према више“
- Нема потребе за честом ндоградњом софтвера. Интерфејс за програмирање апликација (API) омогућава интеграцију различитих делова софтвер

2.3.2 IaaS (Infrastructure as a service)

Поред софтвера као услуге, као услуга се пружа и инфраструктура као рачунарски ресурс, познат као IaaS (Infrastructure as a service). IaaS укључује виртуелизоване рачунаре са загарантованом процесорском снагом, резервисаним пропусним опсегом за складиштење и приступ интернету [1].

Пружа испоруку рачунарских ресурса у облику хардвера, мреже, складишта, оперативног система и уређаја за складиштење као услуга на захтев. Заправо IaaS је комбинација јавне и приватне инфраструктуре, али се може користити и као индивидуална инфраструктура.

Карактеристике IaaS модела [5] :

- Испоручује ресурсе као услугу
- Динамичко скалирање је дозвољено у IaaS-у
- Цена се креће у зависности од захтева корисника
- Више корисника или купаца може приступити на истом хардверу
- Нема потребе за администрацијом

2.3.3 PaaS (Platform as a service)

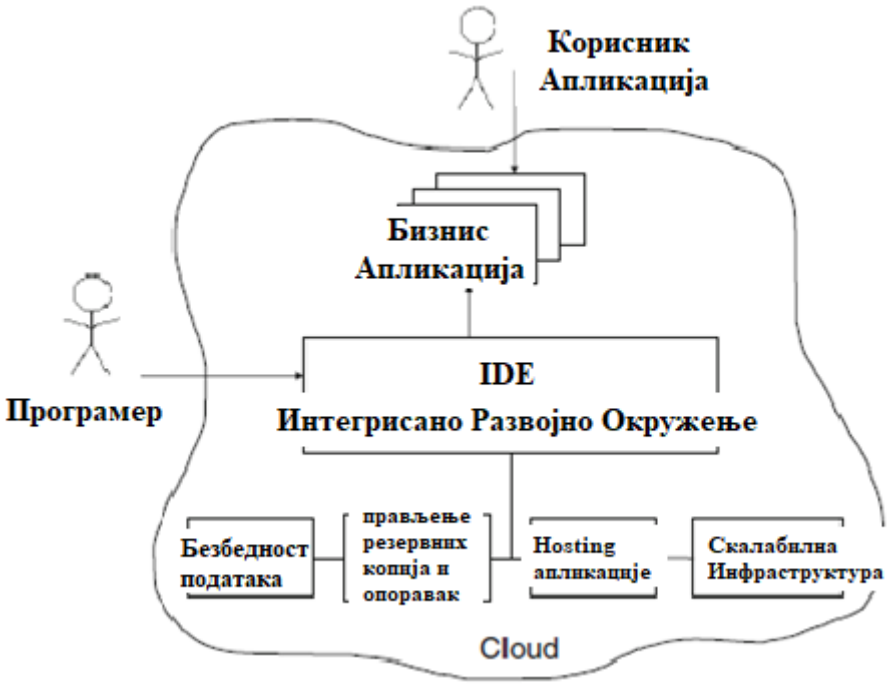
PaaS (Platform as a service) је веома сличан IaaS-у, али за разлику од инфраструктуре као услуге укључује и оперативне системе. Извршава потребне услуге за одређену апликацију. Простије речено PaaS је IaaS са прилагођеним софтверским пакетом за дату апликацију [1].

У PaaS-у се сама платформа даје потрошачима на коришћење. Потрошачи раде на развијању сопственог софтвера. Програмери раде на коду и развијају апликације преко облака. Приступ је организован према софтверу и развојним алатима. На пример: Апликациони сервер (Java, NET Framework) и сервер базе података (MySql, Oracle), који клијент може користити за израду сопствених апликација како би се удовољило специфичним потребама организације за чије се потребе развија апликација.

Карактеристике PaaS модела [5] :

- Смањује трошкове развоја и одржавања. Када се софтвер развија примењује се и тестира било која апликација у истом интегрисаном окружењу.
- Могућност обезбеђења и управљања базом података.
- Нема потребе за преузимањем или инсталирањем апликација да би корисник приступио истој и користио за своје потребе.
- Пружа поузданост, скалабилност, и сигурност која је уграђена.
- Истовремено више корисник може приступити апликацији због заједничке архитектуре и лаког приступа платформи.

На слици 2 је дат пример рачунарства у облаку PaaS. PaaS пружа интегрисано развојно окружење (IDE) укључујући сигурност података, прављење резервних копија, опоравак, hosting апликацију и скалабилну архитектуру [1].



Слика 2 Концепт платформе као услуге (PaaS) [1]

Приступ интегрисаном развојном окружењу имају програмери који развијају софтвер уз помоћ технологије интегрисане у облаку. Корисник може сам прилагодити свој бизнис захваљујући прилагодљивости PaaS-а.

2.3.4 Data-Storage-as-a-Service (dSaaS)

Data-Storage-as-a-Service (dSaaS) пружа складиште у облаку које користи потрошач на захтев. Корисник услуга има могућност избора опсега пропусности за складиштење. На слици 1 налази се dSaaS као крајња инстанца тока података тј. само складиште у облаку [1].

2.4 Модели примене у облаку (Cloud Deployment Model)

Један од важнијих задатака примене рачунарства у облаку јесте одабрати који облак ће се применити. Модели примене заправо описују на који начин се приступа облаку. Постоје четири модела примене рачунарства у облаку а то су :

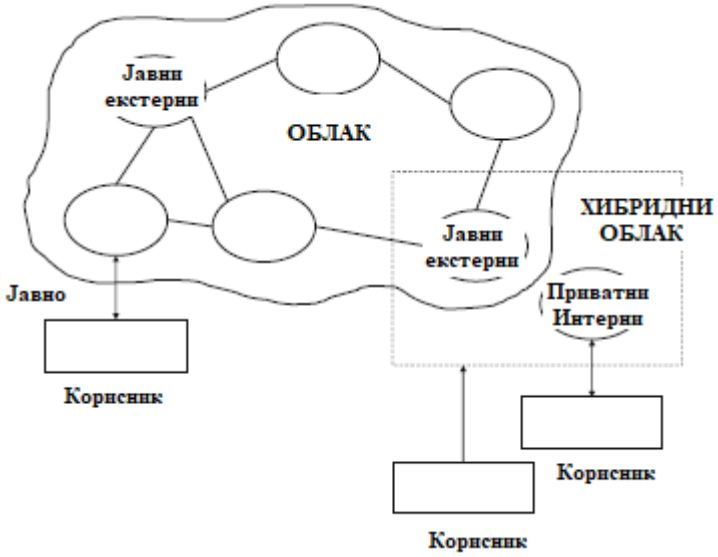
1. Јавни облак (Public cloud)
2. Приватни облак (Private Cloud)
3. Хибридни облак (Hybrid Cloud)
4. Облак заједнице (Community Cloud)

Како технологија у облаку пружа корисницима бројне предности, те погодности морају бити категорисане на основу захтева корисника. Који се модел користи у организацији зависи од саме природе пословања. Модел примене у облаку представља

тачну категорију окружења у облаку засновану на власништву, величини и приступу, а такође описује природу и сврху облака.

Организације и компаније прелазе на пословање у облаку како би се смањили капитални трошкови и регулисали оперативни трошкови, што је уједно и главни разлог преласка са класичног на оваквог концепта пружања услуга [7].

Ради лакшег разумевања дати типови рачунарства у облаку су приказани на слици 3.



Слика 3 Типови cloud рачунарства [1]

Као што се може видети са слике 3 јавни облак је доступан готово свима, док је приватни облак доступан само одређеним корисницима, обично су то приватни подаци који се тичу само одређене организације.

2.4.1 Јавни облак (Public cloud)

Рачунарски ресурси се у јавном облаку обезбеђују динамичким путем, преко веб апликација или веб услуга од независног добављача. Облацима управља трећа страна, а апликације различитих купаца вероватно ће се мешати заједно на серверима у облаку, системима за складиште и мрежама [1].

Корисници преко веб прегледача приступају јавним облацима. Корисници морају да плаћају само за време коришћења услуге, тј. плаћање по употреби. Тиме се постигао ефекат коришћења и природне наплате услуга као код класичних начина. Плаћа се само онај износ који потрошачи оствари као корисник услуга јавног облака. Овакав начин плаћања помаже у смањењу оперативних трошкова за IT трошкове. За разлику од осталих модела јавни облак је најподложније место за неовлашћене радње, јер су сви подаци и апликације на јавном облаку склони нападима од стране присутних малвера и злонамерних програма којма се жели приступ подацима и ресурсима на мрежи. Безбедносне провере могу да се примене валидацијом обе стране, како од добављача у облаку, тако и од клијента. Такође обе стране морају да идентификују своје одговорности у оквиру својих граница деловања. Јавни облак је ван премисе у којој се различита предузећа могу користити за пружање услуга кориснику узимањем услуге од треће стране [5].

Предности јавног облака [7].:

- Флексибилност
- Поузданост
- Висока скалабилност

- Ниска цена
- Независност локације

Недостаци јавног облака :

- Мања безбедност
- Тежа прилагодљивост

2.4.2 Приватни облак (Public cloud)

Приватни облак или интерни облак, односи се на рачунарство у облаку на приватним мрежама. Приватни облаци су креирани искључиво за употребу једног клијента, пружајући потпуну контролу над подацима, сигурношћу и квалитетом услуге. Приватне облаке може изградити компанија чијој организацији је потребна ова технологија и њена информационо технолошка организација или добављач облака [1].

Рад са приватним облацима налази се у унутрашњем центру података предузећа. Главна предност лакша контрола над безбедношћу, одржавањем и надградњом, а такође пружа контролу над применом и употребом. Може се упоредити са интернетом. У поређењу са јавним облаком где свим ресурсима и апликацијама управља добављач услуга, у приватном облаку ове услуге се удружују и стављају на располагање кориснику на организационом нивоу. Овим ресурсима и апликацијама управља сама организација. Како само корисници организације имају приступ приватном облаку, сигурност је знатно побољшана [5].

Предности приватног облака :

- Висок ниво приватности и заштите података: Дељење ресурса у приватном облаку је изузетно заштићено.
- Потпуна контрола : Приватни облаци пружају већу контролу над својим ресурсима од јавног облака јер му се може приступити само у границама организације.

Недостаци који су присутни код приватног облака су :

- Лоша скалабилност : Приватни тип облака се скалира у оквиру интерних ограничених хостованих ресурса.
- Виша цена : Зато што пружа више функција и већу заштиту зато је и скупљи од јавног облака.
- Ограничења : Приватном облаку се може приступити локално у организацији, док га је теже изложити глобално

2.4.3 Хибридни облак (Hybrid Cloud)

Хибридно окружење у облаку комбинује више јавних и приватних модела. Хибридни облаци уводе сложеност одређивања начина дистрибуције апликација и у јавном и у приватном облаку [1].

Овај модел се састоји и од јавног и од приватног модела облака, где се окружење рачунарства у облаку хостује и њиме управља трећа страна, али неке наменске ресурсе приватно користи само организација. У овом моделу приватни облак је повезан са једном или више спољних услуга у облаку. То је сигурнији начин за контролу података и апликација и омогућава странкама приступ информацијама путем интернета. Омогућава организацији да задовољи своје потребе у приватном облаку и ако се јаве неке повремене потребе затражи од јавног облака интензивне рачунарске ресурсе [5].

Хибридни облак је још један тип рачунарства у облаку, који је интегрисан и може бити комбинација два или више сервера у облаку, тј. приватни, јавни или заједница комбиновани као једна архитектура, али остају појединачни ентитети. Мање критични задаци попут развојних и тестних оптерећења могу се обављати помоћу јавног облака, док се критични задаци који су осетљиви, попут руковања подацима организације, обављају помоћу приватног облака. Предности оба модела примене, као и модела примене у заједници, могуће су у хибридном хостингу у облаку. Хибридни модел примене у облаку не само да штити и контролише стратешки важне ресурсе, већ то чини на најекономичнији могући начин у сваком појединачном случају. Такође, овај приступ олакшава пренос података и апликација [7].

Предности хибридног облака :

- Флексибилност
- Сигурност
- Исплативост
- Висока скалабилност

Недостаци који су присутни код хибридног облака су :

- Компликовани проблеми на мрежи
- Усклађеност са безбедношћу организације

2.4.4 Облак заједнице (Community Cloud)

Модел заједнице у великој мери подсећа на приватни облак, једина разлика је у скупу корисника. Док приватни тип подразумева да само једна компанија поседује сервер, у случају заједнице, неколико организација са сличним пореклом дели инфраструктуру и сродне ресурсе. Пример такве заједнице је где су организације и фирме заједно са финансијским институцијама, банкама.

Више-станарска конфигурација развијена је коришћењем облака међу различитим организацијама. Организације припадају одређеној заједници или групи која има сличне рачунарске проблеме. За заједничке пословне организације, предузећа, истраживачке организације и тендере, облак заједнице је одговарајуће решење. У овом случају је пресудан избор праве врсте хостинга у облаку. Дакле, корисници облака засновани на заједници морају прво да знају и анализирају пословну потражњу [7].

Предности модела заједнице су :

- Смањени трошкови
- Побољшана сигурност, приватност и поузданост

- Једноставна размена података и лака сарадња

Недостаци модела заједнице :

- Скупљи у поређењу са јавним моделом примене
- Дељење фиксног капацитета за складиштење и пропусног опсега
- Није превише распрострањен

2.5 Разлика између cloud рачунарства и cloud услуга

У овом одељку биће предочене најзначајније разлике између рачунарства у облаку и рачунарства у облаку као услуге. Разлике су приказане у табелама 1 и 2 које показују особине cloud рачунарства и cloud услуга. Рачунарство у облаку је информациона технологија која је у основи рачунарства у облаку као услуге и састоји се од технологија које омогућавају услуге у облаку [1].

Кључни атрибути рачунарства у облаку приказани су у табели 1.

Табела 1 Кључни атрибути рачунарства у облаку [1]

Атрибути	Опис
Инфраструктурни систем	Укључује сервере, складишта и мреже које се могу прилагодити по захтеву корисника.
Апликациони софтвер	Пружа веб интерфејс, API за веб услуге, и богат избор конфигурација.
Развој апликација и софтвер за размештање	Подржава развој и интеграцију облака апликациони софтвер.
Систем и софтвер за управљање	Подржава брзо пружање и конфигурацију самопослуживања и праћење употребе.
IP мреже	Оне повезују крајње кориснике са облаком и инфраструктуром компоненте.

Кључни атрибути услуга у облаку сажети су у Табели 2 [1].

Табела 2 Кључни атрибути услуга у облаку [1]

Атрибути	Опис
Независни добављач	У извршењу у облаку, претпоставља се да независна компанија пружа услуге. Такође постоји могућност интерног пружања услуга у облаку.

Приступ путем интернета	Услугама се приступа путем стандардне универзалне мреже приступа. Такође може укључивати сигурност и квалитет услуге
Опције	Минимална или никаква информатичка вештина није потребна. Поједностављена је спецификација захтева.
Резервисање	Укључује захтев за самопослуживање, готово у реалном времену уз примену динамичког скалирање.
Цене	Цене се формирају на основу могућности и коришћењу услуга.
Кориснички интерфејс	Кориснички интерфејс укључује прегледаче за разне уређаје и са богатим могућностима.
Системски интерфејс	Системски интерфејси се заснивају на API-има веб услуга, пружајући стандардни оквир за приступ и интегрисање међу услугама у облаку.
Заједнички ресурси	Ресурси се деле између корисника услуга у облаку; Међутим преко опција конфигурације са услугом, постоји способност прилагођавања.

2.6 Карактеристике рачунарства у облаку

Важно је знати карактеристике све популарније технологије за пружање услуга. Како би се пружала услуга путем рачунарства у облаку потребно је разумети његове главне карактеристике. Тиме се добијају информације које су потребне за реализацију услуга, а које могу бити веома различите.

„Рачунарство у облаку донело је нове функције у поређењу са другим парадигмама“ (Wang et al., 2008; Grossman, 2009). Главне карактеристике које поседује cloud рачунарство су следеће [1]:

- Скалабилност (могућност накнадног проширивања система када се јави потреба за тим)
- Услуге на захтев корисника
- Кориснички орјентисан интерфејс који не зависи од локације и може му се приступити путем веб услуга и интернет претраживача
- Гарантовани квалитет услуге у погледу хардвера, перформанси, пропустности и капацитета меморије

- Аутономни систем који омогућава кориснику транспарентно управљање. Софтвер и подаци унутар облака могу се аутоматски поново конфигурисати и реорганизовати на једном месту у зависности од потребе корисника

- Рачунарство у облаку не захтева велика улагања. Корисници плаћају услуге и капацитет по потреби

Удруживање ресурса – добављач има могућност повлачења рачунарских ресурса како би пружио услуге купцима уз помоћ више-станарског модела. Могу се доделити или прерасподелити различити физички и виртуелни ресурси, зависно од потражње купаца. Купац најчешће нема контролу нити информацију о локацији обезбеђених ресурса, међутим могуће је одредити локацију на вишем нивоу апстракције.

Једноставно одржавање – једна од карактеристика јесте и лако одржавање сервера, а време застоја је врло мало, чак у неким случајевима нема застоја. Рачунарство у облаку се постепено побољшава и долази до сталних ажурирања која га постепено побољшавају. На тај начин се исправљају евентуалне грешке и добија се на брзини рада уз особину компатибилности свим уређајима.

Широк приступ мрежи – Приступање и отпремање података у облаку може се извршити са било ког места уз помоћ уређаја који подржава технологију приступа облаку и интернет везе.

Доступност – Различите потребе и захтеви корисника стварају различиту архитектуру облака, а једна од карактеристика рачунарства у облаку јесте прилагодљивост и доступност. Облак се може модификовати према употреби и може се проширити уколико је то потребно. Cloud рачунарство нуди простор за складиштење и омогућава кориснику да купи додатни простор за складиштење ако је то потребно.

Аутоматски систем – облак аутоматски анализира потребне податке. Аутоматски систем прате и стални надзор и контролу над подацима.

Економичност – Економичност се огледа у томе што компаније улажу свој новац у једнократну инвестицију за куповину простора. Новац се троши највише на одржавање и још неколико трошкова који су јако мали и занемарљиви.

Безбедност – безбедност је једна од упечатљивих карактеристика рачунарства у облаку. Начин да се постигне већа безбедност јесте да се праве резервне копије података у складишту, на тај начин су подаци сачувани од губитка чак и ако дође до физичког оштећења сервера. Подаци се чувају у уређајима за складиштење, које ниједна друга особа не може да злоупотреби и користи. Услуга складиштења је брза и поуздана.

Плаћање након приступа - У рачунарству у облаку корисник плаћа услугу или простор који користи. Не постоје скривени или додатни трошкови. Услуга је са економске стране гледишта повољна а добар део простора је додељен бесплатно.

Мерење услуга – Коришћење ресурса анализира се подржавањем могућности наплаћивања по употреби. То значи да се употреба ресурса које могу бити инстанце виртуелног сервера које се изводе у облаку надгледају и извештавају од стране добављача услуга. Модел плаћања је променљив на основу стварне потрошње производне организације [8].

3. Архитектура cloud рачунарства

У овом одељку се разматрају архитектонски принципи који су типични за услуге рачунарства у облаку. Биће објашњене преовлађујуће технологије које се користе за реализацију рачунарства у облаку, такође се разматрају недостаци и предности архитектуре cloud рачунарства [24].

Компанија Intel о архитектури рачунарства у облаку износи став: „Услуге и подаци егзистирају у дељеном, динамичком скалабилном скупу ресурса заснованом на технологији виртуелизације или скалираним апликативним окружењима“ [1].

3.1 Дефиниција архитектуре рачунарства у облаку

Када се говори о термину архитектуре прво на шта се помисли су свакако пројектовање и конструкција објеката, заступљених у високоградњи. Иако се уобичајено термин везује за сам дизајн објекта, овај израз се односи и на функционалност која се постиже применом одређених принципа. У свету информационих технологија, ако једна од компоненти не ради исправно дуж ланца приступа, имплементација облака неће бити успешна.

Cloud инжењеринг јесте примена инжењерских дисциплина у рачунарству у облаку. Доноси систематичан приступ питањима високог нивоа комерцијализације, стандардизације и управљања у осмишљавању, развоју, раду и одржавању система рачунарства у облаку. То је мултидисциплинарна метода која покрива различите области као што су системи, софтвер, веб, перформансе, инжењеринг информационе технологије, сигурност платформа, ризик и квалитета [9].

Cloud архитектура се бави кључним потешкоћама око обраде података великих размера. У традиционалној обради података тешко је добити онолико машина колико је апликацији потребно. Тешко је набавити машине када су потребне. Потребно је дистрибуирати и координирати велики посао на различитим машинама, покретати процесе на њима и обезбедити другу машину за опоравак ако једна машина закаже. Постоје потешкоће да се аутоматски скалира на основу динамичких радних оптерећења. Тешко је отарасити се свих тих машина када је посао завршен. Cloud архитектура решава такве потешкоће захваљујући виртуализацији о којој ће бити говора у наредним одељцима.

Апликације изграђене по правилима cloud архитектуре раде у облаку где добављач одређује физичку локацију инфраструктуре. Апликације користе предности једноставних API-ја који се прилагођавају захтевима да би се услуга реализовала. Коришћење ресурса у архитектури облака је по потреби, понекад краткотрајно или сезонски, пружајући на тај начин највећу искоришћеност и оптималан учинак [9].

3.2 Пословне предности архитектуре у облаку

Постоје јасне пословне користи од израде апликација помоћу cloud архитектуре. Неке од најзначајнијих предности имплементирања архитектуре у облаку су:

- **Готово да нема унапред уложених средстава у инфраструктуру**: Ако се реализује систем великих размера, највише ће бити улагања у опрему, притом се мисли на хардвер (постоља, машине, рутери, резервна напајања), затим улагања у погледу управљања хардвером (управљање напајањем, хлађење) и оперативно особље. Због трошкова унапред, обично би требало неколико кругова одобрења пре него што пројекат уопште може да започне. Сада, са рачунарским услужним програмом, нема фиксних трошкова нити трошкова покретања.

- **Правовремена инфраструктура**: У прошлости, ако се постане успешна компанија, а систем или инфраструктура се нису повећавали, настају велики трошкови који се углавном односе на недостатак капацитета. Супротно томе, ако се уложе велика средства и изостане успех, долази до потпуног економског краха и пропасти бизнис идеје. Размештањем апликација у облаку са софтвером за динамичко управљање капацитетом, архитекте не морају да брину о томе да ли ће унапред набавити капацитет за велике системе. Решења су ниског ризика јер се скалира према потребама (капацитети се прилагођавају потребама). Cloud архитектуре могу да се одрекну инфраструктуре онолико брзо колико је било потребно и поставити систем.

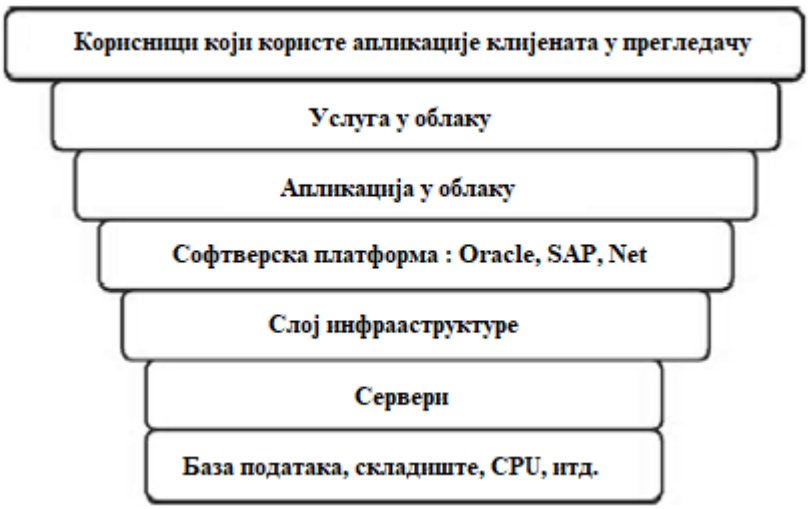
- **Ефикасно коришћење ресурса**: Администратори система обично брину о набавци хардвера (када им понестане капацитета) и бољем коришћењу инфраструктуре (када имају вишак и неактиван капацитет). Помоћу cloud архитектуре могу ефикасније управљати ресурсима, апликацији се уступају ресурси само они који су потребни (на захтев).

- **Израчунавање трошкова засновано на употреби**: Цене се одређују као код комуналних услуга, омогућавају наплату купцу само за кориштену инфраструктуру. Купац није одговоран за целокупну инфраструктуру која постоји. Ово је суптилна разлика између desktop апликација и веб апликација. Апликација за радну површину или традиционална апликација клијент-сервер ради на сопственој инфраструктури купца (PC или сервер), док у апликацији cloud архитектуре купац користи независну инфраструктуру и наплаћује се само за њен део који је коришћен.

- **Потенцијал за смањење времена обраде**: Паралелизација је један од сјајних начина за убрзање обраде. Ако једном рачунарски интензивном послу или захтеву података који се може паралелно изводити треба 500 сати да се обради на једној машини, помоћу cloud архитектуре, могло би се појавити и 500 инстанци и исти посао обрадити за 1 сат. Расположивост еластичне инфраструктуре пружа апликацији могућност да искористи паралелизацију на исплатив начин смањујући укупно време обраде.

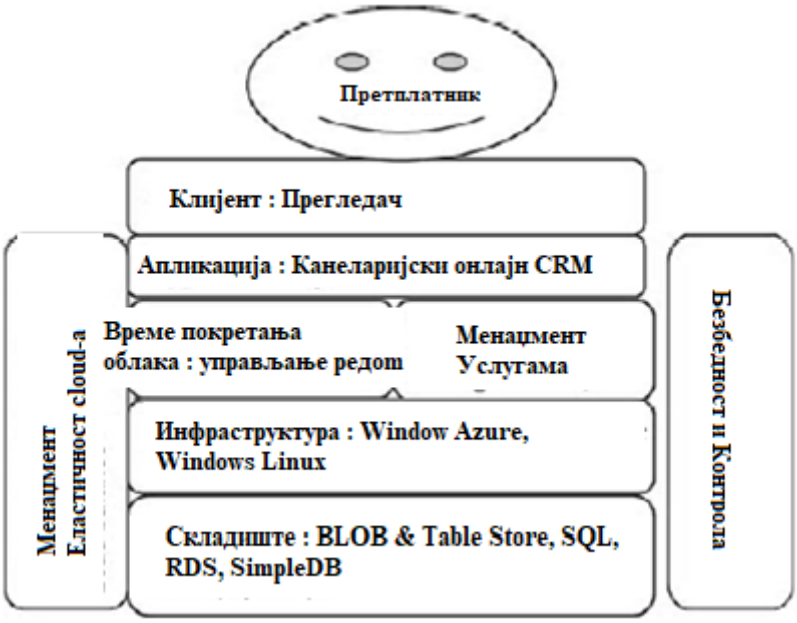
3.3 Слојеви архитектуре облака

Имплементација архитектуре облака састоји се од неколико слојева. На врху ових слојева налази се прегледач покренут на радној површини компјутера и мобилним уређајима које корисник користи за приступ апликацијама хостованим у облаку. На слици 4 приказани су типични слојеви архитектуре облака [10].



Слика 4 Слојеви рачунарства у облаку [10]

Архитектура рачунарства у облаку имплементирана је кроз неколико компоненти. Корисници или претплатници у облаку су првенствено људи који користе услуге у облаку или као SaaS, PaaS или IaaS модел. На слици 5 налазе се компоненте cloud архитектуре [24].



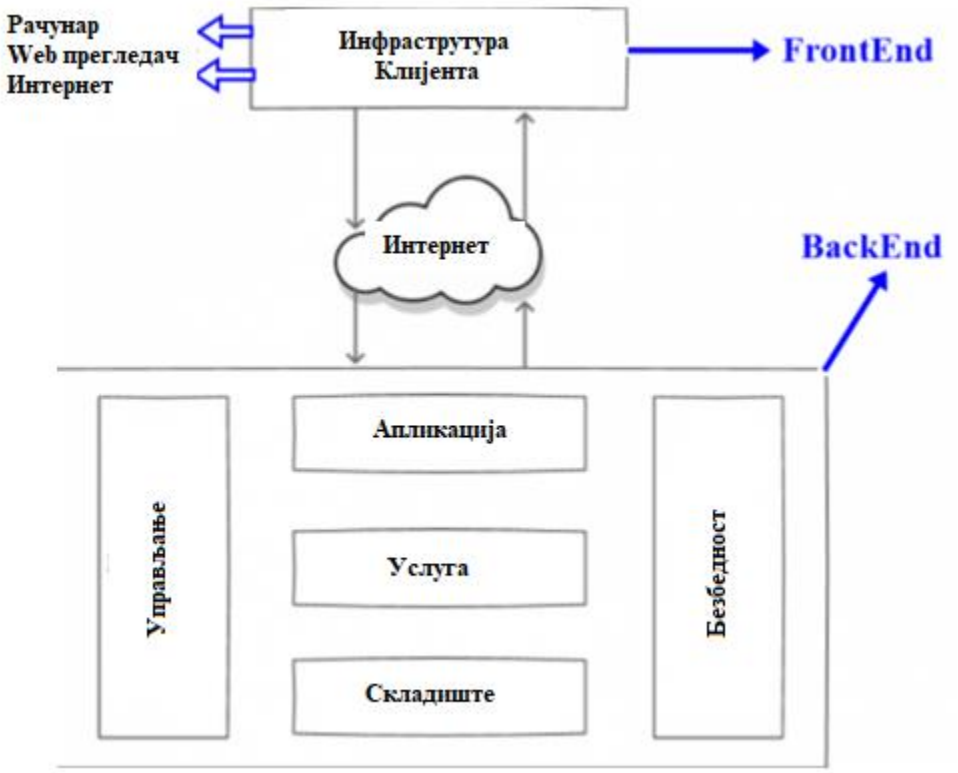
Слика 5 Архитектура облака компоненте [10]

Архитектура рачунарства у облаку састоји се од две главне компоненте :

- **Front-end** (Предњи део) - Део који је видљив крајњем кориснику назива се предњи део. Ово укључује радну површину или било који други уређај крајњег корисника (мобилни телефон, I-pad итд.) прегледач и мрежу. То су клијентски рачунари или рачунарске мреже као и апликације које су неопходне за приступ облаку. Интерфејси различитих облака се разликују. На пример web-mail-у се приступа преко постојећих читача (Firefox, Chrome), док други системи имају јединствене апликације којима се обезбеђује мрежни приступ клијенту.

- **Back-end** (Задњи део) - Задњи део је део архитектуре рачунарства у облаку који је скривен иза мреже која се састоји од различитих апликација, софтвера, рачунара и уређаја за складиштење података. Ту спадају сервери, системи за складиштење података и софтвери који чине облак рачунарских сервиса. Сервери не раде увек пуним капацитетом па се услед тога јавља не искоришћена процесорска снага. Предњи и задњи део су повезани путем мреже, најчешће је то интернет.

На следећој слици је графички приказан међусобни однос FrontEnd-a i BackEnd-a.



Слика 6 Графички приказ међусобне везе између предњег и задњег дела [11]

Cloud архитектура обухвата низ различитих система и технологија, као што су модели сервиса, модели примене и пословни модели. Комбинација је три под-архитектуре, пословне, техничке и оперативне.

Пословна архитектура - дизајнира пословне аспекте услуга у облаку који покривају цене, уговоре о услугама и моделе трошкова. Такође укључује пословни модел и његову комуникацију са разним актерима.

Техничка архитектура - детаљно описује дизајн различитих компоненти у облаку.

Оперативна архитектура покрива оперативну изводљивост, доступност мреже, правна питања у вези са локацијом хостовања података, праћење оперативних перформанси.

Управљање облаком - укључује активности као што су управљање догађајима, конфигурација и усаглашеност, обезбеђивање ресурса, уравнотежење радног оптерећења и интеграција услуга.

Безбедност облака - укључује функције као што су управљање идентитетом и приступом, шифровање података, сегрегација између корисника и заштита, изолација VM (Виртуелних машина), сигурна миграција VM-а, изолација виртуелне мреже, безбедносна

интелигенција и софтвер, платформа и безбедност инфраструктуре и надзор догађаја и надзор приступа [10].

Безбедност осигурава [10]:

- Приступ аутентичности и ауторизацији
- Обезбеђивање непрекидне доступности
- Одржавање поверљивости клијента
- Управљање идентитетом претплатника

3.4 Екосистем cloud архитектуре

Брокери - Иако корисници желе услугу, њима ће бити потребан посредник који ће заступати њихов интерес. Посредник између захтева корисника и услуге комбинује различите захтеве корисника са стандардизованим захтевима. Пример посредника могу бити аутомобилске компаније које продају навигационе системе, а који својим посредством разумеју и пружају подршку на захтев корисника о правцу кретања при вожњи.

Улога посредника у облаку је да делује као посредник између добављача облака и корисника како би корисника учинио транспарентним због сложености облака. Своју улогу играју као потрошач услуге, као и пружалац услуге обављајући посредовање у услугама, агрегирање и арбитражу услуге. Овај ентитет пружа посредничке услуге попут управљања идентитетом, извештавања о учинку, побољшане безбедности, а такође нуди и агрегације услуга, као што су интеграција података и кретање између различитих корисника и добављача у облаку [1].

Стваралац услуга: То би били људи или ентитети који планирају и развијају услуге и представљају их корисницима / брокерима уз накнаду. Дакле, ова особа прави апликацију и представља је корисницима и брокерима. Овај ентитет такође хостује услугу у окружењу у облаку које нуди добављач услуга у облаку.

Алокатор ресурса: Повезује кориснике и добављача услуга у облаку. Овај ентитет се брине о управљање ресурсима и гарантује ниво услуге.

Cloud провајдер: Централни играч међу свим екосистемима у облаку назива се добављач облака који пружа услуге у облаку. нпр. Amazon, Microsoft, IBM или Google. Овај ентитет пружа и управља рачунарском инфраструктуром и хардвером и софтвером за испоруку услуга у облаку корисницима путем интернета. Улога коју пружа добављач облака ће се разликовати у зависности од врсте услуга у облаку као што су SaaS, PaaS или IaaS.

Испитивач и контролор захтева за услугом: Ова особа (или аутоматизовани систем под надзором стручњака) додељује и прерасподељује ресурсе на основу унапред дефинисаног приоритета, као што су доступност ресурса и критичност.

Менаџер финансија : На основу врсте захтева и плана плаћања, ова особа (или аутоматизовани систем под надзором стручњака) одређује цене и обрачунава употребу.

Управљач VM-а: Управљач VM-а брине о виртуелним машинама и њиховој доступности [1].

4. Пословни софтвер као услуга и примена cloud рачунарства у пословне сврхе

Cloud апликације постају све популарније и учесталије када је у питању обављање неког задатка везаног за сам посао који се обавља. Сталним усавршавањем технологије и надградњом се побољшава њихова ефикасност и употреба. Рачунарство у облаку се више посматра као нови пословни модел, а не као нова технологија. Овакав начин пословања нуди повољне могућности за управљањем рачунарским ресурсима и софтверским платформама и могућности за брзо додавање нових карактеристика у складу са променљивим потребама. Практично то значи да уколико компанија уведе нови производ или постројење за рад, врло лако може да се надогради систем и прилагоди потребама које су новонастале [13].

Cloud пословање омогућава компанијама да извршавају своје главне функције у новом окружењу које пружа добру основу за започињање или ширење посла без великих улагања. Постоје могућности за оптимизацију пословних процеса и смањење времена за прилагођавање променљивим тржишним условима.

Технологије подржавају брзи раст пословања осигуравајући приступ практично неограниченим ресурсима. На основу cloud технологија, компаније могу створити флексибилну стратегију за развој уз максимално коришћење ресурса, минималне напоре за њихово одржавање и ефикасно спровођење пословних активности [13].

4.1 Лак приступ компанијама - cloud технологија

Рачунарство у облаку је модел који пружа свеприсутан и погодан приступ ресурсима дељеног рачунара који се могу брзо испоручити великом броју корисника (на захтев) и активирати уз минимални напор управљања или помоћ добављача услуга. Ова особина је нарочито корисна компанијама јер су увидели предност примене оваквог начина пословања. Такође оно што је у основи рачунарства у облаку јесте особина лаког приступа са уређаја са било ког места и са било којим уређајем [13].

4.2 Рачунарство у облаку и бизнис

Рачунарство у облаку постало је неизоставна технологија за сваку компанију. Има значајан потенцијал и пружа ефикасне пословне могућности за организације које су усвојиле овај приступ.

Заједно са свим предностима повезаним са рачунарством у облаку, предузећа могу имати и додатне користи а то су [13]:

- Смањене инвестиције за изградњу IT инфраструктуре и административни трошкови за IT особље. Cloud технологије елиминишу потребу за значајним капиталним улагањима - компаније не морају да купују скупу опрему (сервере и мрежну опрему) и софтверске лиценце. Своје пословање могу започети запошљавањем мање рачунарских ресурса и повећати их тек када њихове потребе расту. Долази до трансформације капиталних инвестиција у оперативне трошкове и на тај начин се уклања велика баријера за улазак у посао. Мала и средња предузећа могу себи приуштити да ангажују ресурсе и технологије, које не могу да купе, и полазе са једнаких позиција са осталим конкурентима на тржишту.

- Могућности коришћења савремених ICT (Информационо телекомуникационе технологије), које омогућавају ефикасно управљање пословним процесима. Мањи предузетници не могу приуштити куповину најновијих верзија софтвера и плаћање лиценци, али захваљујући технологијама у облаку имају савремене апликације без скупих лиценци на годишњем или месечном нивоу.

- Скалабилност пословања. Из пословне перспективе технологије у облаку омогућавају организацијама не само да повећају или смање софтверски капацитет, већ и да прошире своје пословне процесе и активности. Могућност за брзо и готово неограничено пружање рачунарске снаге и софтверских апликација подржавају раст и ширење компанија.

- Прилагођавање променљивим тржишним условима. Данашња економска ситуација и окружење захтевају способност брзе реакције и реаговања на променљиве услове и потребе потрошача. Кроз рачунарство у облаку компаније могу брзо прилагодити процесе, производе и услуге у новим околностима и тиме бити конкурентније на тржишту.

4.3 Cloud рачунарство и примена канцеларијских пакета

Cloud апликације су нашле примену као помоћ у канцеларијским пословима. Предности ових пакета у односу на традиционалне су [13]:

- **Једноставна администрација.** Office пакетима је могуће приступити путем веб прегледача и могу се користити без обзира на оперативни систем. Нема потребе за инсталирањем пакета на локалне уређаје, а добављач услуга редовно ажурира верзије софтвера.

- **Смањени трошкови.** Компаније не морају да плаћају старе накнаде за лиценцу. Обично су цене на месечном нивоу по кориснику, али понекад постоје годишњи планови са попустима.

- **Приступачност.** Документи су доступни било где и било када, са различитих уређаја (укључујући мобилне уређаје) са различитим оперативним системима и прегледачима.

- **Размена докумената и сарадња.** Cloud Office пакети пружају могућности за размену докумената, заједнички истовремени рад на њима са опцијама за праћење промена. Све ове могућности повећавају продуктивност канцеларијског рада.

Неки од најпопуларнијих пакета овог типа су : Google Apps for Work, Microsoft Office 365 and Zoho Docs) [13].

4.3.1 Google Apps for Work пакет

Google Apps for Work (раније познат као Google Apps for Business) је канцеларијски пакет заснован на технологијама у облаку који укључује додатне функције специфичне за пословање у канцеларијама. Апликације у пакету могу се груписати у четири категорије): Комуникација (Gmail, Hangouts и календар итд), Чување (Диск), Сарадња (Документи,

Табеле, Обрасци, Презентације и Сајтови) и Управљање (Администратор и Трезор). Постоји бесплатни пробни период од 30 дана (до 10 корисника). Постоје различите опције плаћања са могућностима флексибилног додавања нових корисничких рачуна - флексибилни план (плаћање се врши за услуге које се користе сваког месеца) и годишњи план (уговор је на годину дана са попустима). Google Apps for Work пружа могућности за рад ван мреже, корисници могу да креирају и уређују садржај чак и када нису повезани са интернетом и касније га синхронизују када су на мрежи [13].

4.3.2 Microsoft Office 365 пакет

Microsoft Office 365 укључује традиционалне компоненте за Office пакете и пружа готово све функције стандардног Office-а. Office 365 пружа алате за сарадњу и размену података у реалном времену - документи се чувају у облаку и сви имају приступ својој најновијој верзији. Постоје опције за праћење промена и опоравак старијих верзија. Сарадња укључује мрежне састанке, портал за размену корпоративних видео записа и слично. Microsoft Office 365 укључује друштвену мрежу предузећа Yammer, која подржава сарадњу међу запосленима. Постоје разне опције за коришћење Microsoft Office 365 као што су business plans and enterprise plans, који нуде различите функције по различитим ценама [13].

4.3.3 Zoho Office Suite пакет

Zoho Office Suite је бесплатни софтверски пакет који укључује апликације за обраду текста, прорачунске табеле и презентације. Постоје могућности за синхронизацију датотека на различитим уређајима и одржавање различитих верзија докумената. Zoho подржава све врсте Microsoft Office докумената, омогућава извоз у XML, PDF и LaTeX формат. Zoho пружа могућности за дељење датотека, интеграцију са Google apps-ом, управљање задацима. Пакет укључује апликацију за олакшавање рада на пројектима. Zoho нуди сарадњу у реалном времену, као што су мрежни састанци, дељење радне површине и приватна друштвена мрежа Connect која запосленима омогућава размену података и међусобну сарадњу. Главна предност Office Suite-а је доступност апликација специфичних за посао као што су маркетиншки и финансијски алати, CRM систем, управљање људским ресурсима и други [13].

4.4 Услуге складиштења у облаку

Услуге складиштења у облаку омогућавају компанијама да избегну куповину додатног хардвера за: складиштење података, одржавање како би се спречио губитак података, редовне активности у прављењу резервних копија података. Ове услуге у облаку омогућавају размену података између запослених у компанији, као и између компаније и њених партнера, купаца, добављача итд. Главне предности услуга складиштења у облаку су:

- Приступ подацима било када и било где, без обзира на хардверске уређаје и софтвер (већина решења у облаку пружа мобилни приступ ускладиштеним подацима).
- Синхронизација података између различитих уређаја и корисника.
- Интеграција са менаџерима датотека оперативног система.

Међу најпопуларнијим услугама складиштења у облаку су Dropbox, Box, Google Drive и OneDrive [13].

4.4.1 Dropbox

Dropbox је једна од најпопуларнијих услуга складиштења у облаку. Његова главна предност је могућност синхронизације података између различитих уређаја. Услуга је доступна како за појединачне тако и за пословне кориснике. Dropbox за предузећа пружа додатне услуге као што је побољшана сигурност података коришћењем шифровања за податке у датотекама, неограничено складиштење, алати за управљање сарадњом (праћење процеса дељења података, ограничавање приступа датотекама или њихово дељење са спољним људима који нису део пословног налога), интеграција са другим апликацијама. Корисници се могу повезати, а истовремено постоји раздвајање између личног и радног Dropbox-а [13].

4.4.2 Box

Box је услуга у облаку која пружа простор за складиштење података - бесплатно са одређеним ограничењима, као и верзије које се плаћају, а намењене су првенствено пословним корисницима. Box for Business нуди могућности за дељење радног простора између више корисника. Box омогућава сарадњу осигуравајући сигурност и приватност података постављањем и додељивањем различитих нивоа дозвола сваком сараднику. Постоје алати за контролу и управљање садржајем који се дели са спољним корисницима и праћење учинка корисника (који садржај деле и са ким раде заједно). Box подржава сарадњу на пројектима путем управљања задацима што омогућава додељивање и праћење појединачних задатака члановима тима и смањење неефикасне комуникације. Box пружа могућности за интеграцију са различитим апликацијама [13].

4.4.3 Google Drive

Google Drive је део решења у облаку које нуди Google и није само услуга за складиштење података, већ пружа и могућности интеракције у реалном времену. Постоје бесплатна услуга са одређеним ограничењима, као и плаћене услуге (Google drive for work) са неограниченим простором за складиштење података. Google диск омогућава синхронизацију информација којима се може приступити са различитих уређаја. Дељење информација може бити и интерно (са колегама) и екстерно (са купцима и партнерима), а могуће је чак и са корисницима који не користе Google disc, a Google документи омогућавају истовремено заједнички рад на истом документу. Постоје алати за аутоматско ажурирање и обавештавање о променама у дељеним документима, праћење и одржавање историје промена, управљање различитим верзијама [13].

4.4.4 OneDrive

OneDrive је Microsoft услуга у облаку која корисницима пружа простор за складиштење и даљински приступ подацима. Услуга омогућава интеграцију Microsoft Offica и Windows Phone и различитим опцијама за отпремање и приступ подацима путем веба, директно из апликација Microsoft Office, путем мобилних апликација. OneDrive нуди бесплатан простор на личном диску за складиштење података. OneDrive For Buisness је услуга намењена организацијама да чувају њихове информације којима многи корисници могу приступити, делити их и синхронизовати. Услуга складиштења је део система Office 365 или SharePoint Server 2019, који такође омогућава сарадњу у документима у реалном времену. OneDrive For Buisness пружа алате за одржавање докумената, преглед и одобравање извршених промена [13].

4.5 Пословни информациони системи у облаку

Данас су пословни информациони системи изузетно важан фактор који пружа потребне информације за доношење одлука. Компаније имплементирају различите софтверске апликације од традиционалних (рачуноводствени, људски ресурси, складиштење) програма до интегрисаних софтверских решења (CRM, ERP, BI, итд.). Информациони системи су скуп софтвер, што је велика инвестиција за компаније и захтева одговарајућу IT инфраструктуру. Више добављача нуди верзије пословних информационих система заснованих на облаку. Решења у облаку омогућавају претварање великих трошкова улагања у оперативне трошкове, што је погодно за мала и средња предузећа и новооснована предузећа.

Предности пословних информационих система у облаку у односу на традиционалне су [13]:

- **Флексибилност и ефикасност.** Нижи су трошкови коришћења услуге (система) који се могу разликовати у зависности од потрошње на основу одређених потреба. Флексибилност се односи на функционалност, у било ком тренутку компаније могу да одлуче да додају нове услуге (модуле) или да напусте постојеће.

- **Побољшана повезаност**. Компаније могу брзо пружити приступ систему или одређеним модулима својим партнерима како би радиле на побољшању сарадње.

- **Лакша администрација.** Администрација и обнова система је одговорност добављача услуга који олакшава IT одељења у компанијама и омогућава њихову оптимизацију.

Коришћење пословних информационих система у облаку прати низ проблема. cloud системи нису тако свеобухватни и функционални као традиционална решења. Постоје потешкоће у прилагођавању услуга у облаку одређеном послу и његовим процесима. Компликована је интеграција са већ постављеним апликацијама (cloud, mobile и традиционалне), које морају да раде у динамичном окружењу.

Упркос овим проблемима и недостацима, cloud системи су добро решење за мала и средња предузећа. Они нису тако скупа опција за употребу савремених пословних информационих система. За компаније које су већ примениле пословне системе, добра одлука је интеграција између облака и традиционалних апликација. Предузећа могу да додају нове модуле са новим функционалностима, који се заснивају на технологијама у облаку, постојећим традиционалним системима. Процес надоградње система омогућава лаку имплементацију и проширење функционалности [13].

4.5.1 Customer Relationship Management (CRM)

CRM је скраћеница од Customer Relationship Management (Управљање односима са клијентима). Софтвер је хостован у облаку тако да корисници могу приступити информацијама путем интернета. CRM софтвер пружа висок ниво сигурности и скалабилности својим корисницима. Лако се користи на мобилним телефонима а приступ подацима је олакшан.

Данас многи пословни добављачи услуга користе CRM софтвер за управљање ресурсима тако да им корисник може приступити путем интернета. Премештање пословних радњи са радне површине у облак показало се корисним кораком како у IT тако и у не-IT областима. Неки од главних добављача CRM-а су : Mothernode CRM, Microsoft Dynamics CRM, Infor CRM, SAGE CRM, NetSuite CRM [5.web].

Неколико предности коришћења CRM-а су следеће:

- Висока поузданост и скалабилност
- Једноставан за коришћење
- Висока сигурност и безбедност
- Пружа флексибилност корисницима и добављачима услуга
- Лако доступан

4.5.2 Enterprise Resource Planning (ERP)

ERP је скраћеница за Enterprise Resource Planning, софтвер је сличан CRM-у који се хостује на cloud серверима који помаже предузећима да управљају и манипулишу својим пословним подацима у складу са њиховим потребама и корисничким захтевима. ERP софтвер се плаћа по коришћењу, односно на крају месеца предузеће плаћа износ према софтверу који користи у току рада. Доступни су различити добављачи ERP-а попут Oracle, SAP, Epicor, SAGE, Microsoft Dynamics, Lawson Softwares и многи други.

Неколико предности коришћења ERP софтвера су [5.web]:

- Исплативост
- Велика мобилност
- Повећање продуктивности
- Нема сигурносних проблема
- Скалабилност и ефикасност

5. Примена технологије за пословни софтвер у облаку

Постојећи интернет нам пружа садржај у виду видео записа, е-поште и информација које се нуде на веб страницама. Са рачунарством у облаку следећа генерација интернета ће нам омогућити да „купујемо“ IT услуге са веб портала, драстично проширујући врсте робе доступне изван оних на веб локацијама за е-трговину као што су eBay и Taobao. Могу се унајмити основне потребе за изградњу виртуелног центра података: као што су CPU, меморија, складиште. Пратећа опрема која је неопходна за реализацију рачунарства у облаку је: сервери веб апликација, базе података, магистрала сервера предузећа као платформу за подршку апликацијама које бисмо желели да изнајмимо од независног добављача софтвера или да се развије сопствена платформа. Заједно, ово називамо „IT као услуга“ или ITaaS (IT as a Serve), који се крајњим корисницима припаја као виртуелни центар података.

Унутар ITaaS-а постоје три слоја која почињу са инфраструктура као услуга или IaaS, а састоје се од физичког дела ког можемо видети и додирнути: сервера, складишта и мрежних прекидача. На нивоу IaaS-а, пружалац услуга рачунарства у облаку може да понуди основне могућности рачунарства и складиштења, као што је центар за рачунарство у облаку које је основао IBM. Узимајући за пример рачунарско напајање, основна јединица коју пружа је сервер, укључујући CPU, меморију, оперативни систем и софтвер за надзор система.

Да би се корисницима омогућило да прилагоде сопствено окружење сервера, прибегава се технологији шаблона сервера, што подразумева повезивање одређене конфигурације сервера и оперативног система и софтвера, као и пружање прилагођених функција по потреби.

Са повећањем виртуализације броја машина за управљање, пружање услуга постаје пресудно, јер директно утиче на управљање услугама, IaaS одржавање и ефикасност рада. Аутоматизација, следећа основна технологија, може учинити ресурсе доступним корисницима путем самопослуживања без укључивања добављача услуга. Стабилан и моћан програм управљања аутоматизацијом може смањити маргиналне трошкове на готово нулу, што заузврат може показати ефикасност рачунарства у облаку. На основу аутоматизације може се реализовати динамичка оркестрација ресурса. Динамичка оркестрација ресурса има за циљ да задовољи захтеве нивоа услуге. На пример, IaaS платформа ће аутоматски додавати нове сервере или просторе за складиштење за кориснике у складу са искоришћеношћу процесора сервера, како би се испунили услови услуге који су претходно направљени са корисницима.

Интелигенција и поузданост динамичке оркестрације ресурса је кључна ствар. Поред тога, виртуализација је још једна кључна технологија. Може максимизирати ефикасност коришћења ресурса и смањити трошкове IaaS платформе, као и употребе корисника промовисањем дељења физичких ресурса. Функција динамичке миграционе технологије виртуелизације може драматично побољшати доступност услуге и ово је пожељно за многе кориснике.

Следећи слој у оквиру ITaaS је платформа као услуга или PaaS. На нивоу PaaS, оно што пружаоци услуга нуде су упаковане IT могућности или неки логички ресурси, као што су базе података, систем датотека и оперативно окружење апликација. Тренутно практични случајеви у индустрији укључују: Rational Developer Cloud of IBM, Azure of Microsoft and AppEngine of Google. На овом нивоу су укључене две основне технологије. Прва је развој софтвера, тестирање и покретање засновано на облаку. Услуга PaaS технологија је оријентисана према програмерима. Некада је програмерима била велика потешкоћа да напишу програме путем мреже у дистрибуираном рачунарском окружењу, а сада због побољшања мрежног опсега две технологије могу решити овај проблем: прва су алати за развој на мрежи. Програмери могу директно довршити даљински развој и апликацију путем прегледача и удаљене конзоле (развојни алати се покрећу у конзоли) технологије без

локалне инсталације развојних алата. Друга је технологија интеграције локалних развојних алата и рачунарства у облаку, што значи да се развијена апликација директно размешта у окружење рачунарства у облаку путем локалних развојних алата. Односи се на скалабилни апликативни међу-програм, базу података и систем датотека изграђен са великом количином сервера.

Ово оперативно окружење апликације омогућава апликацији да у потпуности користи богатство рачунарских ресурса и ресурса за складиштење података у рачунарском центру у облаку како би постигла потпуно проширење, превазишла ограничења ресурса појединачног физичког хардвера и испунила захтеве приступа милионима корисника интернета [1].

Врх ITaaS-а је оно што ће већина корисника видети који нису IT корисници а то је софтвер као услуга (SaaS). На нивоу SaaS-а, добављачи услуга нуде потрошачке или индустријске апликације директно индивидуалним корисницима и корпоративним корисницима. На овом нивоу су укључене следеће технологије: Web 2.0, Mashup, SOA and multi-tenancy (мулти станарство). Развој AJAX технологије Web 2.0 чини веб апликацију лакшом за употребу, а корисницима доноси корисничко искуство десктоп апликација, што заузврат чини људе да се лако прилагоде преносу са десктоп апликације на веб апликацију. Технологија Mashup пружа могућност састављања садржаја на интернету, што омогућава корисницима да слободно прилагоде веб локације и прикупљају садржаје са различитих веб локација, а програмерима омогућава брзу израду апликација.

Слично томе, SOA такође нуди функцију комбинације и интеграције, али пружа функцију у позадини веба. Више-станарско закупништво је технологија која подржава више-станарске закупе и купце у истом оперативном о кружењу. Може значајно смањити потрошњу ресурса и трошкове за сваког купца.

Табела 3 приказује различите технологије које се користе у различитим врстама услуга рачунарства у облаку.

Табела 3 Различите врсте технологија у облаку

Тип Услуге	IaaS	PaaS	SaaS
Категорија услуге	VM изнајмљивање, онлајн складиште	Интернет оперативно окружење, Интернет база података, Ред порука на мрежи	Примена и Изнајмљивање софтвера
Прилагођавање услуге	Шаблон сервера	Логичан ресурс поставки	Шаблон апликација
Пружање услуга	Аутоматизација	Аутоматизација	Аутоматизација
Приступ услузи и коришћење	Удаљена конзола, Web 2.0	Интернет развој и отклањање грешака, Интеграција алата за офлајн развој и cloud	Web 2.0
Надгледање услуга	Праћење физичких ресурса	Логички надзор ресурса	Надгледање апликација
Ниво услуге/ менаџмент	Динамичка оркестрација физичких ресурса	Динамичка оркестрација логичких ресурса	Динамичка оркестрација апликације
Ресурс услуге/ оптимизација	Мрежна виртуелизација, Виртуелизација сервера,	Дистрибуирани систем датотека великих размера, база података, middleware (софтвер	Више-станарски приступ

	Виртуелизација складишта	између базе података и апликације) итд	
Мерење услуге	Мерење физичких ресурса	Мерење употребе логичких ресурса	Мерење употребе пословних ресурса
Интеграција услуга и комбинација	Равнотежа оптерећења	SOA	SOA, Mashup
Сигурност услуге	Шифровање складишта и изолација, VM Изолација, VLAN, SSL/SSH	Изолација података, радно окружење Изолација, SSL	Изолација података, Изолација радног окружења, SSL, Веб аутентификација и ауторизација

Претварање било које IT способности у услугу може бити добра идеја, али да би се то реализовало, мора се догодити интеграција IT скупа.

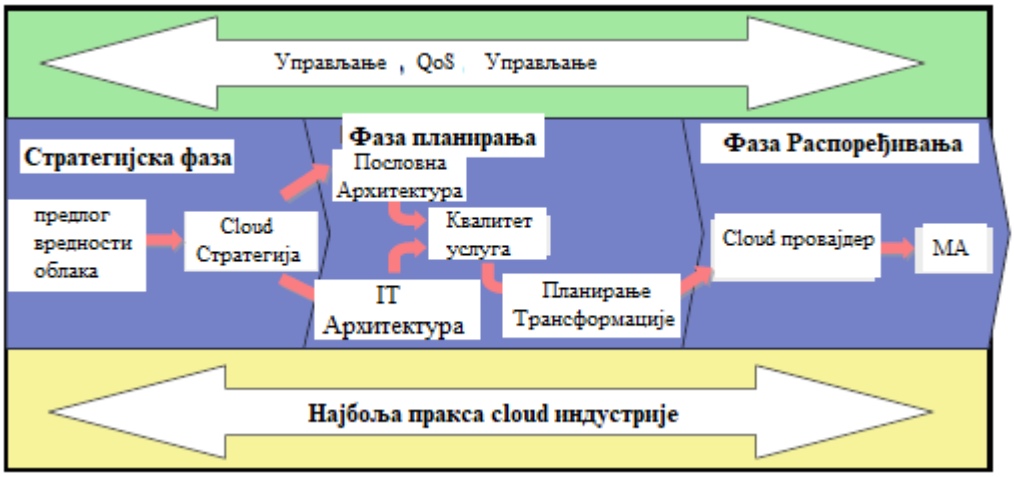
Да резимирамо, кључне технологије које се користе у рачунарству у облаку су: аутоматизација, виртуелизација, динамичка оркестрација, мрежни развој, велико оперативно окружење дистрибуираних апликација, Web 2.0, Mashup, SOA и мулти-станарство итд. Већина ових технологија је напредовала последњих година како би омогућила појаву рачунарства у облаку у реалним апликацијама [1].

5.1 Методологија примене модела рачунарства у облаку

Рачунарство у облаку је нови модел за пружање пословних и IT услуга. Модел пружања услуга заснован је на будућем развоју и истовремено испуњава тренутне развојне захтеве. Три нивоа услуге рачунарства у облаку (Iaas, PaaS i SaaS) покривају широк спектар услуга. Поред рачунарства и модела пружања услуга инфраструктуре за складиштење, различити модели као што су модел података, софтверска апликација, модел програмирања итд. такође могу бити применљиви на рачунарство у облаку.

Још важније, модел рачунарства у облаку укључује све аспекте трансформације предузећа у својој еволуцији, тако да је технолошка архитектура само његов део, а развој више аспеката, као што су организација, процеси и различити пословни модели, такође треба размотрити. На основу методологије стандардне архитектуре са најбољом праксом рачунарства у облаку, методологија примене модела облака може се користити за вођење анализе купаца у индустрији и решавање потенцијалних проблема и ризика који су се појавили током еволуције од тренутног рачунарског модела до модела рачунарства у облаку [1].

Ова методологија се такође може користити као упутство за анализу модела рачунарства у облаку. Користи се за доношење одлука, одређивање процеса, стандарда, интерфејса, примене јавне услуге и управљања IT средствима за промоцију пословног развоја. Слика у наставку приказује укупан састав ове методологије.



Слика 7 Приказ методологије рачунарства у облаку [1]

5.1.1 Стратегијска фаза

Cloud стратегија садржи два корака како би се осигурала свеобухватна анализа стратешких проблема са којима би се купци могли суочити када примењују режим рачунарства у облаку. На основу анализе вредности рачунарства у облаку, ова два корака ће анализирати стање модела потребног за постизање циља купаца, а затим ће успоставити стратегију која ће функционисати као смерница [1].

1. **Предлог вредности за рачунарство у облаку.** Циљ овог корака је да се анализира специфична пословна вредност и начин рада у рачунарству у облаку и одређених корисника, користећи анализу модела захтева корисника рачунарства у облаку и узимајући у обзир најбоље праксе индустрије рачунарства у облаку. Анализирају се кључни фактори који могу утицати на купце да примене режим рачунарства у облаку и дају се предлози о најбољим методама корисничких апликација. У овој анализи се мора идентификовати главни циљ за купца који примењује режим рачунарства у облаку као и кључни проблеми које корисник жели да реши. Следе неколико уобичајених циљева као пример:

    - Поједностављење IT управљања, руковање и смањење трошкова одржавања; иновација у пословном начину; јефтин хостинг outsourcing-a; висококвалитетни хостинг услуге outsourcing итд. Outsourcing је пословна пракса у којој компанија ангажује трећу страну за извршавање задатака, руковање операцијама.

    - Резултати анализе ће бити пружени као подршка о нивоу доношења одлука. Анализа ће се користити за процену стања и као стратегија за будући развој и припрему као и за успостављање стратегије и организацију следећег рачунарства у облаку.

2. **Планирање стратегије у облаку**. Овај корак је најважнији део фазе стратегије. Успостављање стратегије заснива се на резултату анализе вредносног корака и има за циљ успостављање стратешке документације у складу са добрим разумевањем различитих услова са којима се купци могу суочити када примењују режим рачунарства у облаку за планирање будуће визије и перспективе. Професионална анализа направљена горе наведеном методом обично укључује широко истраживање пословног модела купаца, анализу

организационе структуре и идентификацију оперативног процеса, такође постоје неки нефункционални захтеви и ограничења у плану, као што су брига о безбедносном стандарду, захтеви за поузданошћу и правила, прописи итд.

5.1.2 Фаза планирања

У фази планирања у облаку потребно је извршити детаљно истраживање о положају купаца и анализирати проблеме и ризике у примени облака како тренутно, тако и у будућности. Након тога могу се извући конкретни приступи и планови како би се осигурало да купци могу успешно да користе рачунарство у облаку за постизање својих пословних циљева. Ова фаза укључује неколико изведених корака планирања који су наведени на следећи начин [1]:

1. Развој пословне архитектуре

Прихватајући организационе структуре предузећа, пословни модели такође добијају информације о подршци пословним процесима. Како се различити пословни процеси и релативне мреже у архитектури предузећа постављају један за другим, добици и губици које доносе релативни путеви у процесу пословног развоја такође ће ући у разматрање. Категоризујемо их на пословне интересе и могуће ризике које апликација рачунарства у облаку доноси из пословне перспективе.

2. Развој IT архитектуре

Потребно је идентификовати главне апликације потребне за подршку пословним процесима предузећа и кључне технологије потребне за подршку апликацијама предузећа и системима података. Поред тога, требало би увести моделе рачунарства у облаку и направити анализу технолошких референтних модела, како би се пружила помоћ, савети и стратешки водич за дизајн и реализацију начина рачунарства у облаку у архитектури конкретног предузећа.

3. Захтеви за развој квалитета услуге

У поређењу са другим рачунарским режимима услуга, најпрепознатљивија карактеристика рачунарства у облаку је да захтеви за квалитет услуге (који се називају и нефункционалним потребама) треба претходно ригорозно дефинисати, на пример, перформансе, поузданост, сигурност, опоравак од катастрофе итд. Овај захтев је кључни фактор у одлуци да ли је апликација у режиму рачунарства у облаку успешна или није и да ли је постигнут пословни циљ; такође је важан стандард у мерењу квалитета услуге рачунарства у облаку или компетентности за успостављање центра за рачунарство у облаку.

4. Израда плана трансформације

Потребно је формулисати све врсте планова потребних за трансформацију из тренутних пословних система у рачунарство у облаку, укључујући опште кораке, распоређивање, гаранцију квалитета итд. Обично облак инфраструктурних услуга покрива различите ставке као што су извештај о плану консолидације инфраструктуре, план система управљања радом и одржавањем, план процеса управљања, план трансформације апликационог система итд.

5.1.3 Фаза примене

Фаза примене фокусира се углавном на програмирање како фазе реализације стратегије, тако и фазе планирања. У овој фази су наглашена два корака [1] :

1. Добављач рачунарства у облаку (Провајдер):

   Према прошлој анализи, купци ће можда морати да одаберу добављача рачунарства у облаку. Најважније је знати да је услов за споразум о нивоу услуге (SLA) и даље одлучујући фактор за добављаче у успеху пројекта.

2. Одржавање и техничка служба:

   Што се тиче одржавања и техничке услуге, усвојени су различити нивои стандарда. Стандарди су дефинисани захтевом за квалитетом услуга извршених унапред. Добављачи рачунара у облаку морају да обезбеде квалитет услуга. На пример, сигурност купаца у раду услуга и поузданост услуга.

5.2 Cloud рачунарство у развоју и тестирању

Економске неповољности могу изазвати нове пословне препреке ка успеху већу конкуренцију на тржишту итд. Да би се решили ови изазови, предузећа морају да оптимизују и унапреде своје пословање. У данашњем добу нудећи само лако доступне услужне софтвере може се остварити контакт са крајњим корисницима, предузећа могу неповољну ситуацију претворити у могућности и промовисати бољи развој.

Године развоја IT-а уско су повезале IT са пословним системима и системима рада и одржавања предузећа. У великој мери је оптимизација и ажурирање пословања заиста оно што се односи на IT систем, који захтева од предузећа да наставе да унапређују ствари у пословном систему. Као резултат тога, како се брзо развијају нови IT системи, радећи ригорозне тестове за пружање стабилних и поузданих услуга јер су купци постали кључ за развој предузећа. Стога су развојни центри за испитивање постали покретачи раста предузећа, а ефикасан начин пословања постала је главна брига компанија.

Како значај развојних центара у компанијама расте, у тим центрима ће бити све више пројеката, опреме и особља. Инжењери раде на томе како доћи до најуспешнијег начина успостављања паметног развојног центра. Као најновије достигнуће у IT-у, како ће рачунарство у облаку помоћи у трансформисању развојних тест центара и како рачунарство у облаку доноси конкурентску предност предузећима? Овај проблем се може илустровати кроз следећи случај:

Директор А је управник информативног центра и сада је задужен за све развојне пројекте. Од недавно се размишља о томе како најбоље оптимизовати своје окружење за развој и тестирање. Након истраживања, се закључује да су захтеви новог тестног центра следећи [24]:

- Смањење улагања у хардвер
- Брзо обезбеђивање окружења за нове пројекте развојних испитивања
- Поновна употреба опреме
- Осигуравање пројектне информационе сигурности

1. Смањење трошкова

У традиционалним системима за развој тестова, компаније би поставиле окружење за сваки пројекат испитивања и развоја. Различити системи за тестирање могу имати различите функције, перформансе или стабилност, па ће се конфигурације софтвера и хардвера у складу с тим разликовати. Међутим, у платформи за развој тестова у облаку, свим серверима, меморијама и мрежама потребним за развој теста управља се удруживањем како би се учинак довео до свог максимума. Кроз технологију виртуелизације сваки тест или развојни пројекат добија логичку хардверску платформу.

Виртуелне хардверске платформе више пројеката, могу да деле исти скуп хардверских ресурса, па ће се интеграцијом пројекта развојног теста улагање у хардвер знатно смањити.

2. Обезбеђивање окружења за нове пројекте

Облак може крајњим корисницима аутоматски да пружи IT ресурсе, који укључују рачунарске ресурсе, платформе оперативног система и апликативни софтвер. Све се то реализује путем аутоматизованог модула облака. Аутоматизација рачунарских ресурса - у интерфејсу услуге облака, када крајњи корисници уносе рачунске ресурсе (процесор, складиште и меморију) потребне у складу са захтевима апликативног система, cloud платформа ће динамички одабрати ресурсе у одговарајућем спремишту ресурса и припремити се за инсталацију системске платформе.

Аутоматизација системских платформи - када је додела рачунарских ресурса завршена, аутоматизација системских платформи помоћи ће да се динамички и аутоматски инсталира систем са рачунарским ресурсима на бази изабране системске платформе (Windows, Linux, AIX, итд.). Може се истовремено инсталирати оперативни систем платформе за све рачунаре којима је потребно и прилагодите оперативни систем са параметрима за прилагођавање и системску услугу за купце. Штавише, корисници, мреже и системи могу се аутоматски подесити. Аутоматизација апликативног софтвера - софтвер предузећа би био у потпуности контролисан. Модул за дистрибуцију софтвера може помоћи да се брзо и ефикасно распореде сложене критичне апликације са једног централног места на више места.

Кроз аутоматизацију облака може се пружити окружење за нове пројекте развојних тестова и убрзати процес развојних тестова.

3. Поновна употреба опреме

Облак је обезбедио процес управљања ресурсима заснован на тесту животних циклуса развоја. Процес покрива многе операције као што су успостављање, модификација, пуштање и резервација рачунарских ресурса. Када се развојни пројекти тестова обуставе или заврше, cloud платформа може направити резервну копију постојећег тестног окружења и ослободити рачунарске ресурсе, реализујући на тај начин поновну употребу рачунарских ресурса.

4. Обезбеђивање пројектне информационе сигурности

Платформа за рачунарство у облаку пружила је савршена средства за осигурање безбедности и изолације сваког пројекта. Постоје два начина да корисници приступе систему: приступ интерфејсу за управљање вебом или приступ виртуелној машини

пројекта. Да би се приступило веб интерфејсу, потребан је кориснички ID и лозинка. За контролу приступа виртуелној машини могу се усвојити следеће методе:

- Аутентификација корисника се врши путем Vlan ((Virtual LAN - бежична локална рачунарска мрежа) опреме у спољном интерфејсу система.
- Сваки пројекат има један једини Vlan, а виртуелна машина сваког пројекта налази се унутар Vlan-а. Прекидачи и хипервизори у хостовима могу гарантовати изолацију Vlan-а.
- Изолацију виртуелне машине гарантује сам виртуелни софтвер.
- Поред тога, аутентификација корисника оперативних система такође може заштитити корисничке информације.

Vlan се креира динамички заједно са успостављањем пројекта. Једностране или емитоване поруке могу се слати између пројекта виртуелних машина или између виртуелне машине и радне станице чланова пројекта. Виртуелне машине различитих пројеката су међусобно изоловане, што гарантује сигурност пројектних података. Корисник се може укључити у неколико пројеката и у међувремену посетити неколико виртуелних машина различитих пројеката.

Новој генерацији интелигентних развојних тест платформи потребна је подршка интелигентних IT инфраструктурних платформи. Успостављањем интелигентних развојних тест платформи путем рачунарства у облаку може се формирати нови начин снабдевања IT ресурсима. У овом режиму, центар за развој теста може аутоматски да управља и динамички дистрибуира, примењује, конфигурише, реконфигурише и рециклира IT ресурсе на основу захтева различитих пројеката. Осим тога, такође може аутоматски инсталирати софтвер и апликативне системе. Када се пројекти заврше, центар за развој теста може аутоматски рециклирати ресурсе, чиме на најбољи начин користи рачунарске могућности.

5.3 Виртуелизација

Виртуелизација се јавља када се креира виртуелна верзија нечега уместо стварне верзије за обављање конкретног посла. Комбинација хардверског и софтверског инжењеринга која креира виртуелне машине VM (Virtual Mashine у даљем тексту VM) и омогућава рад више оперативних система на истој платформи. На пољу информационих технологија, основна промена која се дешава свуда је очигледно пораст примене рачунарства у облаку. Виртуелизација у рачунарству је стварање виртуелног (а не стварног) нечега као што је хардвер, софтвер, платформа, оперативни систем, складиште или мрежни уређај У виртуелизованом окружењу IT предузеће мора усвојити и управљати многим променама. Због виртуелизације облаци су прилагодљиви и лако променљиви.

Виртуелизација се такође може дефинисати као технологија која има могућност логичког одвајања физичких ресурса сервера и њихове употребе као различитих изолованих машина, званих виртуелним машинама. Појединачни процесор постаје много виртуелних процесора, а рам меморија постаје вишеструка виртуелна рам меморија, а то исто важи и за хард дискове.

Виртуелизација је техника која омогућава стварање апстрактног слоја системских ресурса и скрива сложеност хардверског и софтверског радног окружења. Виртуелизација побољшава хардверску независност, изолацију гостујућег оперативног система и енкапсулацију читаве виртуелне машине груписане у једну датотеку. Виртуелизација се обично примењује са технологијом hypervisor, софтвер или елементи firmwar-а који могу виртуелизовати системске ресурсе. Hypervisor (или монитор виртуелне машине, VMM, виртуализатор) је рачунарски софтвер, firmware или hardware који креира и покреће

виртуелне машине. У рачунарству, firmware је посебна класа рачунарског софтвера који пружа контролу на ниском нивоу за одређени hardware уређај [24].

5.3.1 Виртуелизација предности и мане

Предности преласка на виртуелно окружење су бројне, штеди се новац и време, истовремено пружајући много већи континуитет пословања и способност опоравка. Следеће предности могу бити укључене у виртуализацију :

- Исплативост
- Смањује оптерећење
- Нуди боље време рада
- Омогућава брже распоређивање ресурса
- Промовише дигитално предузетништво
- Боља решења за опоравак
- Ефикасна и економична употреба енергије.

Мане виртуелизације су :

- Може имати високе трошкове имплементације
- Захтевају моћне машине
- И даље има ограничења
- Ствара сигурносни ризик
- Ствара проблем доступности
- Ствара проблем скалабилности
- Потребно је неколико карика у ланцу који морају кохезивно да раде заједно
- Потребно је време имплементације у систем

Предности и недостаци дају нам до знања да виртуелизација може бити корисно средство за : појединце, предузетнике, мале start-up предузећа и корпорације када се правилно користи. Иако је релативно једноставан за употребу, понекад администратори почну да додају нове сервере или складиште и могу створити проблеме. Оно што је додатна предност код оваквог вида проблема што се све може обавити на мрежи врло брзо, некад изузимајући физички контакт са компонентама [1].

5.4 Кластери високих перформанси засновани на облаку

У историји развоја информационих наука у последњих пола века, High Performance Computing (HPC) је увек била водећа технологија у то време. HPC је постао главно средство за будуће иновације како теоријске тако и истраживачке науке. Како се појављују нове научне дисциплине које повезују традиционалне области и HPC тако настају cloud софтвери високих перформанси рачунарске хемије, рачунске физике и биоинформатике. Рачунарска

технологија такође треба да направи искорак како би удовољила захтевима ових нових истраживачких тема.

Једно од питања је како обезбедити веће рачунарске перформансе са мање ресурса. То се поставља као велики изазов за HPC центре. У изградњи нове генерације рачунарског центра са високим перформансама, не треба се обраћати пажња само на избор софтвера и хардвера, већ узети у обзир у потпуности рад центра. Мисли се на : ефикасност коришћења и сарадњи у технолошким иновацијама и другим факторима. Такође би требало у потпуности размотрити рационалност општег оквира и ефикасност управљања ресурсима. Радећи на томе, центар може добити дугорочне капацитете високих перформанси у рачунарском истраживању и снабдевању. Другим речима, нова генерација рачунарских центара високих перформанси не пружа само традиционално рачунање високих перформанси, нити је само решење опреме високих перформанси. Такође би требало узети у обзир : управљање ресурсима, кориснике, виртуелизацију, динамичко стварање и рециклирање ресурса. На тај начин рађа се рачунање високих перформанси засновано на технологији рачунарства у облаку.

Циљ рачунарског центра заснованог на рачунарству у облаку је да реши следеће проблеме:

- Рачунска платформа високих перформанси која се генерише динамички
- Виртуелизовани рачунарски ресурси
- Технологија рачунарског управљања високих перформанси у комбинацији са традицијоналним управљањем

У традиционалном рачунарском окружењу високих перформанси, физичка опрема је конфигурисана да задовољи захтеве купаца; на пример, Beowulf Linux и WCCS архитектура (Windows Compute Cluster Server) изабрани су да задовоље захтеве купаца у погледу рачунарских ресурса. Сви оперативни системи и паралелно окружење су унапред подешени, а софтвер за управљање кластерима користи се за управљање рачунарским окружењем. Међутим, како се рачунарство високих перформанси развија, све је више крајњих корисника и апликативног софтвера, па тако захтеви на рачунарској платформи постају разноврснији. Различити крајњи корисници и апликативни софтвер могу захтевати другачије оперативне системе и паралелно окружење. Рачунарство високих перформанси захтева нови начин снабдевања ресурсима, у којем би платформа требало да се генерише динамички у складу са потребама сваког крајњег корисника и апликативног софтвера; платформа може бити отворена, укључујући Linux, Windows or UNIX [1].

Виртуелизовани рачунарски ресурси :

Будући да се у традиционалном рачунарству високих перформанси користи мало виртуелизоване архитектуре, оваква платформа не може управљати виртуелизованим ресурсима. Међутим, како се рачунарство високих перформанси развија, у многим случајевима мора да се постигне више виртуелизованих ресурса путем виртуелизације, на пример, развој и отклањање грешака паралелног софтвера и подршка за више корисничких апликација итд.

У рачунарском центру високих перформанси заснованом на рачунарству у облаку, виртуелизација физичких ресурса може се реализовати путем платформе cloud, штавише, виртуелизовани ресурси се могу користити за успостављање рачунарске платформе високих перформанси и генерисање рачунарског окружења високих перформанси чији је обим већи од стварног физичког ресурса како би се задовољили захтеви купаца.

Комбинација са традиционалном технологијом управљања :

Платформа високих перформанси заснована на рачунарству у облаку може не само да управља рачунарима путем технологије виртуелизације и динамичке генерације, већ и да ради заједно са традиционалним софтвером за управљање кластерима и операцијама у омогућавању корисницима да традиционалним начином управљања виртуелизованим рачунарима високих перформанси предају свој рад.

Нови модел пружања IT ресурса може се постићи усвајањем инфраструктуре рачунарског облака и изградњом рачунарских центара високих перформанси. У овом моделу, рачунски центар може аутоматски управљати и динамички дистрибуирати, примењивати, конфигурисати, реконфигурисати и рециклирати ресурсе. Може се реализовати и аутоматска инсталација софтвера и апликација.

Коришћењем модела, рачунарски ресурси високих перформанси могу се дистрибуирати ефикасно и динамично. Када је пројекат завршен, рачунски центар може аутоматски рециклирати ресурсе како би у потпуности искористио рачунарску снагу. Користећи предност рачунарства у облаку, рачунарски центар високих перформанси може не само да пружи високу рачунску снагу научноистраживачким институцијама, већ и да прошири услужни садржај рачунарског центра. Другим речима, може послужити као центар података за подршку другим апликацијама и промовисање веће ефикасности коришћења целокупних ресурса [1].

6 Безбедност апликација у облаку

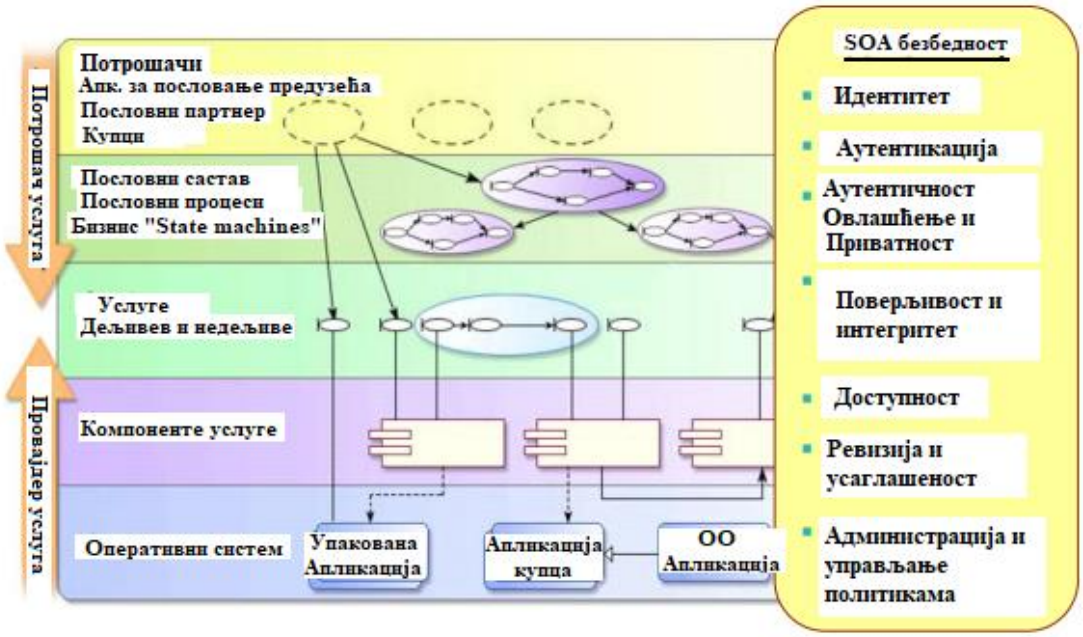
Сигурносна подручја која се морају решити у SOA (Service oriented arhitecture) окружењу не мењају се од оних која су обрађена већ приликом архитектуре других IT система. Једна кључна разлика је ипак у томе што, пошто су IT системи чвршће усклађени са пословним процесима у SOA окружењу, безбедносне праксе морају бити прилагођене да буду усклађене и са пословним процесима. Због ове усклађености сигурносне политике морају се суочити са новим изазовима. Друга кључна разлика је због лабавог спајања услуга и апликација и њиховог могућег рада преко граница поверења. SOA је заправо архитектура IS која првенствено пружа коришћење лабаво повезаних сервиса и добијање флексибилности и проширивост на начин који није зависан од технологије.

Очекује се да ће услужно оријентисана архитектура (SOA) пружити конкретне користи организацијама повећањем брзине примене апликација и смањењем трошкова за интеграционе технологије [1], попут уштеде трошкова. Међутим, безбедност је једна од главних препрека примене SOA у организацијама [2]. Рачунарски системи, а посебно дистрибуирани системи, суочавају се са неколико сигурносних ризика који такође утичу на SOA.

У овом одељку уводимо неке безбедносне претње са којима се суочавају рачунарски системи и безбедностне стандарде.

6.1 SOA безбедност и сигурносни стандарди

Да би се започела дискусија о примени сигурности у SOA-е најпре се треба упознати са појмовима безбедности у SOA. На слици 8 је приказана структура и слојеви безбедности као и седам основних појмова безбедности услужно орјентисане архитектуре [16].



Слика 8 Дефинисање безбедностне терминологије у SOA [16]

1. Идентитет

Генерално, идентитет је својство објекта које омогућава разликовање од других објеката. У нашем контексту предметни објекат је корисник или потрошач. Идентитет ових потрошача обично је представљен јединственом вредношћу или идентификатором, као што је корисничко име или UUID. У SOA окружењу постоји много врста потрошача,

укључујући добављаче, партнере, интерно особље и апликације. Сваки од ових потрошача мора бити исправно идентификовани у свим фазама SOA окружења [16].

2. Аутентикација

Тврдња о идентитету је често недовољна да би нам омогућила да верујемо да потрошач заиста има идентитет који тврди. За доказивање ове тврдње користи се поступак потврде идентитета. Аутентификација је поступак доказивања да потрошач легитимно има свој идентитет за који се тврди давањем додатних података (акредитиви за аутентификацију) који су везани за овај идентитет и које може пружити само потрошач са тим идентитетом. Типичан пример ове врсте додатних информација је лозинка [16].

3. Овлашћење и приватност

Овлашћење је поступак процене да ли се ауторизованом идентитету може испунити захтев. Одлуке о ауторизацији могу се разликовати у зависности од врсте корисника који извршава захтев за приступ. На пример, истој услузи може приступити интерно особље организације, али не и партнери из различитих организација. Интерном члану особља је дозвољен приступ услузи (они су овлашћени), док партнеру није дозвољен приступ (они нису овлашћени).

Приватност је посебан случај ауторизације, где се контролише приступ личним подацима (PPI – Personally Identifiable Information). Ова врста ауторизације се обично заснива на подацима који се преузимају. На пример, можда је прихватљиво приступити кућној адреси купца, али не и његовом кућном телефону [16].

4. Поверљивост и интегритет

Заштита података у стању мировања, у транзиту и у процесу су важна разматрања. Заштита поверљивости обично подразумева шифровање података тако да их неовлашћене особе не могу прочитати. Само неко ко поседује кључ за дешифровање може да прочита податке.

Интегритет значи заштиту од неоткривених модификација података. То се обично постиже коришћењем дигиталних потписа или кодова за потврду идентитета порука. Потписивање података у облику захтева или поруке пружа облик потврде идентитета, односно потврду идентитета поруке. Предлагач захтева ће потписати поруку, доказујући да разуме садржај захтева (на основу шифровања поруке својим јединственим приватним кључем за потписивање) и пружајући заштиту од модификација захтева (на основу немогућности валидације потпис против измењене поруке) [16].

На пример, стандардни WS-Security, може се користити за заштиту порука веб услуга. Пружа поверљивост порука, интегритет и потврду идентитета. Сигурносни подаци, као што су лозинке, кључеви за шифровање, конфигурационе датотеке и подаци апликација који се чувају у базама података или на сличним местима, такође могу бити заштићени уз механизме поверљивости и интегритета [16].

5. Доступност

Доступност услуге или ресурса подразумева да је у стању да благовремено одговори на захтев. Осигуравање доступности услуга када је потребно кључно је у многим SOA окружењима. Архитектура за високу доступност укључује груписање апликација, кластере база података и сличне технике.

6. Ревизија и усаглашеност

Обавеза да се догађаји у вези са безбедношћу бележе, затим анализирају и извештавају је домен ревизије. Ревизија се често примењује у појединачним постојећим системима, па спајање тих података може бити кључни захтев. Провера да ли су безбедносни догађаји у складу са интерном пословном политиком је домен усклађености. Усклађеност такође може значити осигуравање да систем следи законске захтеве [16].

7. Администрација и управљање политикама

Правила о аутентификацији, ауторизацији, заштити података, ревизији и друго су описана су у безбедносним полисама. Будући да се безбедносне политике могу развијати како би ишле у корак са променом пословних политика, администрација и управљање политикама морају бити флексибилни и лако подесиви. Додавање партнера или новог скупа услуга, примена наменских и подесивих безбедносних политика и њихово лагану, сигурну и ефикасну примену. Примену која је олакшана без потребе за поновним разматрањем целокупне архитектуре

6.2 Веб услуге и сигурност

Модел заштите веб услуга уводи скуп појединачних међусобно повезаних спецификација како би се формирао слојевити приступ безбедности. Постоје неколико стандарда који се примењују како би обезбедили сигурност веб услуга. XML (eXtensible Markup Language) представља стандард за дефинисање формата података у електронској форми. Стандард је прописала W3C (World Wide Web Consortium) међународна организација која се бави израдом стандарда на интернету.

Било је неколико покушаја да се између осталог обезбеде SOA безбедносни стандарди за потврду идентитета, поверљивост и интегритет. У наставку следе безбедностни стандарди прописани у служби сигурнности података на интернету и cloud апликацијама [16].

XML потпис — XML потпис је основна технологија за спецификацију WS-Security (Безбедност веб услуга) и за заштиту веб услуга уопште. Суштина је WS-Security, XML спецификације за управљање кључевима (XKMS - XML Key Management Specification) и других безбедносних стандарда веб услуга. Такође је користан за транспорт заједничких тајних кључева који су потребни за XKMS шифровање. XML потпис омогућава кодирање дигиталних потписа у XML. Синтакса XML потписа и обрада W3C (The World Wide Web Consortium – међународна заједница) дефинише синтаксу XML потписа и повезана правила обраде [16].

XML шифровање - Слично XML потпису, XML шифровање је направљено коришћењем технологије шифровања са заједничким кључем и представља препоруку W3C. Основни захтеви за XML шифровање су да мора бити у стању да шифрује XML поруку произвољне величине и то мора да ради ефикасно. Разлог зашто је XML шифровање потребно преко шифрирања на нивоу транспорта, као што је SSL, је тај што се мора чувати поверљивост поруке када порука на свом одредишту одскочи више пута. То ће бити уобичајено када се користе заједничке услуге. XML енкрипција такође чува поверљивост порука када се XML порука чува чак и након што стигне на крајње одредиште. XML шифровање примењује стандардне алгоритме на податке, а затим тај шифровани резултат чува у XML [23].

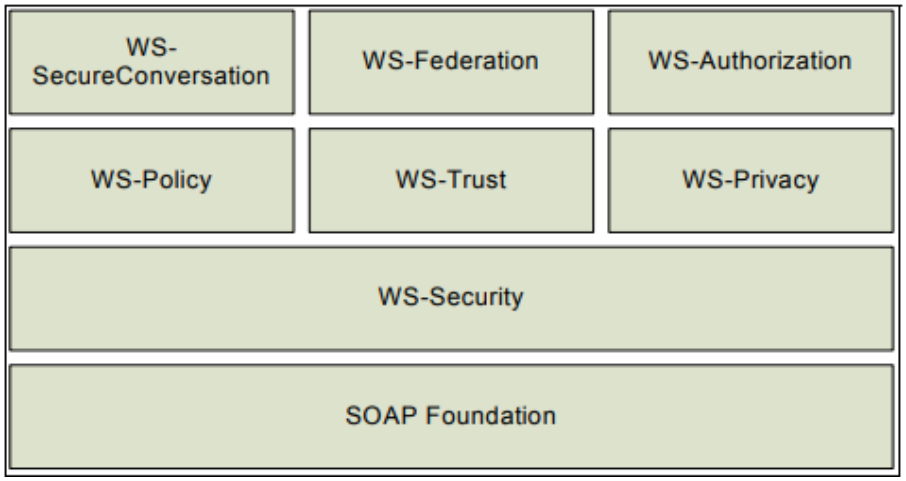
Спецификација управљања XML кључевима - XML Key Management Specification (XKMS) је спецификација изграђена на самом врху и допуњује XML стандарде за дигитални потпис и шифровање. Технологије XML потписа и XML шифрирања најбоље се скалирају када користе криптографију јавног кључа. Криптографија јавног кључа захтева подршку инфраструктуре Public Key Infrastructure (PKI) за управљање дистрибуцијом, сертификацијом и управљањем животним циклусом (на пример, опозивом) кључева. Сами веб сервиси пружају другачији приступ омогућавајући PKI приступ као услугу, стога нема потребе да сваки подносилац захтева и добављач веб услуга изради свој PKI. XKMS има за циљ управо то. Одређује протоколе за дистрибуцију и регистрацију јавних кључева погодних за употребу у вези са XML потписом и стандардима XML шифрирања [23].

SAML — Security Assertion Markup Language (SAML) који је предложио OASIS (Organization for the Advancement of Structured Information Standards) - организација за унапређење структурираних информационих стандарда, је сигурносна спецификација заснована на XML-у за размену информација о аутентификацији и ауторизацији корисника или субјекта. Дефинише XML шема и дефиниција за сигурносне тврдње. Постоје три врсте тврдњи : потврда идентитета, сви атрибути повезани са безбедношћу субјекта и одлуке о ауторизацији дате на основу атрибута безбедности и привилегија. SAML се такође може проширити тако да шаље било које произвољне сигурносне тврдње. То показује да се SAML првенствено користи за пренос атрибута безбедности и привилегија повезаних са предметом из једног ентитета у други ентитет у мрежи. Једини услов је да оба ентитета поштују SAML стандард [16].

6.3 WS-Security и сродни стандарди

У априлу 2002. године, IBM и Microsoft објавили су заједничку књигу под називом „Security in a Web Services World: A Proposed Architecture and Roadmap“ која се бави безбедношћу веб услуга у свету. У њој се налази и предложена архитектура која би имала сврху постизања циља у пружању услуга на интернету са максималном безбедношћу. Ова техничка књига описује скуп безбедносних стандарда и технологија који треба да створе обједињавајући приступ бављења сигурност у свету веб услуга. Баш као што WS-security омогућава безбедносним механизмима као што су инфраструктура јавног кључа (PKI) и SAML који учествују у заштити веб услуга. План архитектуре веб услуга уопштава многе сигурносне функције које су раније постојале у другим доменима и предлаже оквир за испуњавање безбедносних захтева домена веб услуга. Присталице овог оквира и тела за стандарде, постижу прво избацивањем темељних спецификација као што су WS-Security (која је, пак, изграђена на XML потпису, XML енкрипцији, SAML-у и другим стандардима сигурносних типова), а затим развијањем других стандарда који се ослањају на ове темељне стандарде [15].

Слика 9 илуструје ове спецификације и слојевити приступ развијање ових стандарда.



Слика 9 Спецификације безбедности веб услуга [15]

Уводимо неке од битних SOA безбедносних стандарда, спецификације са слике 8 пружају следеће могућности:

1. WS-Security - описује проширења SOAP (Simple Object Access Protocol) за сигурну размену порука. Спецификација WS-Security пружа сигурност на нивоу поруке. То је општи механизам за повезивање сигурносних токена са SOAP порукама. WS-Security се гради и у потпуности је компатибилан са успостављеним и безбедносним технологијама као што су SSL, IPSec13, XML Signature и XML Encryption. Дизајниран је за адресирање интегритета порука, поверљивости порука, аутентификације поруке и кодирања безбедносних токена који путују са заштићеним порукама. То значи да су поруке заштићен чак и ако порука пролази кроз више услуга или посредника [15].

2. WS-Policy - дефинише како да изрази могућности и ограничења безбедносне политике. WS-Policy омогућава организацијама које нуде веб услуге да одреде захтеве својих веб услуга за питања као што су приватност или безбедност. WS-Policy је спецификација на високом нивоу која пружа основне конструкције потребне за састављање одређеног језика политике (као што је WSSecurityPolicy) . Уско повезана са спецификацијом WS-Policy је WS-PolicyAssertions спецификација, која пружа неке основне тврдње о политици која би се односила на било коју врсту политике, која даје смернице о томе како приложите политику ресурсу. WS-PolicyAssertions је посебна врста смерница која користи WS-Policy оквир који одговара на одређене безбедносне захтеве и конфигурациона питања за веб услуга, као што су типови алгоритама шифровања који треба да буду подржани, параметри који се шифрују и типови безбедносних токена које треба навести [16].

3. WS-Trust - описује модел успостављања директних и посредничких односа поверења, укључујући посреднике. Поверенички језик веб услуга (WS-Trust) користи механизме сигурне размене порука WS-Security за дефинисање додатних основа и проширења за издавање, размену и проверу безбедносних токена. WS-Trust такође омогућава издавање и ширење акредитива у различитим доменима поверења. Да би осигурале комуникацију између две стране, две стране морају разменити поверљиве податке (било директно или индиректно). Међутим, свака странка треба да утврди да ли може да ’верује’ у потврђене акредитиве друге стране. Ова спецификација дефинише

проширења за WS-Security за издавање и размена сигурносних токена и начина успостављања и приступања присуству односа поверења. Користећи ове екстензије, апликације могу да се укључе у сигурну комуникацију дизајнирану за рад са општом архитектуром веб услуга [23].

4. **WS-Privacy** - Ова спецификација ће омогућити корисницима да наведу преференције приватности, а веб услуге да наведу и примене праксе приватности. Пројекат платформа за преференције приватности (P3P - Platform for Privacy Preferences) дефинише протокол који омогућава веб локацијама да одреде како намеравају да користе приватне информације корисника. Протокол омогућава корисницима да донесу одлуку у погледу приватности, да ли да користите веб страницу или не [16].

5. **WS-SecureConversation** - описује како се управља и потврђује идентитетом размене порука између страна, укључујући размену безбедносних контекста и успостављање и извођење кључева сесије. Језик за безбедну конверзацију веб услуга (WS-SecureConversation) изграђен је на врху модела WS-Security и WS-Policy како би се обезбедила сигурна комуникација између веб услуга [16].

6. **WS-Federation** - Описује како управљати и посредовати у односима поверења у хетерогеном федералном окружењу, укључујући подршку за федеративне идентитете. Спецификација федерације веб услуга дефинише механизме који омогућавају удруживање различитих безбедносних подручја омогућавањем и посредовањем поверења идентитета, атрибута и потврде идентитета између веб услуга које учествују. Механизме дефинисане у спецификацији могу користити и пасивни и активни подносиоци захтева. Претпоставља се да корисници веб услуга разумеју нове безбедносне механизме и могу да комуницирају са добављачима веб услуга [15].

7. **WS-Authorisation** - Ова спецификација ће дефинисати како се управља подацима и политикама ауторизације веб услуга. Предложено је неколико модела веб ауторизације [15].

7. Безбедност Базе података у облаку

База података се може описати као скуп међусобно повезаних података, који су ускладиштени у меморији рачунара. Подаци који се налазе у бази података могу бити доступни корисницима, а да би било могуће остваривање сврхе cloud апликације подаци су доступни и програмима. На тај начин се врши управљање над базом података. Управљање базом података се своди на убацивање, брисање, промене и читање података. Заправо апликације које користе податке из базе као и корисници не морају знати физички приказ података, већ се референцирају на логичку структуру базе. Остваривање повезаности базе података и програма или корисника остварује се помоћу система за управљање базом података (Database Managament System – DBMS). Пошто корисницима није позната физичка структура података у бази, DBMS обликује физички приказ у захтевану логичку структуру. DBMS је способан да управља са више база, које се могу разликовати према својој структури али морају припадати истом моделу. DBMS је задужен за административне послове са базом као и за безбедност података.

Да би се успешно пројектовала база података мора се знати модел базе који ће се примењивати у супротном имплементација се неће моћи извршити. Системи за управљање базом података подржавају најпознатије моделе а то су :

- Релациони модел - Релациони модел (RM) за управљање базама података је приступ управљању подацима користећи структуру и језик у складу са логиком, коју је први пут описао 1969. године енглески информатичар Едгар Ф. Код (Edgar F. Codd), где су сви подаци груписаних у скуп релација између којих се дефинише веза. У релационој бази података примарни кључеви играју значајну улогу. Они представљају атрибут помоћу кога се индентификује n-торка из скупа. Повезаност релација се остварује помоћу спољног кључа.

- Мрежни модел - Мрежни модел је модел базе података замишљен као флексибилан начин представљања објеката и њихових односа. Његова препознатљива карактеристика је та је што шема посматрана као граф у којем су типови објеката чворови. Мрежни модел није ограничен као хијерархијски модел.

- Хијерархијски модел - Хијерархијски модел базе података је модел података у којем су подаци организовани у структуру налик стаблу. Подаци се чувају као записи који су међусобно повезани преко веза. Запис је колекција поља, при чему свако поље садржи само једну вредност. Тип записа дефинише која поља садрже запис.

- Објектни модел – Заснован на идеји програмских језика у чијој су основи објекти и њихова повезаност. Објектни модел базе података се састоји од објеката које сачињавају интерни подаци и методе које их карактеришу [23].

7.1 Безбедносни компромис између сервисних модела

Сваки модел услуге у оквиру SPI (SaaS, PaaS, IaaS) разликује се међусобно у погледу карактеристика и безбедносних захтева.

SaaS модел пружа највише уграђених функција сигурности и обећава висок ниво безбедности, али потрошачима нуди најмању проширивост.

PaaS пружа потрошачима већу проширивост за разлику од SaaS-a, јер омогућава програмерима да граде апликације на врху платформе. Међутим, ово резултира мање

интегрисаним сигурносним функцијама, али потрошачи имају могућности да додају додатну сигурност ако је потребно.

IaaS пружа највећу проширивост за потрошаче. То заузврат резултира мање интегрисаних сигурносних карактеристика и функција, осим заштите саме инфраструктуре. Овај модел услуге захтева да потрошачи у облаку управљају и штите систем оперативним системима, апликацијама и садржајем [18].

Као што се може видети из горе наведених карактеристика и стандардних функција безбедности међу системима, тренд је да се сва одговорност пребаци на потрошаче рачунарства у облаку. Другим речима подаци и апликације у облаку све више захтевају сопствену безбедност док је добављач ту само да обезбеди сигурни рад и складиштење. То значи да потрошачи, на пример, имају већу одговорност за управљање и безбедност услуга ако користе IaaS него ли моделе PaaS или SaaS. На слици 10 су приказане одговорности међу појединим моделима :

Слика 10 Безбедносни компромис између сервисних модела [17]

Један од важнијих алата који је доступан потрошачима у вези са управљачким и безбедносним одговорностима је споразум о нивоу услуге (SLA - Service-Level Agreement). SLA је документ који уговором одређује нивое услуга, сигурност и доступност које потрошачи могу очекивати од добављача. Уговор о нивоу услуге (SLA) представља обавезу између добављача услуга и клијента. Посебно se односи на доступност, квалитет, одговорности. У одсуству SLA, потрошачи би сами били одговорни за многе административне и управљачке задатке. Стога је присуство SLA о којем се може преговарати веома важно када је реч о избору добављача услуга у облаку [17].

7.2 Услуге базе података у облаку

Због велике потражње, добављачи облака сада нуде и нову услугу поред традиционалних услуга (SaaS, PaaS, IaaS) познату као база података као услуга или DbaaS (database as a service) која је у основи база података на захтев доступна потрошачима рачунарства у облаку.

Преношење услуга базе података у облак постало је важан део технологије рачунарства у облаку у новије време. У протеклој деценији, због брзог напретка у мрежној

технологији, трошкови и кашњење преноса великих делова података на велике удаљености знатно су се смањили [14].

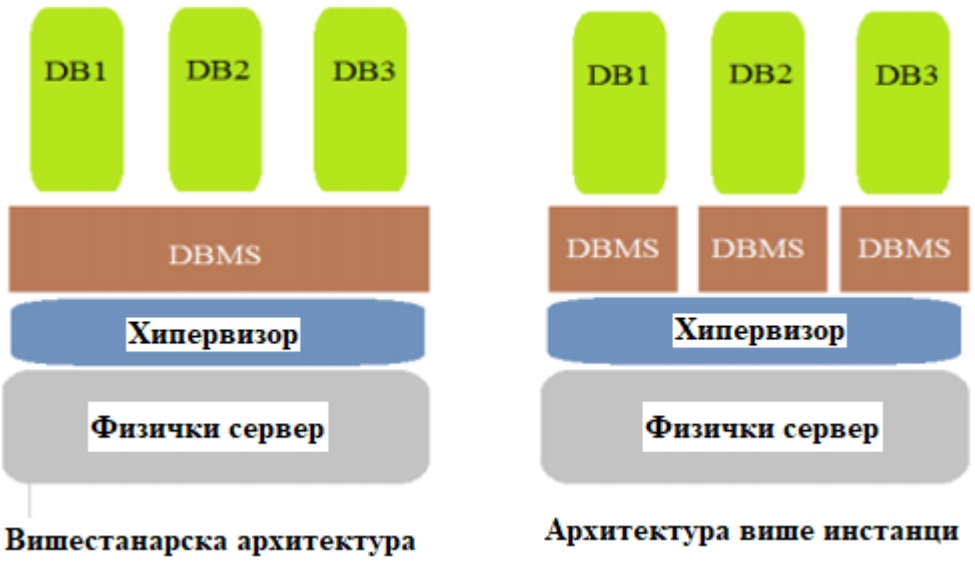
У међувремену се сматра да су оперативни трошкови и трошкови управљања одржавањем база података неколико пута већи од почетних трошкова прибављања. Штавише, због употребе мултимедијалног садржаја, величина данашњих база података експоненцијално расте и достиже више терабајта. Такве базе података захтевају аутоматско скалирање у покрету уз што мање интеракције са корисником. Технологија рачунарства у облаку нуди ова решења дељењем података из великих база података и њиховим ширењем на стотине сервера за паралелну обраду. Као резултат тога, све више организација показује спремност у преношењу задатака управљања базама података добављачима у облаку за много ниже трошкове.

У основи постоје два главна приступа постављању база података у облаку:

- „Уради сам“ - У овом приступу потрошач купује IaaS услуге од добављача облака по свом избору и инсталира сопствену инстанцу базе података на пружену платформу. Све одговорности за одржавање, управљање и измена инстанци базе података биће на купцу. Међутим, нуди предности инсталирања додатних алата за надзор и ревизију заједно са инстанцом базе података на виртуелној платформи.

- Претплата на пуноправну базу података као услуга (DBaaS) - За разлику од горе наведеног, у овом приступу потрошачи добијају прилику да читав пакет база података купе као услугу од добављача. Све одговорности за управљање и одржавање биће на добављачу, а једино што би потрошач морао да уради је да своје апликације повеже са базама података и наплаћиваће се на основу употребе. Овај приступ је много погоднији за потрошаче, али недостатак је тај што добављачи често не подржавају инсталирање додатних алата заједно са базама података у облаку на својим платформама. То га чини мање сигурним јер се од потрошача очекује да верују у алате за праћење и ревизију добављача.

DBaaS окружења доступна у облаку могу се значајно разликовати. Неки добављачи нуде модел вишеструких инстанци, док други подржавају модел више-станарства. У моделу са више инстанци сваки потрошач има јединствени DBMS који ради на наменској виртуелној машини која припада само одређеном купцу. Ова функција омогућава потрошачима да имају бољу контролу над административним и другим безбедносним задацима као што су дефинисање улога и ауторизација корисника. С друге стране, модел више станара користи метод означавања и пружа унапред дефинисано окружење базе података које деле многи станари. У овом моделу подаци за сваког станара означени су идентификаторима који су јединствени за сваког од њих. Одговорности за одржавање и успостављање сигурног окружења базе података ослањају се искључиво на добављача облака. Модел више инстанци се користи више од модела са више станара, јер даје одређене безбедносне функције, попут шифровања података, лакше применити у моделу са више инстанци него у моделу са више станара.



Слика 11 Модел више-станара и модел више-инстанци [20]

На почетку треба раздвојити неке ствари и превазићи заблуде. Многи верују да ће употребом DBaaS бити елиминисана потреба за администраторима база података. За разлику од веровања, и даље ће бити потребан већи део посла DBA(Database administrator-a), попут модификације шема база података, подешавања упита, размештања података и праћења активности базе података. Део посла који се пребацује са DBA ка добављачима база података у облаку повезан је са физичком имплементацијом база података. Са базе података у облаку, DBA више не би требало да брину о стварима попут алокације датотека, управљања меморијом и конфигурације доступности [12].

7.3 Предности услуга базе података у облаку

У новије време све је више предузећа која су постепено почела да усвајају услуге база података у облаку због предности које пружа. Неке од предности преласка на услуге базе података у облаку су следеће :

- Приступачност: Као и друге услуге рачунарства у облаку, један од разлога због којих организације размишљају о преласку на услуге база података у облаку је због њихове ефикасности. Услуге базе података у облаку у великој мери смањују оперативне трошкове и трошкове одржавања, а потрошачима наплаћују само коришћење.

- Флексибилност и скалабилност: Данас базе података могу брзо да расту у величини због прекомерне употребе формата мултимедијалних података и потребна су нова скалабилна решења која нуде услуге база података у облаку. Користећи базе података у облаку, потрошачи могу повећати или смањити своје услуге како би удовољили променљивим потребама свог пословања често без људске интеракције.

- Повећана ефикасност путем мобилности: Са базама података које бораве у облаку, администратори би могли да приступе бази података са било ког места помоћу рачунара, мобилног уређаја или прегледача. Истовремено, све више апликација може да се повеже на исту базу података без икаквих промена конфигурације у базама података у облаку.

Упркос горе поменутим предностима, многе организације нерадо усвајају базе података у облаку због сигурносних разлога. Неки од безбедносних изазова са којима се суочавају услуге база података у облаку истражени су у следећем одељку.

7.4 Задатак Безбедности

Смештање база података у облаку доноси бројне сигурносне проблеме које организације морају узети у обзир, пошто је крајња одговорност за сигурност базе података препуштена корисницима базе у облаку, а не добављачима. Када се интерне базе података са осетљивим подацима смештају у облак, корисници морају бити уверени да су успостављена одговарајућа мерења безбедности базе података које обухватају поверљивост података, интегритет и доступност.

Главни аспекти сигурности базе података у облаку су да подаци морају бити заштићени док мирују, док су у транзиту и у употреби, а приступ подацима мора бити контролисан. Што ће рећи [19] :

- Да би се осигурало да подаци не буду оштећени или противправно присвојени, веома је важно да постоје сигурни поступци који би заштитили пренос података из база података која се налазе у облаку.
- Да би се обезбедила висока поверљивост, важно је да се подаци који се чувају у базама података у облаку увек криптирају. Криптирање представља конверзију постојећег податка који је читљив у нечитљив текст који је разумљив једино онима који имају кључ.
- Да би се осигурао висок интегритет, приступ ускладиштеним подацима на платформи добављача базе података у облаку, мора се правилно контролисати и надгледати за све кориснике, укључујући администраторе базе података у дата центру.

Данас су доступни стандардни протоколи и процедуре комуникационе безбедности (HTTPS, SSH, сертификати јавних кључева итд.) које се могу користити за заштиту података у покрету. HTTPS (енгл. Hypertext Transfer Protocol Secure) је комбинација Hypertext Transfer Protocol-a са SSL/TSL протоколом. Користи се за сигурну и безбедну индентификацију сервера. Међутим, стандарди за заштиту података који се налазе у дата центрима добављача услуга у облаку тек треба да постану примењени. Главни сигурносни изазови са којима се суочавају услуге базе података у облаку и предложена решења размотрени су у следећим одељцима почев од доступности.

7.4.1 Доступност

Доступност једноставно значи у којој мери су ресурси система доступни и употребљиви за појединачне кориснике или организације. То је један од критичних аспеката безбедности који организације морају узети у обзир приликом разматрања услуга база података у облаку. Након неуспеха, на доступност се може утицати привремено или трајно, а губитак може бити делимичан или комплетан. Постоје многе претње по доступност које укључују DoS нападе (denial-of-service attack), кварове опреме и природне катастрофе. Често је већина застоја непланирана што може имати озбиљне последице на свакодневне рутине организација. Иако све базе података не захтевају стопостотну доступност, али одређене апликације могу много да трпе ако базе података постану недоступне у непознатом временском периоду.

Услуге рачунарства у облаку, упркос томе што имају инфраструктуру дизајнирану да обезбеди високу доступност и поузданост, трпе због непланираних прекида. Бројни примери илуструју ову поенту. У фебруару 2008. године, популарна услуга у облаку за складиштење и преузимање било које количине података, у било које време, са било ког места на мрежи (Amazon S3) претрпела је прекид рада од три сата што је утицало на њене потрошаче, укључујући Twitter и друге startup компаније. Стога, када се добављачу обраћају за расположивост базе података, потрошачи би увек требало да захтевају стандард високе доступности познат као „Five Nines“ где је застој краћи од 5,26 минута годишње. То је једнако раду од 99,999%, што је попут прекида од око пет минута годишње. Ниво расположивости услуге базе података у облаку, опције за прављење резервних копија података и механизми опоравка од катастрофе треба правилно размотрити у оквиру организације пре разматрања потеза смештања података у облак.

7.4.2 Проблеми са контролом приступа у јавном облаку

Једна од главних безбедносних претњи присутних за базе података у облаку је губитак контроле приступа. Када организације препусте осетљиве податке добављачима у облаку, оне губе физичку, логичку и кадровску контролу над њима, што са собом носи уграђени безбедносни ризик. Иако су спољне претње сигурно велика брига, али недавне студије показују да већина претњи контролом приступа потиче не само од интерних запослених у организацијама, већ и од запослених у добављачима услуга у облаку.

Стога су правилне процедуре за контролу приступа и надгледање за администраторе база података у облаку веома битне како би се осигурала сигурност осетљивих података.

7.4.3 Питања ревизије и праћења

Иако се еластичност и флексибилност сматрају главним предностима рачунарства у облаку, али са собом носе својствен сигурносни проблем. Да би задовољили потребе потрошача, базе података у облаку често се повећавају или смањују, што значи да се физички сервери који хостују базе података често припремају и уклањају без претходног знања потрошача.

Штавише, да би се обезбедила велика доступност, подаци се обично копирају у неколико дата центара на више локација. Сви ови фактори резултирају нестатичним окружењем у којем потрошачи готово немају видљивост или приступачност физичкој инфраструктури.

7.4.4 Санитизација података

Следећи безбедносни ризик који је повезан са физичком сигурношћу је уклањање / брисање података са уређаја за складиштење познато као санитизација података. Санитизација укључује брисање података са медијума за складиштење преписивањем, исправљањем или уништавањем самог медија, како би се спречило неовлашћено откривање информација. У јавном окружењу у облаку, подаци различитих купаца се физички налазе заједно, што компликује поступке санитизације. Редовне резервне копије које пружа добављач услуга у облаку како би се осигурала велика редудантност додатно појачавају компликације.

Постоји много примера где су истраживачи успели да поврате велике количине осетљивих информација са половних дискова купљених на аукцијама на мрежи. Ако се подаци не избришу правилно, можда се могу опоравити па чак и критични подаци користећи одговарајућу опрему. Због тога је од изузетне важности да SLA треба да наведе да ли добављачи облака пружају довољна мерења како би се обезбедило да се санитизација података врши на одговарајући начин током животног циклуса система.

7.5 Надгледање дистрибуиране базе података

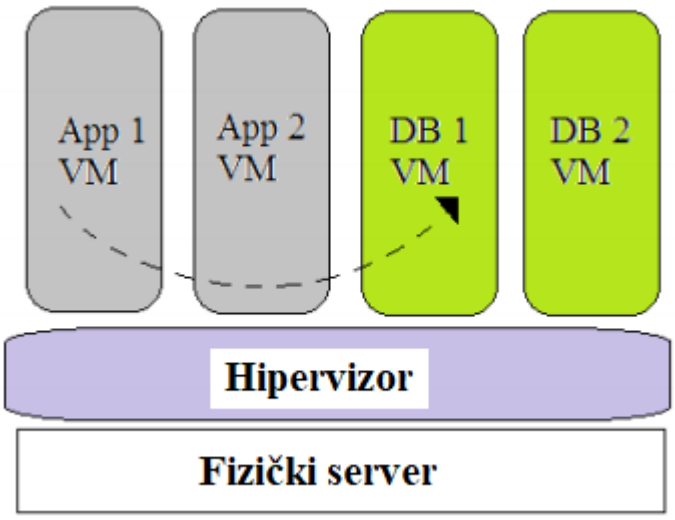
Надгледање или ревизија базе података у основи је способност сталног и сигурног снимања и извештавања о свим догађајима који се догађају у систему базе података. Ревидиране базе података генеришу извештаје о томе како, када и ко приступа различитим објектима или их мења. Снажан алат за ревизију и надзор базе података, који треба да пружи потпуну видљивост активности базе података, без обзира на његово место, изузетно је важан за услуге база података засноване на облаку.

Да би се суочили са изазовима заштите традиционално на базама података, локални стручњаци су у почетку усвојили мрежни IDS (intrusion detection system) и IPS - уређај који ће бити постављен негде у мрежи и који ће прегледати саобраћај због кршења протокола, злонамерног кода, вируса итд. Иако су предузећа у почетку игнорисала унутрашње ризике и претње, али убрзо се испоставило да унутрашње претње могу бити штетне и надгледање стога мора покривати и локалне и нападе унутар базе података [20].

Усвајање локалних агената (софтвера) се користи за праћење активности извршених на серверу базе података, што обично укључује активности администратора базе података. Ови системи могу пружити свеобухватан траг ревизије базе података поред механизма за откривање упада могу садржати и системе за прекидање сесија корисника или изоловати корисника који крши или злоупотребљава политику унутар заједнице. У овом решењу, агенти домаћини шаљу локални саобраћај натраг мрежном уређају на анализу, где се свака трансакција мери према унапред постављеној политици. Иако овај хибридни приступ није идеалан (неефикасан за локално кршење безбедносних политика), али многа предузећа и даље усвојили као безбедносно решење.

У случају база података заснованих на облаку, модел „Sniffing Network“ (Њушкање на мрежи) не успева да одговори на неколико техничких изазова јер су уређаји (осим за локална приватна решења у облаку) изван предузећа. Због скалабилности и сувишности, базе података које се налазе у облаку могу се динамички појављивати на новим локацијама током времена. Ова динамична природа облака чини традиционалне методе непрактичним и захтева да се узму у обзир нови приступи дизајнирани за дистрибуирана окружења.

Још једно ограничење мрежних решења за надгледање у облаку је технологија виртуелизације. У прошлости су се апликације које су користиле базу података обично распоређивале на одвојеним физичким серверима, док је сама база података која је била домаћин апликацијама инсталирана на одвојеним умреженим серверима [20]. Међутим, коришћењем технологије виртуелизације, физички ресурси се деле у облаку што понекад резултира окружењима у којима се и апликација и базе података налазе на истим физичким серверима. На пример, у примеру на слици 12, комуникација између апликације и базе података се одвија у потпуности унутар истог физичког сервера. Уређаји за надзор мреже неће моћи да открију ове трансакције јер се неће генерисати мрежни саобраћај током комуникације између виртуелних машина.



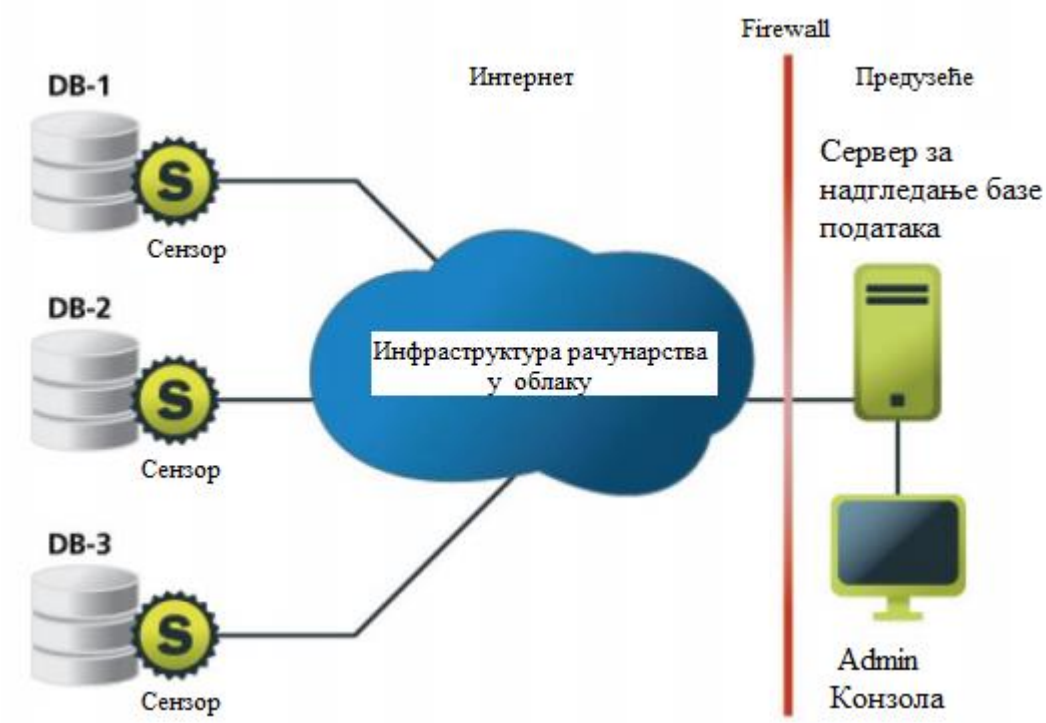
Слика 12 Комуникација се одвија унутар сервера [20]

Једно од очигледних решења за ово питање било би приближавање алата за праћење што је могуће ближе циљу. Један од начина да се то постигне је натерати једну од виртуелних машина да делује као надзорни уређај и тиме извршити реорганизацију саме архитектуре тако да виртуелни сервери шаље сав саобраћај кроз виртуелну машину за надзор. Међутим, овај приступ има два главна недостатка јер прво драстично погоршава перформансе (све трансакције у базу података морају проћи кроз виртуелни уређај), а други проблем је што ствара архитектонске компликације.

Компликације у архитектури настају јер би предузећа требала да дизајнирају систем на такав начин да сав промет ка базама података треба прво да прође кроз виртуелни уређај [20]. Узимајући у обзир динамичку природу облака, овај приступ неће бити практичан за cloud окружења у којима хостови долазе и одлазе, а додавање виртуелних уређаја било би крајње непрактично.

Да би решење било ефикасно, локални сензори или агенти морају бити способни да брзо реагују на упозорења, спроводећи потребне заштите у случају кршења смерница и давати благовремена упозорења. На основу скупа смерница и правила која се преузимају од централног управљачког сервера, сензори / агенти ће вршити ревизију, слати упозорења или обустављати сесије које крше унапред задате услове. Ради сигурне и ефикасне трансакције полиса и упозорења, саобраћај између сензора и конзоле за даљинско управљање треба да буде шифрован и компримован [20].

На слици 13 је приказано праћење дистрибуиране мреже засноване на сензорима.



Слика 13 Праћење дистрибуиране активности засновано на сензору [20]

Ови агенти / сензори морају бити дизајнирани тако да не трпе исте слабости попут наметљивих процедура имплементације и проблема са перформансама које су претрпела стара решења заснована на хосту. Сензори морају бити лаган софтвер који треба да делује као додатак и који се лако може додати на виртуелну машину паралелно са инстанцама базе података. Сензор не сме бити заснован на имплементацијама на нивоу језгра које захтевају поновно покретање машине.

Компанија за безбедносни софтвера, McAfee, пружа једно такво решење пружајући софтверски заснован сензор. McAfee пружа напредна безбедносна решења која штите податке и заустављају претње отвореним, предвидивим и интелигентним приступом. Сензор се може инсталирати на исту виртуелну машину заједно са другим инстанцама базе података. Сензор функционише тако што надгледа трансакције базе података које се јављају у меморији и на тај начин штити систем од свих врста унутрашњих и спољашњих напада. Да би несметано радио, једина информација која је потребна од новоинсталираног сензора је логична локација централног управљачког сервера која би агентима хоста омогућила праћење активности базе података и спречавање напада на систем [20].

7.6 Разматрање шифровања

Један од најбољих начина да се обезбеди поверљивост осетљивих података у облаку је коришћење шифровања за податке у транзиту, као и податке који мирују. Подршку за шифровање података у транзиту нуде готово сви добављачи база података у облаку (који користе TLS / SSL за пренос података), али врло мало њих нуди могућности шифровања података у стању мировања [16]. У основи постоје три опције шифровања које су доступне потрошачу у облаку за податке који мирују :

- Делимично шифровање базе података засновано на стандардним техникама шифровања
- Потпуно шифровање базе података засновано на стандардним техникама шифровања

- Потпуно шифровање базе података засновано на власничкој техници шифровања добављача услуга у облаку

Главна пословна идеја добављача услуга у облаку заснива се на ефикасном коришћењу ресурса од стране групе потрошача. То ће рећи, што више купаца користи исте физичке ресурсе, то више добављачи услуга остварују профит. Овај пословни модел игра важну улогу за добављаче услуга у облаку да ли нуде услуге шифровања или не. Шифровање, као интензиван процес, смањује укупну количину купаца по ресурсу и повећава укупне трошкове. Стога већина добављача у облаку нуди само делимично шифровање на неколико поља базе података, као што су лозинке и бројеви рачуна. [16] Иако неки добављачи нуде пуне опције шифровања базе података, то драстично повећава трошкове да хостинг база података у облаку постаје скупљи од интерног хостинга. Неки добављачи нуде алтернативе потпуном шифровању базе података, које имају мање утицаја на перформансе система, али користи неефикасну технику коју је лако заобићи. Друга доступна техника шифровања за потрошаче су прилагођена решења за шифровање које пружа облак. То не утиче на укупне перформансе система, али се такође не сматра сасвим сигурним.

Стандарди шифровања као што су AES, DES, 3DES итд. су темељно испитивани и верификовани. Годинама многи истраживачи и квалификовани криптографи раде на стандардним криптографским техникама. Мало је вероватно да би добављач услуга у облаку потрошио исту количину финансија и времена на истраживању заштићених решења за шифровање, због тога се препоручује да се заштићена решења за шифровање не користе по сваку цену на уштрб безбедности и провереності стандардних криптографских метода.

8. Стандардне безбедности и примена

Cloud рачунарство нам омогућава да креирамо, конфигуришемо и прилагодимо пословне апликације на мрежи. Стручњаци покушавају да осмисле и преобликују дизајн рачунарства у облаку како би се што боље прилагодио данашњем добу. Када се појаве безбедносни проблеми у којима се јављају губици због крађе података и приватности података, тада аутоматски настају различити проблеми са којима се суочава добављач услуга у облаку. Заузврат се потрошач услуга у облаку такође суочава са разним проблемима као што су шифровање података, приватност, малвер апликације. Зато се мора сигурност рачунарства у облаку сматрати главним задатком, јер ако она није задовољена систем не функционише у смеру обостраног добитка.

Прва ствар на путу ка обезбеђивању сигурности података је да подаци у облаку морају бити ускладиштени у шифрованом облику. Трећа страна пружа инфраструктуру на којој ће корисник складиштити податке на cloud платформи. Подаци се увек чувају у удаљеном серверу и приступиће им се кад год је то потребно из удаљеног подручја. Услуге хостинга и складиштења путем интернета су комбинација технологија и платформи. Већ је речено да постоје три врсте облака, то су : приватни облак, јавни облак и хибридни облак.

Сада је ствар размишљања како би се могло лако приступити подацима и одржавању система на поверљив начин. Након истраживања у ове сврхе, генерално главно безбедносно питање у рачунарству у облаку које се лако може решити, а купци ће се моћи задовољити коришћењем ове технологије, а то је примена AES стандарда. Због свега тога је потребан стандард шифровања за спречавање неовлашћеног приступа свим функционалним јединицама система. Испитивање значаја коришћења Advance Encription Standard (AES) и шеме за аутентификацију за обезбеђивање сигурности података док су у складишту се сматра значајним питањем [21].

8.1 Безбедност и криптографија

У данашње време сигурност је главна брига на интернету, а главни проблем је обезбеђивање података на што ефикаснији начин у складишту облака. У успостављању стандардне технологије требало би се укључити и питање мрежа, оперативних система и распоређивање ресурса. Такође се укључује управљање трансакцијама, базе података, виртуелизацију, уравнотежење оптерећења, контролу паралелности и управљање меморијом. Сигурносни циљеви података покривају три тачке: доступност; поверљивост и интегритет. У сигурности облака постављају се четири врсте проблема: издавање података, питања тајности, безбедносна питања и проблеми са зараженом апликацијом. Сва ова питања треба правилно размотрити. Због наведених проблема је криптографија обавезна. Криптографија је метода која се у великој мери заснива на математичким и информатичким правилима. Криптографски алгоритми могу израчунати закључак о тежини шифровања, а такође помажу у стварању таквих алгоритама које је тешко дешифровати у пракси од стране било ког нападача на систем. На једноставан начин можемо рећи да је криптографија уметност и наука која скрива поруке на начин који не може да се дешифрује без знања кључа, у информационој сигурности која је препозната као криптографија. У раду ће бити речи о алгоритама за шифровање са симетричним кључем [22].

Криптографија је метода чувања и прикривања критичних и тајних информација у криптичном облику, тако да само људи који су намеравали да их читају могу имати приступ.

Шифровање се врши претварањем обичног текста у текст шифре помоћу одговарајућих сигурносних алгоритама, а касније се врши дешифровање које враћа текст шифре натраг у обичан текст [7]. Криптографија пружа функције поменуте у наставку [21]:

- Интегритет података: Интегритет података значи да су информације вредне само ако су тачне. Бави се одржавањем и осигуравањем конзистентности информација.

- Аутентификација: Аутентификација се односи на утврђивање да ли је неко уствари оно што декларише да јесте.

- Нерепутација: Односи се на уверење да странка или појединац не може порећи аутентичност свог потписа

- Поверљивост: Односи се на крађу, неовлашћени приступ и губитак приватности.

Управо је због криптографије облак сигурнији у поређењу са традиционалним безбедносним системима. Разлике између заштите рачунара у облаку и традиционалног система безбедности се налазе у табели 4.

Табела 4 Разлика између Традиционалног система безбедности и сигурност у облаку

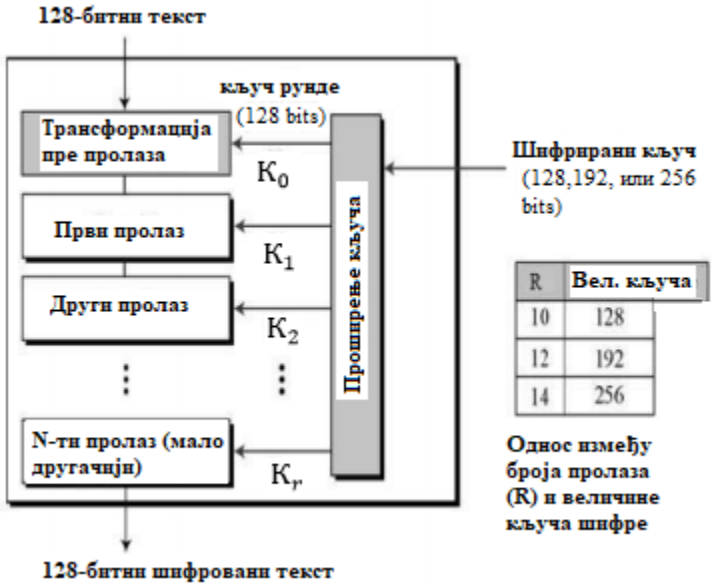
Традиционални систем безбедности	**Сигурност у облаку**
Интерни центри за обраду података	Центри за податке независних произвођача
Велики почетни трошкови	Ниска почетна улагања у инфраструктуру
Споро скалирање	Брзо скалабилно
Нижа ефикасност	Ефикасно коришћење ресурса
Дуже време за стављање на тржиште	Скраћено време за стављање на тржиште
Већи трошак	Трошкови засновани на употреби

8.2 AES (Advanced Encryption Standard)

Data Encryption Standard (DES) треба заменити неким новим алгоритмом за шифровање јер му је кључ постао недовољно безбедан. Сваким даном повећавајући рачунарску снагу, сматрало се да више није безбедан од исцрпних напада претраживача кључева. Поред тога брзина DES-а није најбржа. Набројане недостатке је употпунио AES (Advanced Encryption Standard) алгоритам шифровања који је предложен као адекватна замена [21].

Рад AES алгоритма :

AES укључује замену улаза одређеним излазима или мешање битова. AES је дизајниран да извршава све своје операције на бајтовима, а не над битовима. Због тога се AES блок отвореног текста од 128 битова третира као 16 бајтова који садрже по 8 бита. Ових 16 бајтова распоређено је у матрицу од 4 * 4 (четири реда и четири колоне). Број рунди није фиксиран у случају AES [9]. Он зависе од дужине кључа. 128-битним кључевима је потребно 10 рунди, 192-битним кључевима 12 рунди, а 256-битним кључевима 14 рунди. Свака рунда користи различити 128-битни кључ рунде који се израчунава из оригиналног AES кључа. Читав поступак је приказан на слици 14 [21].



Слика 14 Рад AES алгоритма [21]

Процес шифровања

Свака рунда се састоји од четири потпроцеса која су приказана на слици 115.

Слика 15 Кораци укључени у процес шифровања [21]

Замена бајтова (под-бајтови)

16 улазних бајтова замењује се тражењем фиксне табеле (S-кутије). Резултат је матрица од четири реда и четири колоне.

Промени редове

Сваки ред матрице 4 * 4 померен је улево. Уноси који отпадају поново се убацују на десну страну реда. Поступак који се примењује за обављање замене је следећи [21]:

- Први ред није померен.
- Други ред пролази кроз једно (бајтно) померање положаја улево.
- Трећи ред је подвргнут померању два положаја улево.
- Четврти ред пролази кроз три положаја померања улево.

- Резултат је нова матрица која се састоји од истих 16 бајтова, али померена један према другом.

Микс колона

Сада се користи посебна математичка функција за трансформисање сваке колоне од четири бајта. Функција узима четири бајта једне колоне као улаз и избацује четири потпуно нова бајта која замењују изворну колону. Резултат даје нову матрицу од 16 нових бајтова. Овај корак се не изводи у прошлом кругу.

Додавање кључа рунди

16 бајтова се сада разматра као 128-битним и XOR 128 битним кључем. Резултат је шифровани текст ако је тренутно покренута последња рунда. У супротном, резултујући 128-битови се опет тумаче као 16 бајтова и следећа рунда почиње.

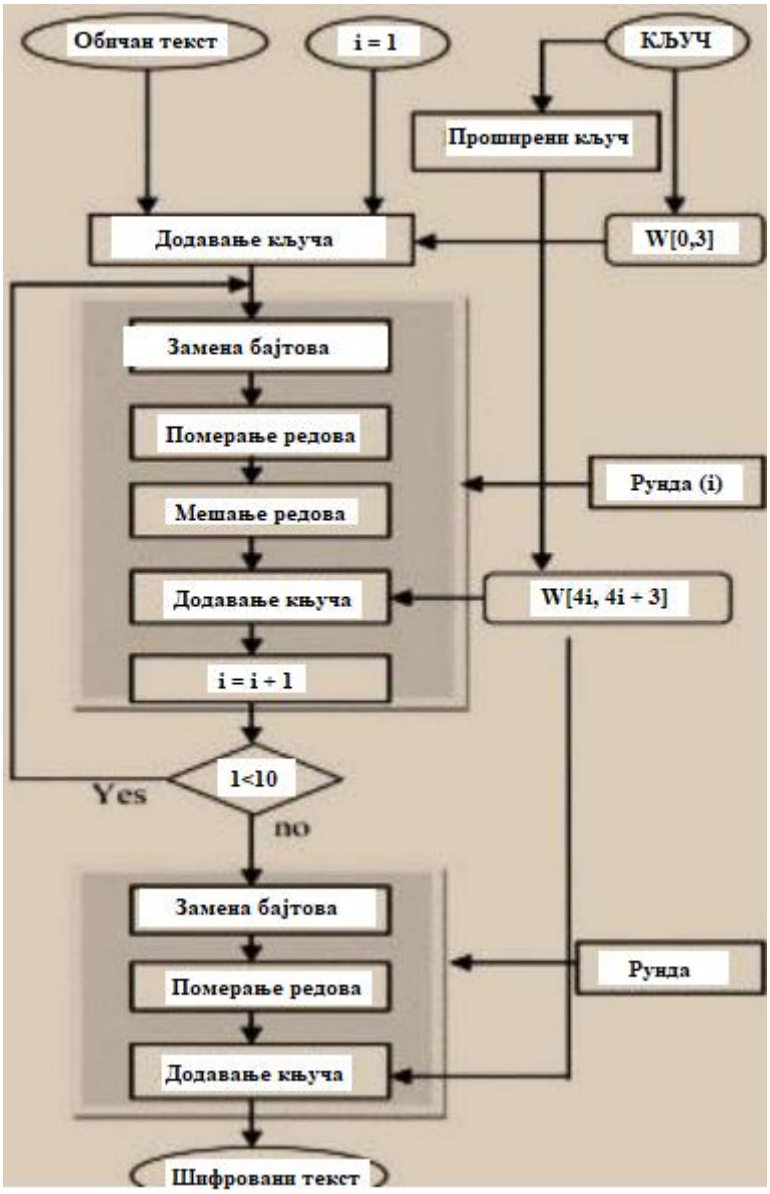
Процес дешифровања

Процес дешифровања текста AES шифре сличан је процесу шифровања само у обрнутом редоследу. Свака рунда садржи четири процеса изведена у обрнутом редоследу :

- Додавање кључа рунди
- Мешање колоне
- Померање редова
- Замена бајтова

Будући да су потпроцеси у сваком кругу обрнути, за разлику од Феистеловог шифровања, алгоритми за шифровање и дешифровање морају се применити одвојено, иако су врло уско повезани [21].

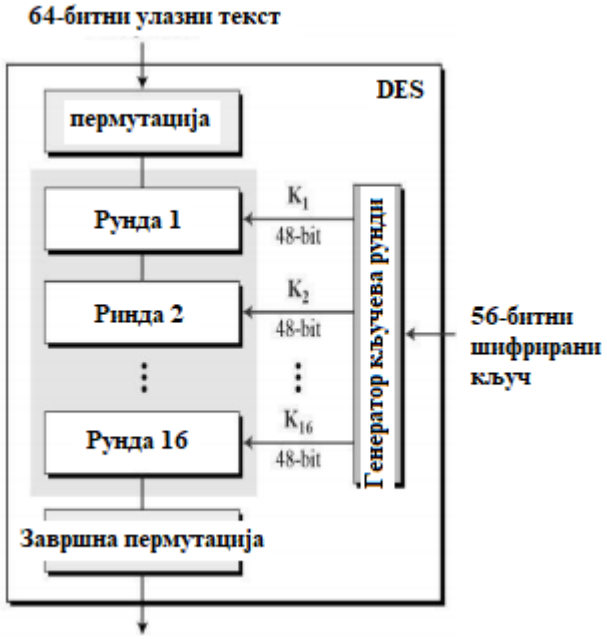
Дијаграм тока приказан на слици 16 резимира целокупан рад AES-а.



Слика 16 Дијаграм тока који приказује рад AEC-а [21]

8.3 DES (Data Encryption Standard)

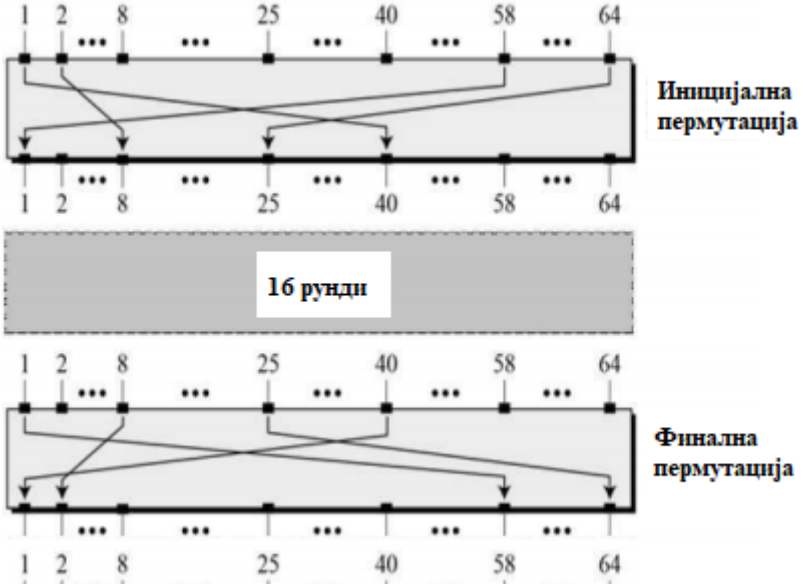
Алгоритам DES је најкоришћенији алгоритам за шифровање података. Као такав представљао је стандардни алгоритам за криптовање података који енкриптује блок величини 64 бита. Стандард за шифровање података (DES) је блок шифра симетричног кључа коју је предложио национални институт за стандарде и технологију (NIST). DES је конструисан применом Феистелове шифре [11]. Користи 16 рундни Феистелове структуре и величина блока 64-бита. Иако је дужина кључа DES 64-битна, алгоритам шифровања не користи 8 од 4 бита, а ефективна дужина кључа смањује се на 56 бита. Општа структура DES приказана је на слици 17.



Слика 17 рад DES алгоритма [21]

Почетна и завршна пермутација

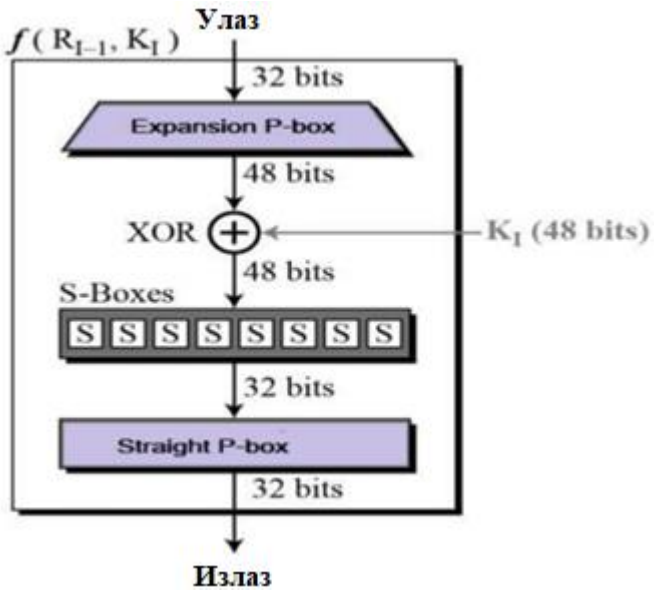
Почетна и завршна пермутација су равне пермутационе и обрнуте су једна од друге. Слика 18 приказује почетну и завршну пермутацију као испод.



Слика 18 Почетна и завршна пермутација [21]

Функција рунде

Овде DES функција игра своју улогу. Функција примењује 48-битни кључ на крајњих 32 бита да би се добио излаз од 32-битног као што је приказано на слици 19.



Слика 19 Рад функције рунде [21]

Кутија за пермутацију проширења

Будући да је десни улаз 32-битни, а дужина кључа 48-битна, потребно је проширити десни улаз на 48 битова, као што је приказано на слици 20.

Слика 20 Проширење десног улаза од 32 бита до 48 бита [21]

Графички приказана логика пермутације описана је као DES табела као што је приказано у табели 5.

Табела 5 DES тебла

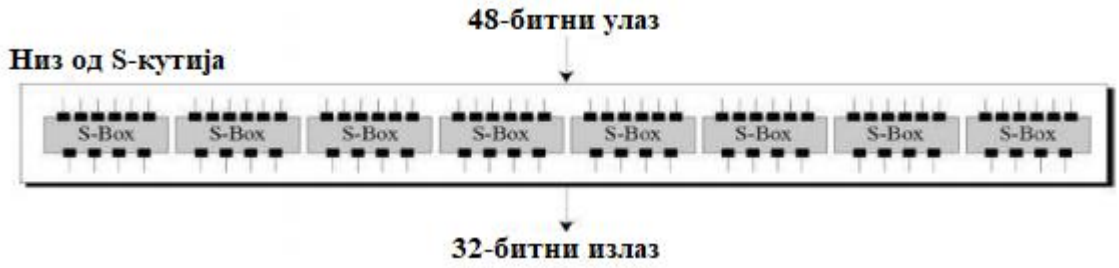
32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	01

XOR (Whitener)

Пратећи пермутацију проширења, DES ради XOR операцију на проширеном десном делу и кључу рунде. Кључ рунде се користи само у овој операцији.

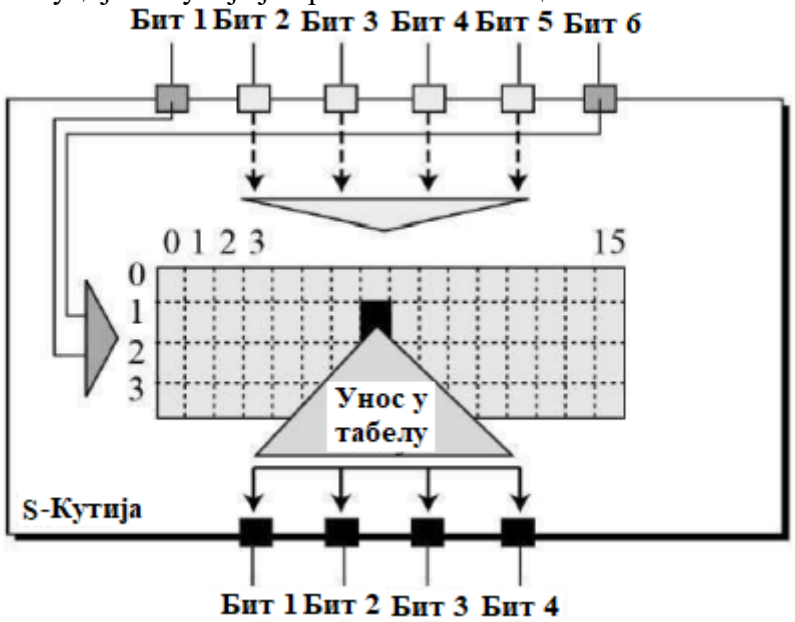
Супституцијске кутије (Substitution Boxes)

Супституцијске кутије изводе стварно мешање. DES користи 8 супституцијских кутија, свака са 6-битним улазом и 4-битним излазом, као што је приказано на слици 21.



Слика 21 Супституцијски процес кутија [21]

Правило супституцијске-кутије је приказано на слици 22.



Слика 22 Правило супституцијске кутије [21]

Постоји укупно осам табела уноса s-кутија. Излаз свих осам с-кутија се затим комбинује у 32-битnим секцијама.

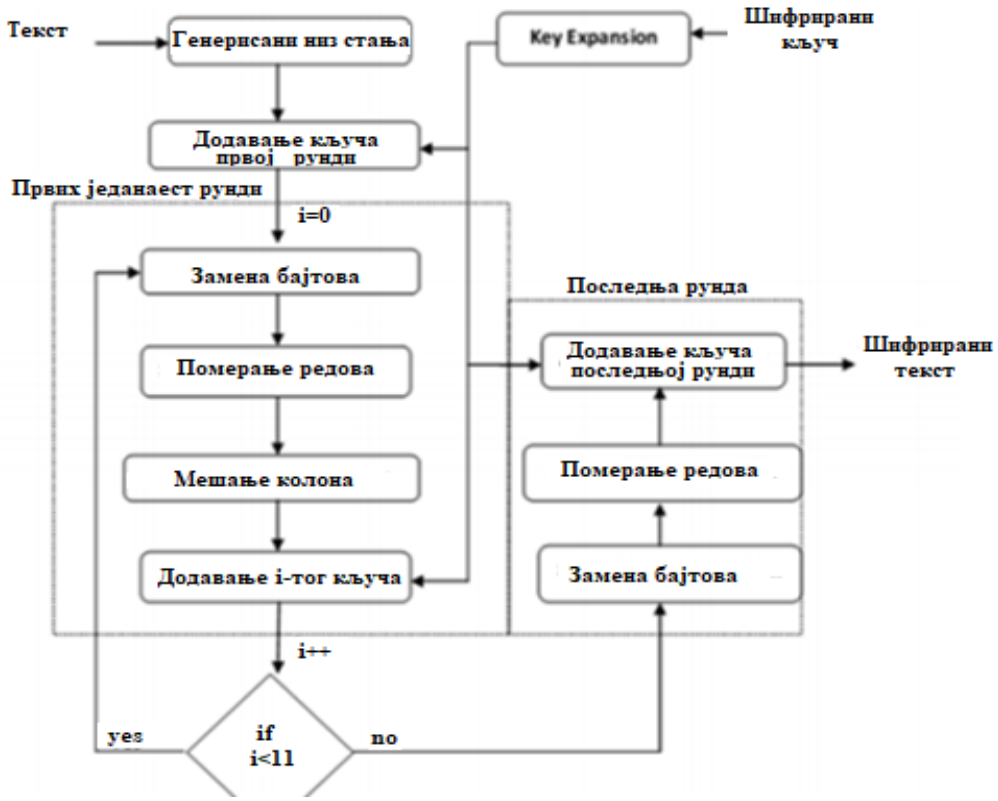
Директна пермутација

Затим се 32-битни излаз s-кутија подвргава директној пермутацији са правилом приказаним у табели 6.

Табела 6 Директна пермутација [21]

16	07	20	21	29	12	28	17
01	15	23	26	05	18	31	10
02	08	24	14	32	27	03	09
19	13	30	06	22	11	04	25

Рад DES-а сажет је у дијаграму тока приказаном на слици 23.



Слика 23 Ток рада дес алгоритма [21]

8.4 Примена AES алгоритма за енкрипцију података

Премена алгоритма AES за енкрипцију података и блок шифре коју генерише алгоритам је усвојила влада Америке. После веома дуге анализе нашао је примену као стандард шифровања података. Алгоритам је доступан свима а његов код је отвореног типа. У наставку биће приказана практична примена и изворни код уз помоћ програмског језика javascript.

8.5 Подручје примене

AES алгоритам је један од најмоћнијих алгоритама који се широко користи у различитим областима широм света. Овај алгоритам омогућава брже шифровање и дешифровање података него алгоритми DES и 3DES. Поред тога, користи се у многим протоколима криптографије, као што су Socket Security Layer (SSL) и Transport Security Layer протоколу, како би се пружила много већа сигурност комуникације између клијента и сервера преко интернета. Пре него што је AES алгоритам објавио оба протокола за шифровање и дешифровање података, ослањао се на DES алгоритам, али након појављивања неких рањивих делова овог алгоритма, Internet Engineering Task Force (IETF) је одлучио да DES замени AES алгоритмом. AES се такође може наћи у већини савремених апликација и уређаја којима је потребна функција шифровања као што су WhatsApp, Facebook, Messenger, Intel и AMD процесор и Cisco уређаји попут рутера, комутатора итд. Поред тога, AES Crypt пакет доступан је у многим библиотекама софтверских програма као што су библиотека C++ library, C# /.NET, Java и JavaScript која се користи за лако и сигурно шифровање датотека од уљеза.

8.6 Програм за Енкрипцију и Декрипцију

Једноставан пример примене технологије енкрипције је приказан на слици 26. Најпре се мора инсталирати пакет npm i crypto-js како би Viual Studio Code имао библиотеку са свим потребним функцијама и методама које се користе у криптографији. На слици 24 се налази Terminal у којем се уписује ' npm i crypto-js ' како би се обезбедила криптографска библиотека javascript пакета.

```
PS C:\Users\nikol\desktop> npm i crypto-js
[.....................] - rollbackFailedOptional: verb npm-session bff6eee42b2b9e03
```

Слика 24 Инсталација библиотеке

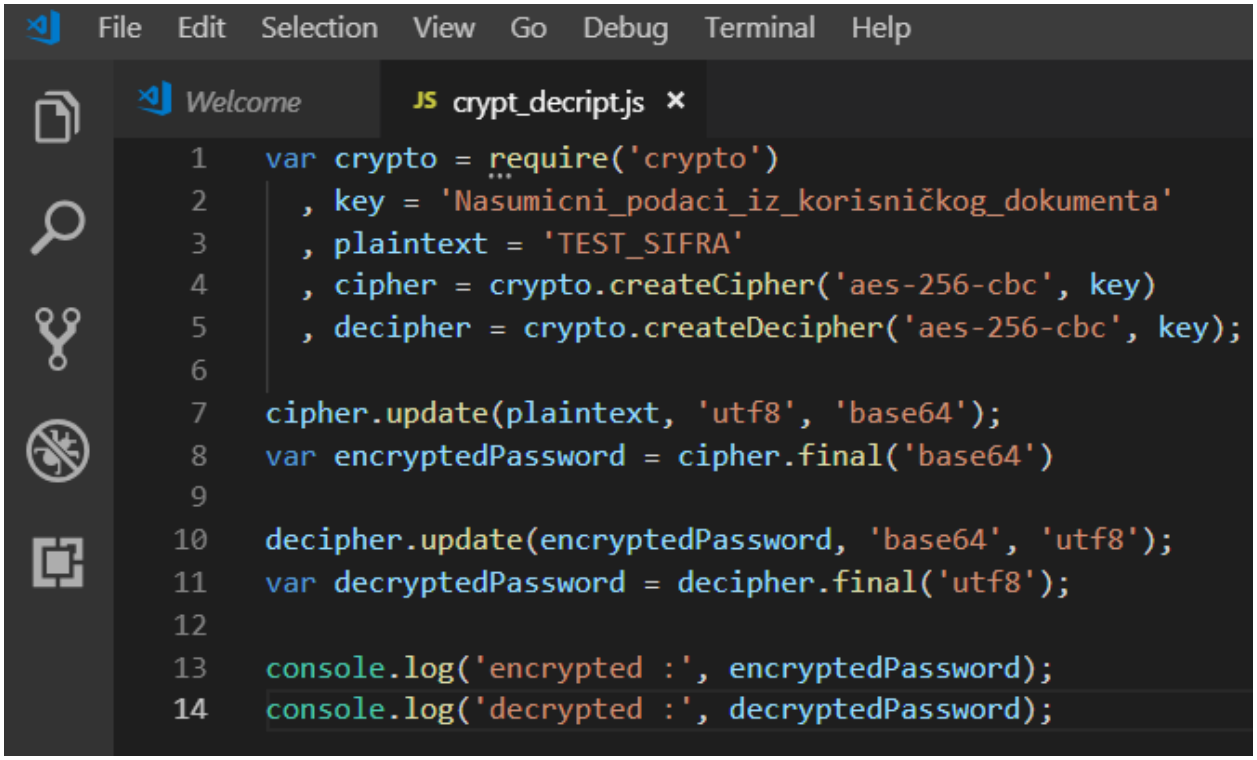
Након што је преузета библиотека, треба се појавити следећи текст у терминалу као што је приказано на слици 25.

```
npm WARN ajv-keywords@3.2.0 requires a peer of ajv@^6.0.0 but none is installed. You must install peer dependencies yourself.
npm WARN nikol@1.0.0 No description
npm WARN nikol@1.0.0 No repository field.

+ crypto-js@4.0.0
added 1 package from 1 contributor, updated 1 package and audited 555 packages in 60.358s
found 83 vulnerabilities (35 low, 22 moderate, 25 high, 1 critical)
```

Слика 25 Извештај npm пакета

Након овог једноставног корака могу се користити све функције из библиотеке crypto-js, а која пружа енкрипцију и декрипцију докумената, текста, слика итд. У следећем примеру извршена је енкрипција текста који се налази на слици 26 (линија 2) изворног кода. Текст над којим се врши шифровање сачуван је у променљиивој 'plaintext'. Променљива ’key’ су у пракси додатни подаци корисника за једносмерно шифровање.

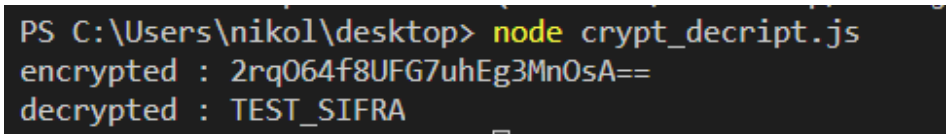


Слика 26 Изворни код програма за шифровање текста

Примери класе Cipher користе се за шифровање података. Може користити на један од два начина:

- Као ток који је и читљив и записиван, где су записани обични нешифровани подаци за производњу шифрованих података на читљивој страни, или
- Коришћење метода cipher.update() и cipher.final() за стварање шифрованих података.

Методе The crypto.createCipher() или crypto.createCipheriv() користе се за креирање инстанци шифре. Објекти шифре се не смеју креирати директно помоћу нове кључне речи. Тринаеста и четрнаеста линија слике 26 приказује шишровани и дешифровани текст.



Слика 27 приказ Шифрованог и дешифрованог текст

На слици 27 приказан је шифровани и дешифровани текст очитан у конзоли Visual Studio Code-a.

9 Закључак

Са применом cloud рачунарства као новим начином пружања IT услуга добиле су се додатне погодности у погледу флексибилности и продуктивности у коришћењу динамички додељених ресурс. Cloud ће се и даље развијати као основа за будући интернет где ћемо бити повезани заједно са мрежом садржаја и услуга.

Рачунарство у облаку је врло флексибилна парадигма за испоруку рачунарских ресурса. За неке то значи могућност оснивања нове startup компаније знајући да почетни ресурси неће бити скупи, али нагли пораст потражње корисника неће компанију учинити жртвом сопственог успеха, као што се то у неким случајевима догодило у прошлост у којој сервери нису могли да се носе са потражњом, а компанија губила клијенте јер постају незадовољни лошим временом одзива. За друге људе рачунарство у облаку значи лакшу администрацију, а питања попут лиценцирања, прављења резервних копија и безбедности воде се на другим местима. У другим случајевима, рачунарство у облаку значи имати моћно рачунарско окружење доступно било где, где корисник може да приступи веб прегледачу. Уз ову флексибилност, скалабилност и лакоћу одржавања, није ни чудо што се рачунарство у облаку истиче као технологија будућности. Наравно, постоје питања приватности података која могу бити забрињавајућа, потребна је добра интернет веза, а неке организације ће можда желети да задрже контролу над сопственим ресурсима.

Међутим, ови проблеми се обично могу ефикасно решити добрим избором cloud модела, а коришћење облака остаје врло ефикасан начин за брзо постављање моћног система. Разни облици услуга, инфраструктура, платформа и софтвер као услуга пружају сигуран начине за испоруку нових производа до којих би купци могли доћи. Већ постоје примери широко коришћених производа и веб локација који су забележили изузетан раст јер су се креативне идеје могле брзо применити, зато што се накнадна потражња могла лако задовољити флексибилношћу рачунарства у облаку. Чини се да је будућност ограничена само маштом иноватора који могу смислити апликације које ће људима помоћи да комуницирају, чувају и обрађују огромне количине информација, било да се ради о милионима појединаца са малим колекцијама личних података или једна велика организација са великом колекцијом података која се обрађује.

У овом раду представљени су бројни безбедносни захтеви за архитектуру рачунарства у облаку. Размотрени су захтеви, а идентификовани су безбедносни обрасци и архитектонски елементи који чине да облак буде сигурнији за кориснике. Затим је било речи о неколико репрезентативних архитектура сигурносног система у облаку и размотрени важни аспекти истих. Испитивањем неколико кључних стратегија које ако се узму у обзир током дизајнирања могу донети значајне оперативне користи. Такође је испитана широка тема безбедности података у облаку. Као што се видело, осетљиви и контролни подаци треба да буду шифровани. Мрежни саобраћај до и од приступних тачака у облаку треба да буде шифрован због поверљивости, интегритета и сталне доступности. Шифровање података се треба користити за податке који мирују ради заштите поверљивости и интегритета. Било да се шифровање података врши на елементима података, датотекама, директоријумима, може бити закомпликовано многим факторима, укључујући перформансе и функционалност.

У раду је разрађена важност сигурности у рачунарству у облаку и како енкрипција може заштитити комуникацију и ускладиштене податке од неовлашћеног приступа. Тренутно је AES најнапреднији и усвојени алгоритам за извођење криптографије у хардверу и софтверу. До данас није откривен ниједан успешан криптоаналитички напад на AES. Карактеристика флексибилне дужине кључа омогућава одређени степен будуће заштите од исцрпних напада кључева. У овом раду су приказани проблеми повезани са сигурношћу података у рачунарству у облаку, као што су приватност података, губитак података и доступност података.. У јавном облаку подаци се хостују ван локације, а ресурси се јавно деле, стога не обезбеђује виши ниво сигурности. Ако се овај модел архитектуре правилно

успостави, може заштитити јавни модел облака према стандардној сигурности. Овде се AES сигурност обезбеђује применом доброг система управљања кључевима и добро развијене структуре. Овај модел би могао да се имплементира у различите платформе за рачунарство у облаку како би се добио ефикаснији начин рачунарства у облаку као што су SaaS, PaaS итд.

Породица WS-security пружа основни скуп стандарда за заштиту SOA-а, међутим број и сложеност стандарда су дефинитиван проблем. Та сложеност може обесхрабрити усвајање ових стандарда у SOA, посебно за програмере апликација, чији је посао компликован због безбедносних потреба. Ови стандарди се такође развијају а са њима и нови безбедносни стандарди, па се очекује да ће се SOA безбедносни део временом развијати у доста сигурнији и једноставнији систем.

Добављачи пружају нове алате за упрошћавање интеграције WS-security стандарда у веб услуге. У овом тренутку, међутим, још увек није лак задатак интегрисати WS-security стандарде у веб услуге без обзира на многобројна унапређења.

За практичну примену безбедности могу се искористити стандардни принципи безбедности који помажу у вођењу архитеката и програмера у одабиру одговарајућих механизама за заштиту SOA-а.

10 Литература

1. Furht, B. and Escalante, (2010): *Handbook Of Cloud Computing,* Department of Computer & Electrical Engineering and Computer Science, Florida Atlantic University, Boca Raton, FL, USA

2. J. Srinivas, K. Venkata Subba Reddy, Dr. A. Moiz Qyser (*2012*): *Cloud computing basics,* International Journal of Advanced Research in Computer and Communication Engineering

3. Peter Mell and Timothy Grance (2011): *The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, Gaithersburg

4. Monjur A. and M. A. Hossain (2014): *Cloud Computing and Security Issues in the Cloud*, International Journal of Network Security & Its Applications, Daffodil Institute IT, Dhaka, Bangladesh.

5. Swati I. Bairagi, Ankur O. Bang (2015): *Cloud Computing: History, Architecture, Security Issues,* International Journal of Advent Research in Computer and Electronics, Pankaj Laddhad Institute of Technology and Management Studies

6. S.K. Sowmya, P. Deepika, J. Naren (2014): *Layers of Cloud – IaaS, PaaS and SaaS, A Survey*, Sastra University,Tirumalaisamudram, Thanjavur

7. *Веб страница приступљено 7.10.2020 - https://medium.com/@manrai.tarun/cloud-computing-deployment-models-technical-know-how-33a3ad30cb66*

8. *Веб страница приступљено 19.10.2020 - https://data-flair.training/blogs/features-of-cloud-computing*

9. Christoph Fehling (2015): *Cloud Computing Patterns Identification, Design, and Application,* Stuttgart University

10. Lee Badger ,Tim Grance ,Robert Patt-Corner ,Jeff Voas (2012) - NIST Special Publication 800-146, DRAFT Cloud Computing Synopsis and Recommendations, Recommendations of the National Institute of Standards and Technology

11. *Веб страница приступљено 21.10.2020 - https://cloudscomputing.net/cloud-architecture*

12. *Веб страница приступљено 22.10.2020 - https://www.geeksforgeeks.org/crm-and-erp-in-cloud-computing [5.web]*

13. G. Kiryakova, N. Angelova, L. Yordanova (2015) "Application of cloud computing services in business", Faculty of Economics, Trakia University, Stara Zagora, Bulgaria

14. Jaydip Sen (2014): *Security and Privacy Issues in Cloud Computing*, Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

15. Sarath Indrakanti (2012)*: Service Oriented Architecture Security Risks and their Mitigation*, DSTO Defence Science and Technology Organisation, Edinburgh South Australia

16. Axel Buecker, Paul Ashley, Martin Borrett, Ming Lu, Sridhar Muppidi, Neil Readshaw (2007),*Understanding SOA Security Design and Implementation*, International Business Machines Corporation IBM, U.S.A

17. Imal Sakhi (2012): *Database security in the cloud*, School of Engineering Sciences in Chemistry, Biotechnology and Health, Sweden

18. Ankur Pandey,Kirtee Shevade, Roopali Soni (2012) - *Application Level Security in Cloud Computing* - Thakral College of Technology Bhopal,India.[*4]*

19. Winkler, Vic (J.R.) (2011): *Securing the Cloud Cloud Computer Security Techniques and Tactics*, Elsevier, Amsterdam

20. John W. Rittinghouse and James F. Ransome (2009): Cloud Computing Implementation, Management, and Security, Taylor & Francis Group

21. S.Bansal , Dr. Gagandeep J. (2017) "*Analyzing Working of DES and AES Algorithms in Cloud Security*" - Dept. of Comp. Science, Punjabi University Guru Kashi College, Damdama Sahib

22. Md R. B. Emdad, Md Shahin K. (2019): *A Standard Data Security model Using AES Algorithm in Cloud Computing*, Department of Computer Science and Engineering, Jahangirnagar University, Savar, Dhaka [8]

23. Mr Srđan Atanasijević, (2009): *Bezbednost informacionih sistema,* Visoka tehnička škola, Kragujevac

24. Harold F. Tipton, Micki Krause (2008): *Information Security Management Handbook*, Taylor & Francis Group