Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-661-667

PRIMENA I BEZBEDNOSNI RIZICI CLOUD REŠENJA U EZDRAVLJU

Vladimir J. Radunović[1], Marko Č. Barjaktarović[2]
[1]DiploFoundation / Univerzitet Singidunum, Beograd
[2]Elektrotehnički fakultet, Univerzitet u Beogradu

Abstract:
Uvođenje elektronskog kartona pacijenta omogućilo je neuporedivo lakšu pretragu u odnosu na stari, ručno pisani sistem kartona, pojednostavilo je praćenje istorije bolesti i obezbedilo veliku istraživačku bazu. Prikupljeni podaci daju uvid u dijagnozu simptoma, preduzete tretmane i uticaj lekova, a mogu se iskoristiti i za razvoj sistema koji će pomagati doktorima u donošenju odluka.
Razvoj *Cloud* rešenja otvara i pitanje prenosa eZdravlja u *Cloud* domen. Zdravstvene organizacije mogu uštedeti sredstva potrebna za serversku opremu i razvoj sopstvenih softverskih rešenja, kao i prostor neophodan za smeštanje računarske opreme. Takođe, smanjuje se i broj tehničkog osoblja potrebnog za održavanje jednog bolničkog informacionog sistema. Podaci o pacijentima iz baza međusobno udaljenih zdravstvenih organizacija postaju dostupni za sprovođenje različitih statističkih analiza omogućavajući uvid u zdravstveno stanje stanovništva i rano uočavanje epidemija. Sa druge strane, bezbednost elektronskog zdravstvenog sistema predaje se u ruke provajderima *Cloud* servisa, čime se pojednostavljuje održavanje ali i gubi direktna kontrola nad bezbednosti ovih osetljivih podataka.
U radu je razmatrana arhitektura *Cloud*-a primenjena na eZdravlje, ekonomski aspekti uvođenja *Cloud* rešenja u eZdravlje, kao i problemi bezbednosti servisa i podataka o pacijentu u *Cloud*-u.

Key words:
Cloud,
eZdravlje,
bezbednost,
zaštita podataka.

UVOD

Korišćenje najnovijih informacionih tehnologija u zdravstvu unapređuje kvalitet zdravstvenih usluga i smanjuje troškove poslovanja [1], Prisutan je nedostatak kvalifikovanog medicinskog osoblja dok su zahtevi za zdravstvene usluge u konstantnom porastu. U cilju racionalizacije rada medicinskih ustanova, od 2006. godine ubrzan je razvoj eZdravlja u Srbiji [2], i do kraja 2012. godine preko 85 % ustanova primarne zdravstvene zaštite je dobilo informacione sisteme. Do kraja 2013. godine bolnički informacioni sistemi (BIS, odnosno eng. HIS - *Hospital Information System*) realizovani su za 10 ustanova, za još 9 ustanova realizacija u toku, ali i dalje nedostaje značajan deo računarske opreme [3].

Osnovnu komponentu zdravstvenog informacionog sistema predstavlja elektronski karton pacijenta (EHR - *Electronic Health Record*), odnosno skup elektronskih zapisa o pacijentu. Zamena klasičnog papirnog kartona EHR- om doprinosi bržem lečenju pacijenata, manjoj mogućnosti greške u dijagnostici, boljoj organizaciji medicinskih usluga i slično [4]. Takođe, EHR olakšava razvoj ekspertskih sistema za dijagnostiku kao što su CASNET/glaucoma (konsultativni sistem za glaukom), INTERNIST-I (konsultant u internoj medicini) i drugi.

Komponente zdravstvenog informacionih sistema Srbije predstavljaju: bolnički informacioni sistemi (BIS), laboratorijski informacioni sistemi (LIS), radiološki informacioni sistem (RIS) kao i informacioni sistemi ustanova primarne zdravstvene zaštite (domovi zdravlja). Na nivou Srbije svi oni su objedinjeni u centralni informacioni sistemi (CIS) koji sadrži još i resursne baze, šifarnike usluga, podatke o receptima, elektronske fakture, bazu osiguranika, bazu zaposlenih, izabrane lekare i drugo [2], Slična je struktura i zdravstvenih informacionih sistema drugih zemalja [4].

I pored ubrzanog razvoja eZdravlja u Srbiji i dalje nedostaje IKT oprema i IT osoblje potrebno za realizaciju i održavanje informacionih sistema [5], U cilju smanjenja troškova implementacije i održavanja eZdravlja *Cloud* rešenja dobijaju sve više zagovornika, jer se smanjuju sredstva neophodna za nabavku opreme [6], povećava sigurnost podataka sa stanovišta čuvanja, ali i sa aspekta privatnosti, omogućava se brže unapređenje servisa uz smanjenje ili potpuno eliminisanje prekida rada, obezbeđuje se mobilan pristup, pri čemu se koristi najsavremenija tehnologija [7]. Takođe, smanjuje se i potrošnja električne energije, kao i potrebno IT osoblje [7]. Sakrivanjem ličnih podataka iz EHR-a mogu se obezbediti podaci za sprovođenje analiza bolesti i tretmana u cilju brže

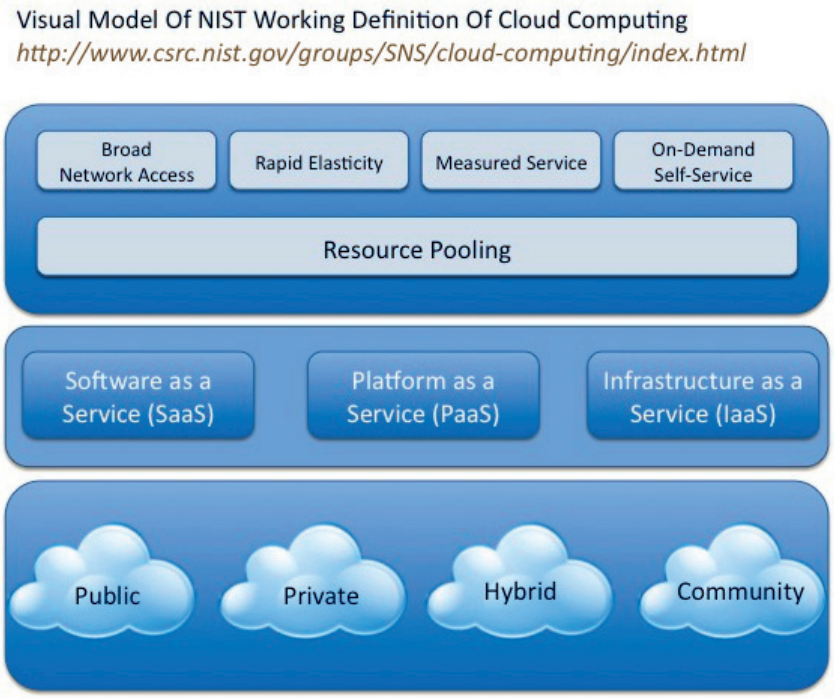
i preciznije dijagnostike, kao i razne statističke analize, a potrebni hardverski resursi zauzimaju se samo kada je to

U nastavku će biti prikazani modeli *Cloud*. rešenja, kao i mogućnost implementacije eZdravlja u oblaku sa osvrtom na ekonomske prednosti uvođenja eZdravlja u *Cloud* domen. Razmatraće se i bezbednosti rizici *Cloud* rešenja.

SPECIFIČNOSTI *CLOUD* REŠENJAI SERVISI EZDRAVLJA U OBLAKU

Prema NIST-u (*National Institute for Standards and Technology*, United States) računarstvo u oblaku (*Cloud Computing*) definiše se kao model koji omogućava, prema potrebi, mrežni pristup deljivim računarskim resursima (serverima, diskovima, aplikacijama i servisima), koji se mogu vrlo brzo zauzeti i osloboditi, pri čemu provajder usluga vrši minimalne intervencije [9]. Tri modela se definišu za *Cloud* u odnosu na resurse koji se obezbeđuju korisniku: softver, platformu i infrastrukturu, slika 1:

- Softver kao servis (*SaaS - Software as a Service*) - Provajder *Cloud*-n obezbeđuje korisniku aplikaciju i sve potrebno za njen rad. Korisnik ima pristup preko web browser-a i nema mogućnost kontrole resursa.
- Platforma kao servis (*PaaS - Platform as a Service*) - Korisnik može razviti aplikaciju koja se izvršava na platformi (*VM - virtual machine*) i koristi potrebne hardverske resurse. Korisnik nema mogućnost podešavanja servera, operativnog sistema i diskova za čuvanje podataka.
- Infrastruktura kao servis (*IaaS - Infrastructure as a Service*) - Provajder obezbeđuje računarske resurse dok korisnik *Cloud*-z postavlja sve potrebne aplikacije uključujući i operativni sistem.
- *Cloud* mora ispuniti i sledećih pet karakteristika:
- Servis na zahtev (*On-demand self-service*) - korisniku su uvek dostupni računarski resursi i oni se obezbeđuju automatski, tj. bez intervencije provajdera.
- Širokopojasni pristup (*Broad network access*) - servisi su dostupni kada postoji mrežni pristup bez obzira na tip uređaja (mobilni telefon, tablet, laptop ili desktop).
- Dostupnost resursa (*Resource pooling*) - računarski resursi se dodeljuju različitim korisnicima na osnovu njihovih trenutnih zahteva.
- Elastičnost resursa (*Rapid elasticity*) - sa stanovišta korisnika, računarski resursi su uvek dostupni, bez obzira na zahteve drugih korisnika.
- Merljivost usluga (*Measured service*) - obračun korišćenja računarskih resursa i *Cloud* servisa vidljiv je i za korisnika i za provajdera *Cloud*-a.
- Kada se posmatra način implementacije, moguće su četiri realizacije:
- Privatni oblak (*Private Cloud*) - Oblak koristi isključivo jedna organizacija (koja može imati više jedinica), a on je u posedu te organizacije ili drugog lica. Primer je realizacija celokupnog informacionog sistema bolnice u oblaku.
- Zajednički oblak (*Community Cloud*) - Oblak koristi isključivo skup organizacija koji imaju isti zajednički interes. Oblak je u posedu jedne ili više organizacija iz skupa ili drugog lica. Primer je servis za zakazivanje specijalističkih pregleda u ustanovama jedne regionalne oblasti [6],
- Javni oblak (*Public Cloud*) - Pristup oblaku imaju svi, kao u slučaju Google Drive. U slučaju zdravstva, primer predstavlja klinički sistem za pomoć u dijagnostici, pri čemu se mora voditi računa da podaci koji otkrivaju identitet pacijenta, doktora



Slika 1. Opšti model Cloud-a

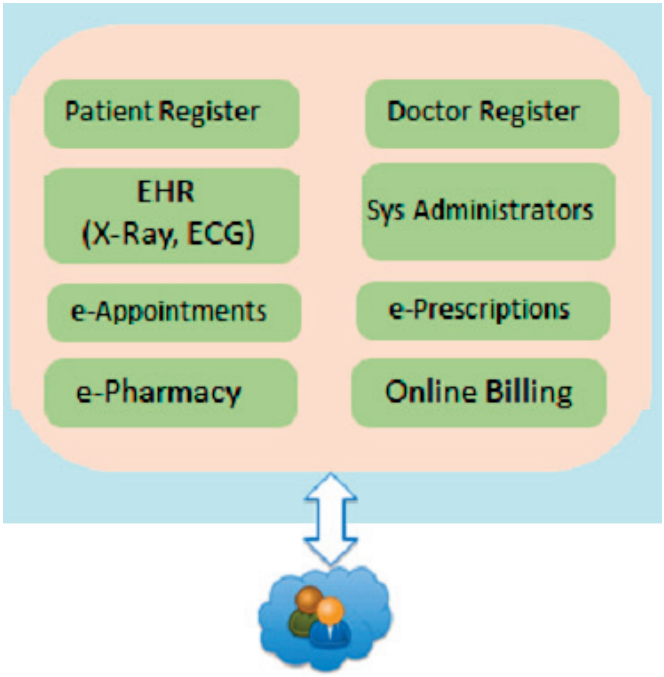
i zdravstvene ustanove nisu vidljivi korisnicima oblaka.

- Hibridni oblak (*Hybrid Cloud*) - Integracija nekoliko gore pomenutih rešenja u zajednički servis. Na primer, komunikacija dva privatna oblaka (dom zdravlja i ortopedska klinika) ostvarena je preko zajedničkog oblaka (servis za zakazivanje specijalističkih pregleda).

U slučaju eZdravlja, ne postoji jedinstven stav o načinu implementacije oblaka. Privatni oblak obezbeđuje maksimalnu zaštitu poverljivih podataka, dok je javni oblak ekonomski najisplativiji [10], ali se smatra da je hibridno rešenje najbolje, jer omogućava najjednostavniji prelazak sa tradicionalnih na *Cloud* rešenja [11]. Osetljivi podaci ostaju u okviru zdravstvenih ustanova, gde se postojeća IT rešenja prebacuju u privatni oblak. Sa druge strane, kada su potrebni računarski resursi za obradu podataka ili koriste se servisi koji ne otkrivaju identitet pacijenta, prelazi se u javni oblak.

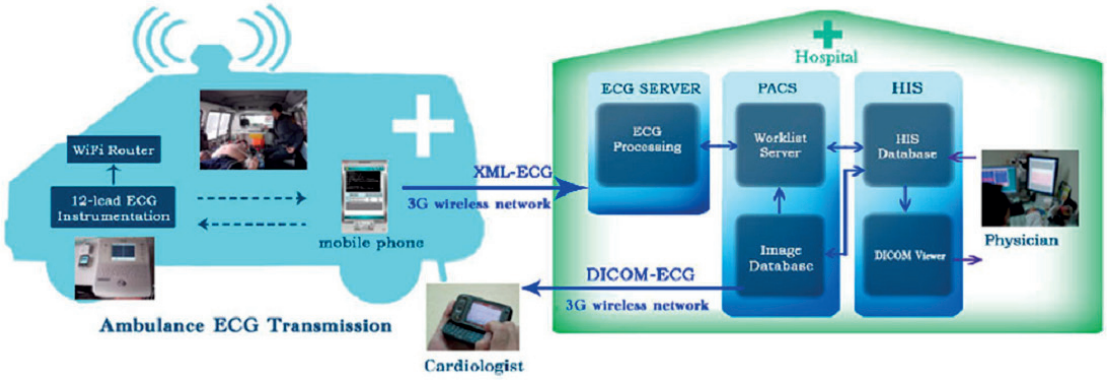
Najvažnije pitanje je ekonomska isplativost prelaska sa tradicionalnih na rešenja u oblaku. U literaturi se može pronaći nekoliko analiza. Studija koju je izvela konsultantska kuća *Booz Allen Hamilton* [12], pokazuje da su troškovi održavanja institucionalnih servisa u oblaku za 2/3 manji u odnosu na postojeća rešenja. Pri tome, što je veća infrastruktura koja se zamenjuje *Cloud* rešenjem to su troškovi manji. Procenjena NSV (neto sadašnja vrednost) je najveća za javni oblak (15.4), zatim sledi hibridno rešenje sa NSV = 6.4 i na kraju je privatni oblak (5.7). Yoo et al [13], razmatrali su isplativost zamene postojećeg bolničkog informacionog sistema (EHR, PACS - *Picture Archiving and Communications System*, i drugih kliničkih i administrativnih servisa) rešenjem u oblaku. Svim servisima je moguće pristupiti putem mobilnih platformi, nezavisno od operativnog sistema (*Windows, Android, iOS*) putem 400 virtuelnih mašina (1100 zaposlenih). Predviđena je ušteda od oko 192 hiljade USD u periodu od 5 godina, uključujući troškove migracije. Većina istraživača je saglasna u proceni da će prelazak na *Cloud* rešenje značajno smanjiti troškove održavanja opreme, osloboditi deo bolničkog prostora koji trenutno zauzima računarska oprema, smanjiti ulaganja u računarsku opremu i omogućiti IT osoblju da se fokusira na razvoj novih servisa umesto svakodnevnih intervencija na održavanju postojeće opreme [6],

I pored dobrih strana, i dalje su prisutne barijere pri uvođenju *Cloud* rešenja u eZdravlje, pre svega zbog privatnosti, kompatibilnosti i potrebe da se uloži napor u migraciju sistema, a postoji i neopravdani strah IT osoblja od gubitka posla [10]. Zbog toga se u literaturi može naći mali broj realizovanih rešenja. Između ostalih, u julu 2011. londonska bolnica *Chelsea and Westminster Hospital* uspostavila je *Cloud* EHR rešenje, kod koga pacijenti imaju punu kontrolu u definisanju ko ima pravo pristupa njihovim podacima. Italijanska pedijatrijska bolnica Bambino Gesu, uvela je rešenje u oblaku 2011. i u eksploataciji je zapaženo unapređenje saradnje između medicinskog osoblja, bolja komunikacija sa pacijentima i više vremena za IT osoblje [14]. Zatim, predstavljen je i telemedicinski servis namenjen dijagnostici na osnovu rezultata sa EKG [15], koji omogućava prenos trenutnog snimljenog EKG pacijenta iz ambulantnih kola u informacioni sistem bolnice, a analizu snimka može da uradi i lekar sa bilo koje lokacije i vam radnog vremena. Servis mogu koristiti i zdravstvene stanice u ruralnim delovima zemlje. Osim za dijagnostiku u kritičnim slučajevima, servis se može upotrebiti i za edukaciju mlađih lekara, kao i za dalja istraživanja. Ušteda se ostvaruje u korišćenju i plaćanju procesorske snage samo kada je to potrebno, kao i u smanjenju izdataka potrebnih za opremanje ambulantnih kola, jer se analiza EKG merenja ne vrše na terenu. Autori rada [16] predložili su servis za teledermatologiju realizovan u oblaku, sa ciljem eliminisanja potrebe za prevoz pacijenta sa teškim povredama u druge institucije radi ispitivanja.



Slika 2. Sistem eZdravlja u oblaku [19]

Osim pomenutih specifičnih rešenja eZdravlja u oblaku koja su razvijena za konkretne zdravstvene ustanove, dostupni su servisi na nivou infrastrukture ili platforme, koji omogućavaju da IT osoblje zdravstvene ustanove dalje razvije aplikacioni nivo za svoje potrebe, a mogu se pronaći i potpuno razvijena rešenja (SaaS). U zavisnosti od provajdera servisi se dele na istraživačke, servise otvorenog koda (*open-source*) i komercijalne. Istraživačka rešenja su realizovana od strane akademskih institucija: *VISION Cloud, EU (IaaS); Midas, EU (PaaS); Celar, EU* (PaaS za intenzivno izračunavanje); *neuGrid, EU* (PaaS za obradu 3D slika mozga, mamograma); *KC class, EU* (PaaS sa posebnih osvrtom na zaštitu podataka pacijenata); *Stratosphere*, Nemačka (PaaS za intenzivno izračunavanje i data mining); *e-Health GATEway to the Clouds*, EU (servis za pretraživanje EHR i pronalaženje svih tekstualnih podataka koji omogućavaju identifikaciju pacijenta, kako bi se ti tekstualni podaci uklonili, što bi omogućilo prenos ostalih podataka iz EHR u oblak radi istraživanja); *An Open Source Cure to Cancer,* Italija (servis koji omogućava objavu podataka u oblaku o pacijentima obolelim od raka, kome mogu pristupiti doktori sa svojim predlozima, bez mogućnosti identifikacije obe strane). *Open-source* im-



Slika 3. Servis za telemedicinu u oblaku [18]

plementacije: *HealthCloud,* firma *ClearHealth,* SAD (SaaS za manje ordinacije), *OpenEMR*, SAD (servis za evidenciju EHR i administracija zdravstvene ustanove, ali klijent mora obezbediti platformu i infrastrukturu). Komercijalni servisi: *EMC Collaborative Healthcare Solutions*, potpuno rešenje zdravstvenog informacionog sistema koje implementira sve standarde *(IHE, HL 7, DICOM*, više detalja o standardnima mogu se pronaći u [4]); *Microsoft Cloud Servicesfor Health* predstavlja mogućnost razvoja servisa za eZdravlje korišćenjem *Microsoft Windows Azure Cloud-a.* (PaaS, nekoliko aplikaciju razvijenih u cilju istraživanja [18]); *Infoway Blueprint,* Kanada (SaaS); *VMware (PaaS); MedScribbler, SAD (SaaS - EHR* sa mogućnošću prepoznavanja rukopisa); *CareCloud,* SAD (SaaS - EHR, zakazivanje, naplata, ako i IaaS za analizu podataka); *HarmoniMD, firma OffSite Care Resources*, SAD (implementacija EHR rešenja u oblaku [19]).

Sami servisi za eZdravlje, koje je potrebno realizovati u oblaku, analogni su postojećim, tradicionalnim servisima. Centralni deo predstavlja servis za upravljanje elektronskim kartonom pacijenta (EHR - lekarski nalazi, laboratorijski rezultati, medicinski tretmani, rentgenski i drugi snimci, itd) i sistem za administraciju medicinske ustanove, koji se sastoji od evidencije pacijenata, medicinskog osoblja, servisa za zakazivanje, prepisivanje lekova, izdavanje lekova, naplatu usluga i drugo, slika 2. Zatim, neophodni su servisi za razmenu podataka između ustanova primarne zdravstvene zaštite, specijalističkih klinika, laboratorija, ustanova za rehabilitaciju i drugih. Potrebno je obezbediti i integraciju servisa telemedicine, slika 3. Takođe, podaci iz svih medicinskih ustanova moraju biti vidljivi pružaocu zdravstvenog osiguranja (Republički fond za zdravstveno osiguranje), nadležnim ministarstvima, kao i istraživačkim centrima.

Bezbednosni rizici realizacije servisa eZdravlja u oblaku razmatrani su u sledećoj glavi.

BEZBEDNOSNI RIZICI

Čest razlog oklevanja pri prelasku na rešenja u oblaku jeste nedostatak poverenja u bezbednost podataka i servisa u takvom sistemu. Rezultati jednog istraživanja iz 2010. pokazali su da, iako je 60% od oko 800 ispitanih kompanija ozbiljno razmišljalo da pređe na rešenja u oblaku, svega 8% njih je zapravo i prešlo, a usled nedostatka poverenja u bezbednost i gubitka kontrole nad svojim podacima [20], Problem je međutim u nedovoljnom razumevanju specifičnosti oblaka. U sopstvenom IKT sistemu institucije naizgled imaju potpunu kontrolu nad bezbednosnim nivoima i proverama; ipak, one u stvarnosti najčešće nemaju dovoljno svesti o izazovima, stručnog znanja niti resursa da angažuju istinske stručnjake pa ta potpuna kontrola ostaje samo neiskorišćeni potencijal. U oblaku, pak, najveći deo bezbednosne kontrole jeste u rukama kompanija koje pružaju usluge u oblaku, ali njima otvoreno tržište diktira visoke bezbednosne standarde kako bi opstali; u isto vreme klijenti i dalje imaju kontrolu nad segmetom koji sami implementiraju - program, platforma ili deo infrastrukture koja je rentirana.

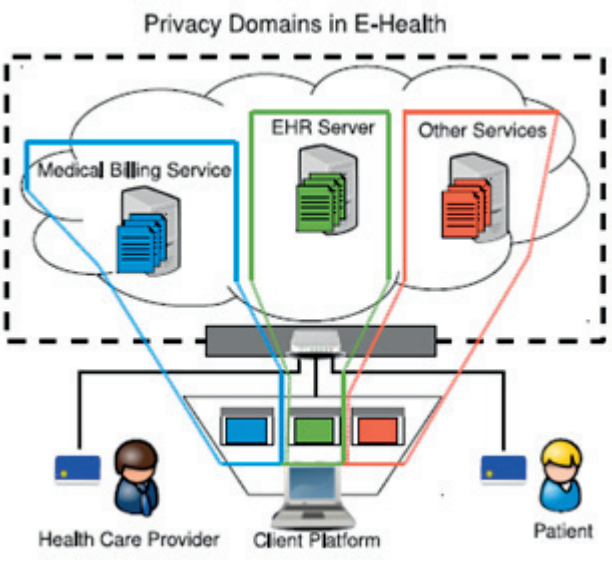
To svakako ne znači da rešenja u oblaku nemaju specifičnih bezbednosnih rizika koji se razlikuju od rizika u tradicionalnim sistemima. Osnovni koncepti informacione bezbednosti zasnivaju se na takozvanom CIA modelu:

Poverljivost predstavlja onemogućavanje pristupa podacima od strane neovlašćenih lica, dok integritet odnosno celovitost daju sigurnost da su podaci tačni i verodostojni. U slučaju sistema eZdravlja u oblaku, potrebno je onemogućiti neovlašćeni pristup osetljivim podacima - pre svega elektronskim zdravstvenim kartonima i ličnim podacima korisnika - u više slojeva:

1) Prava pristupa: Specificikacija prava pristupa i osiguranje kompleksnog sistema korisničkih imena i šifri je odgovornost na strani institucija koje u oblaku postavljaju sopstveni program ili platformu, sem u slučaju javnih oblaka kada su za ovo odgovorne kompanije koje pružaju celokupnu uslugu. Poseban bezbednosni izazov jeste distribuirani pristup centralnom sistemu od strane raznovrsnih krajnjih korisnika - pacijenata, lekara, agenata osiguranja i drugih - koji moraju imati različita prava pristupa. Ldhr, Sadeghi i Winandy [22] predlažu uvođenje virtuelnih domena privatnosti (Trusted Virtual Domains, TVD) u samom oblaku, slika 4.
2) Šifrovanje: Šifrovanje celokupne baza podataka koji su uskladišteni u oblaku je neophodno kako bi, čak i u slučaju neovlašćenog pristupa fajlovima, oni bili beskorisni bez ključa za dešifrovanje. Šifrovanje uskladištenog sadržaja najčešće već rade komercijalni pružaoci usluga u oblaku kako bi podigli nivo bezbednosti i svoju konkurentnost. Pored šifrovanja celokupne baze u oblaku, neophodno je i šifrovanje lokalnog (i privremenog) sadržaja na

uređajima krajnjih korisnika sa kojih se pristupa centralnoj bazi: kompjuterima, laptopovima, pametnim telefonima i tabletima.

3) IKT sistemi i mreže: Bezbednost pojedinačnih komponenti i komunikacione mreže oblaka je u nadležnosti pružaoca usluga koji su tržišno motivisani. Ove kompanije su u mogućnosti da redovna unapređenja (antivirus, zamena opreme, itd) vrše brzo, jeftino i uz minimalni prekid servisa, što nije moguće u slučaju internih IKT sistema van oblaka. Dominanti rizik ovde je u bezbednosti pristupnih tačaka odnosno uređaja sa kojih krajnji korisnici pristupaju: zahtevno je (pa i nemoguće) obezbediti redovnu „kompjutersku higijenu" korisnika poput osvežavanja anti-virus programa, pa postoji rizik od kompromitovanja pristupnih naloga ili uređaja putem virusa i trojanaca. Obrazovanje krajnjih korisnika igra izuzetno važnu ulogu, a sam servis u oblaku tome može doprinese kroz centralizovanu distribuciju edukativnih materijala i principa.



Slika 4. TVD virtuelni domeni privatnosti [22]

4) Transfer podataka: Podaci i pristupni nalozi mogu biti kompromitovani i tokom transfera između komponenata u oblaku kao i na putu od krajnjih korisnika. Pružaoci usluga u oblaku uglavnom su tržišno stimulisani da obezbede šifrovanu komunikaciju između segmenata unutar samog oblaka (uključujući i IPSec VPN veze), ali osmišljavanje i osiguravanje bezbedne komunikacije sa krajnjim korisnicima je uglavnom zadatak institucije.
5) Uklanjanje privatnih podataka: Deljenjenje skladišta podataka koje klijentima na raspolaganje stavljaju komercijalni pružaoci usluga u oblaku povlači i pitanje pouzdanosti uklanjanja podataka prethodnog korisnika pre izdavanja prostora novom korisniku. Idealno bi bilo da se brisanje prethodnih podataka vrši razmagnetisavanjem magnetnih diskova ili uništavanjem optičkih diskova, ali to nije uvek osigurano u oblaku.

Dostupnost odnosno raspoloživost je garancija da se podacima može pristupiti od strane autorizovanih osoba. U slučaju oblaka, ovo se najčešće odnosi na:

1) Gubitak podataka: Kao i u klasičnim IKT sistemima, neophodno je redovno praviti rezervne kopije (*backup*) baza podataka, kako bi se u slučaju havarije podaci mogli brzo vratiti. S obzirom na centralizovanost svih podataka u bazi u oblaku, ovaj postupak je mnogostruko lakši i automatizovan.
2) Nedostupnost podataka i servisa: Decentralizovani pristup centralnom sistemu eZdravlja u oblaku mora biti neometan i moguć u svakom momentu. Nedostupnost e-servisa od nacionalnog značaja - bilo kao posledica havarije ili kiber-napada poput DDoS (*Distributed Denial of Service*) na institucionalnu ili čak nacionalnu infrastrukturu - može doneti velike gubitke [23], Veći pružaoci usluga u oblaku uglavnom su u mogućnosti da obezbede redudantnost sistema pa čak i rezervni sistem u slučaju nepogode (disaster site) na udaljenim lokacijama, što bi bila prevelika i prekomplikovana investicija za samu instituciju.

Izbor nekog od modela oblaka pomenutih u glavi II - javnog, zajedničkog, privatnog ili hibridnog - za određene servise eZdravlja treba napraviti shodno specifičnim rizicima koje nose kao i mogućnostima da se rizici umanje.

Javni oblak u većini slučajeva predstavlja uslugu po principu „sa police", u kojoj institucije mogu da preuzmu „sve ili ništa", i nemaju mnogo mogućnosti za prilagođavanje javno ponuđene usluge svojim specifičnim potrebama niti imaju kontrolu rizika. Bezbednost celokupnog sistema - uključujući i bezbednost podataka u sistemu - u rukama je komercijalnog pružaoca tog servisa u oblaku. Takvi servisi, međutim, mogu biti i te kako od koristi za eZdravlje - kako za internu funkcionalnost sistema poput elektronske pošte, platformi za profesionalno ili društveno umrežavanje ili deljenih opštih dokumenata - tako i za specifične servise usmerene ka pacijentima poput podrške kliničkom odlučivanju (*clinical decision support,* CDS) ili unapređenja javnog zdravlja. Važno je osmisliti upotrebu javnih oblaka tako da se izbegne unošenje ličnih podataka i zdravstvenih kartona, čime se izbegava i bezbednosni rizik.

Zajednički i privatni oblaci se najčešće implementiraju uz zakup usluga oblaka od nekog od komercijalnih pružaoca usluga - bilo na nivou oblaka kao softvera, platforme ili infrastrukture. Ovakav oblik eZdravlja u oblaku pruža najviše mogućnosti za prilagođavanje sopstvenim potrebama institucije i sistema, ali i ostavlja direktnu kontrolu nad bezbednosti sistema u rukama kompanije koja pruža usluge. Pa ipak, rastuće tržište usluga u oblaku i borba za poverenje klijenata neminovno stimuliše kompanije da ponude ozbiljnu podršku bezbednosti sistema i privatnosti podataka klijenata. Pride, nacionalne politike i strategije za informacionu bezbednost sve češće nalažu pojačanu bezbednost celokupnog lanca komercijalnih visokotehnoloških usluga, pa i sertifikaciju [24], Konačno, pojavljuje se sve više međunarodnih standarda za bezbednost u oblaku - poput standarda Alijanse za bezbednost u oblaku (*Cloud Security Alliance*) i američkog Nacionalnog instituta za standarde i tehnologiju (NIST), koje su ponuđači usluga primorani da prate.

I dok institucije ne mogu da imaju direktnu tehničku kontrolu nad bezbednosti u iznajmljenim oblacima, one mogu da se osiguraju kroz vrlo precizne ugovore o servisima (*Service-Level Agreement*) i procedure dogovorene sa pružaocem usluga. Ugovori bi trebalo da sadrže veliki broj detalja, uključujući i detaljnu definiciju servisa, standarde, tehničke i pravne revizije, sveobuhvatne analize stanja i „dužne pažnje" (*due dilligence*), upitnike za redovnu proveru bezbednosti, transparentnost rada i organizacije servisa pružaoca usluge, okvir za upravljanje rizikom (*Risk Management Framework*) u oblaku, procedure za monitoring, mehanizme za pritužbe, ispravke i naknade štete, i drugo. S obzirom da komercijalni pružaoci usluga u oblaku često mogu imati komponente oblaka (npr. servere, i prostor za skladištenje podataka) na različitim geografskim lokacijama pa čak i po različitim zemljama, kao i da i oni mogu iznajmljivati neke komponente oblaka od trećih strana (npr. internet konekciju ili rezervni sistem u slučaju nepogode), geografska razuđenost naizgled centralizovanog sistema može predstavljati pravni izazov. Stoga je važno u ugovoru detaljno definisati tačnu lokaciju podataka (pogotovo elektronskih zdravstvenih kartona), kao i pravnu jurisdikciju u slučaju sporova.

Svakako, moguće je oformiti sopstveni oblak u okviru same institucije - bio on javni, zajednički, privatni ili hibridni. U tom slučaju celokupna infrastruktura i održavanje bili bi u rukama same institucije, bez prenešenog rizika na treću stranu. Ovakav model, međutim, stavlja celokupni teret sistema (oprema, podešavanje, održavanje, bezbednosne procedure i ekspertizu) na samu organizaciju, i time diže kompleksnost realizacije i umanjuje sveopšte ekonomske dobitke.

ZAKLJUČAK

Cloud rešenja za eZdravstvo nude unapređenje sistema zdravstva, pre svega kroz centralizovanu bazu elektronskih zdravstvenih kartona, ali i uštede u IKT opremi, stručnom osoblju i prostoru za opremu i za 2/3 u odnosu na postojeća rešenja. Korišćenje nekih od mnogobrojnih servisa u javnom oblaku, kao i razvoj sopstvenih servisa u zajedničkom, privatnom ili hibridnom oblaku, mogu unaprediti uslugu, omogućiti korišćenje anonimiziranih podataka iz EHR za istraživanja i praćenje zdravstvenog stanja nacije i eventualnih epidemija, povezati udaljene zdravstvene sisteme kao i druge sisteme vezane za zdravstvo poput osiguranja, omogućiti direktniji kontakt pacijenata sa lekarima pogotovo putem mobilnih uređaja i naprednih aplikacija, i aktivnije uključiti krajnje korisnike u brigu o sopstvenom zdravlju.

Pa ipak, uvođenje sistema eZdravlja u oblak sadrži i mnoštvo izazova, i zahteva uvođenje „korak po korak". Shodno servisu i potrebi, neophodno je proceniti obim, efekte tranzicije, kompleksnost prelaska na novi sistem, potrebno vreme, i inicijalne troškove uvođenja servisa u oblaku (uključujući i preko potrebne edukacije kao i operativne troškove) a koji nisu zanemarljivi. Posebnu pažnju treba posvetiti proceni rizika po zaštitu ličnih podataka pacijenata i bezbednost sistema u svakoj od aplikacija, te pravilnom odabiru odgovarajućeg *Cloud* modela i, u slučaju iznajmljivanja servisa u oblaku od komercijalnih ponuđača, svim detaljima ugovora i samog sistema na raspolaganju. Konačno, prilikom uvođenja svakog od novih servisa u oblaku neophodno je imati jasnu viziju mogućih budućih koraka poput uvođenja mobilnih uređaja i aplikacija, perspektivu potrebne skalabilnosti sistema, kao i pristup koji će omogućiti interoperabilnost između segmenata u slučaju korišćenja različitih oblaka ili prelazak sa jednog komercijalnog ponuđača servisa u oblaku na drugi u slučaju potrebe.

LITERATURA

[1] E. AbuKhousa, N. Mohamed and J. Al-Jaroodi, "e-Health *Cloud*: Opportunities and Challenges", Future Internet, vol 4, pp. 621-645, July 2012.

[2] N. Teodosijević, "Iskustva u razvoju IKT sistema u zdravstvenim ustanovama u Srbiji", prezentacija projekta

[3] Prezentacija V nadzornog odbora projekta EU-IHIS, februar 2014.

[4] R. E. Hoyt (2014), Health Informatics - Practical Guide for Healthcare and Information Technology Professionals, 6th ed, Informatics Education.

[5] I. Ivanović, "Zdravstveni informacioni sistem republike Srbije", Institut za javno zdravlje Srbije Dr Milan Jovanović Batut, 2011.

[6] "*Cloud* Computing in Health - White Paper", Canada Health Infoway, 2012.

[7] B. Harris, "5 ways *Cloud* computing will transform healthcare", Healthcare IT News, October 2012.

[8] J. Vilaplana, F. Solsona, F. Abella, R. Filgueira and J. Rius, "The *Cloud* paradigm applied to e-Health", BMC Medical Informatics and Decision Making, vol 13, March 2013.

[9] P. Mell and T. Grance, "The NIST Definition of *Cloud* Computing", NIST Special Publication 800-145, 2011.

[10] P. K. Bollineni, Implications for adopting *Cloud* computing in e-Health, Master's Thesis, School of Computing Blekinge Institute of Technology, Sweden, 2011.

[11] M. Kaplan, "Hybrid *Cloud*s fuel choices for health IT", Healthcare IT News, July 2013.

[12] T. Alford and G. Morton, "The Economics of *Cloud* Computing", Booz Allen Hamilton Inc, 2010.

[13] S. Yoo, S. Kim, T. Kim, R. M. Baek, C. S. Suh, C. Y. Chung and H. Hwang, Economic analysis of *Cloud*-based desktop virtualization implementation at a hospital, BMC Medical Informatics and Decision Making, 2012,

[14] G. F. Cardenosa, I. T. Diez, Mi. L. Coronado and J. J. P. C. Rodrigues, "Analysis of *Cloud*-based solutions on EHRs systems in different scenarios", Journal of Medical Systems, vol 36, pp 3777-3782, December 2012.

[15] J. Hsieh and M.W. Hsu, "A *Cloud* computing based 12-lead ECG telemedicine service", BMC Medical Informatics and Decision Making vold 12, 2012.

[16] A. Mahapatra and M. Dash, "Design and Implementation of a *Cloud* based TeleDermatology System", International Journal of Engineering Research & Technology (IJERT), vol 2, February 2013.

[17] T. Mustonen, "The SUCRE State of the Art Analysis: *Cloud* solutions in the Healthcare Sector", SUCRE (SUpporting *Cloud* Research Exploitation) project report, January 2013.

[18] S. Lu, P. Strazdins and R. Ranjan, "Reporting an Experience on Design and Implementation of e-Health Systems on Azure *Cloud*", Submitted to third IEEE International Conference on *Cloud* and Green Computing, 2013.

[19] J. Thompson, "Manila hospital implements *Cloud*-based EHR", Healthcare IT News, April 2012.

[20] "*Cloud*y with a chance of rain", The Economist, March 2010.

[21] M. Stamp, "Information Security: Principles and Practice", John Wiley & Sons, Inc., New Jersey, pp. 3-4, May

[22] H. Lohr, A.R. Sadeghi, M. Winandy, "Securing the E-Health *Cloud*", IHI '10 Proceedings of the lst ACM International Health Informatics Symposium, pp. 220-229, 2010.

[23] V. Radunovic, "DDoS - Available Weapon of Mass Disruption", Proceedings of the 21st Telecommunications Forum (TELFOR), pp.5-9, November 2013.

[24] V. Radunovic, "Pacifizam u kiber-prostoru: zašto je za kiberbezbednost važnija saradnja među sektorima i akterima nego njegova militarizacija," Zborniku sa konferencije Informaciona bezbednost 2013, Beograd, 2013.

THE EHEALTH *CLOUD* AND SECURITY ISSUES

Abstract:
The introduction of the Electronic Health Records enabled advanced search capabilities comparing to those with the traditional hard-copy records, simplified the illness history tracking, and ensured a creation of a large research database. The pool of collected data enables an insight into the diagnosis of symptoms, treatments undertaken and the effects of the medicines prescribed, but can also be used to develop a system that would assist the doctors with clinical decisions.
Development of *Cloud* computing solutions has opened the question of a transition of e-Health services into a *Cloud*. Health institutions can significantly cut the costs of servers and equipment needed for the development of own software solutions, as well as for the space needed to place the IT equipment. Besides, number of technical staff required for the maintenance of a clinical information system can be reduced. Patients' data, stored in databases of geographically dispersed health organisations, become available for various statistical analyses, enabling an insight into the health condition of the population and the issuing of early warnings in case of the epidemics. At the same time, the security of personal records and the health system is being handed over to *Cloud* service providers, which simplifies the maintenance but also reduces the control over security and privacy of the sensitive data.
The paper analyses the architecture of *Cloud* services implemented in e-Health solutions, the economic aspects of the introduction of *Cloud* e-Health solutions, as well as the challenges related to security of the service and patients' data in the *Cloud*.

Key words:
Cloud,
e-Health,
Security,
Data protection.