Sigurnosni problemi u Cloud computing rešenju

Predrag Alargić, Tanja Kaurin
Fakultet za pravne i poslovne studije dr Lazar Vrkatić
Novi Sad, Srbija
predrag.alargic@fpps.edu.rs, tanja.kaurin@useens.net

Sadržaj—**Potreba za konstanim povećanjem efikasnosti uz potencijalno smanjenje troškova na ICT resurse čini da koncept Cloud computing-a postaje sve zastupljeniji. Tehnološke prednosti, brži i jednostavniji pristup deljenim resursima uz različite modele isporuke su samo neke od prednosti koje ovaj koncept čine izuzetno atraktivnim. Povećanje potražnje za Cloud computing servisima nameće potrebu za hitnim rešavanjem sigurnosnih problema koji su u vezi sa pristupom ponuđenim servisima ali i samim podacima. U ovom radu, uz kratak osvrt na osnovna Cloud computing rešenja, analiziramo bezbednosne pretnje koje ugrožavaju pouzdanost kao i načine za njihovo prevazilaženje.**

Ključne reči 1; Cloud computing 2; sigurnosni aspekti

I. UVOD

Pored toga što je razvoj bezbednosnih sistema u standardnom informacionom sistemu veoma komplikovan, u Cloud computing rešenjima predstavlja dodatni nivo rizika, jer usluge koje pruža nisu dostupne samo nama već i nekom drugom. Pored unutrašnjih, postoje i spoljašnji aspekti dostupnosti što dodatno otežava održavanje jedinstva, privatnosti i poverljivosti podataka, podršku podataka i dostupnost servisa.

Cloud computing kontrolu nad podacima premešta sa klijentske organizacije na cloud provajdere, gotovo na isti način na koji organizacije povere deo svojih IT poslovanja spoljnim preduzećima. Osnovni zadaci, koji se ogledaju u primeni sigurnosnih zakrpa ali i samo podešavanje sigurnosnog, odnosno zaštitnog zida, kao dodatna usluga može postati odgovornost pružaoca Cloud computing usluga, a ne korisnika. Kao rezultat toga, korisnik mora da uspostavi odnos poverenja sa pružaocem Cloud computing usluge i da bude svestan rizika da njegov pružalac izvršava, primenjuje i upravlja bezbednosnim opcijama umesto samog korisnika. Ovakav odnos između pružaoca Cloud computing usluge i korisnika je poznat i kao usluga od poverenja, ipak klijenti su i dalje u krajnjoj liniji odgovorni za istinitost podataka, ali i za zaštitu svojih važnih podataka, iako je ovo odgovornost pružaoca usluge Cloud computing rešenja. U skorije vreme, neki veliki poslovni sistemi biraju privatne ili hibridne modele Cloud computing rešenja umesto javnih i to samo zbog rizika koji su u vezi sa spoljnim servisima.

Još jedan od aspekata sigurnosti o Cloud computing rešenjima takođe zahteva veliko preispitivanje sigurnosti i rizika. Unutar Cloud computing rešenja, teško je je tačno odrediti mesto gde su podaci uskladišteni. U tradicionalnom pristupu računarstvu bezbednosni i sigurnosni procesi su nekada bili vidljivi a sada su skriveni iza izdvojenih slojeva. Ovaj nedostatak vidljivosti može dovesti do ne poverenja, odnosno do više sigurnosnih i problema istinitosti.

II. CLOUD COMPUTING

Postoji više definicija Cloud computing rešenja. Kao prva definicija izdvaja se Gartnerova definicija: "To je skup disciplina, tehnologija i poslovnih modela koje se koriste da isporuče IT mogućnosti (softver, platformu i hardver) po zahtevu, da bude skalabilna i elastična usluga".[1]

Kao druga definicija Cloud computing rešenja, nameće se definicija Američkog Nacionalnog instituta za tehnologiju i standarde (NIST) koja glasi: "Cloud computing je model koji omogućava jedinstven, precizan pristup deljivim računarskim resursima koji mogu da se konfigurišu (mreže, serveri, skladišta podataka, aplikacije i usluge) i mogu na zahtev, brzo da se realizuju uz minimalne resurse i uz minimalnu interakciju sa pružaocima usluga".[2]

Za razliku od tradicionalnog pristupa računarstvu gde se podrazumeva kupovina programa, u Cloud computing rešenjima poslovni sistem plaća samo naknadu za korišćenje. To znači da umesto dosadašnje kupovine kompletnog računarskog sistema i rešenja, korisnik koristi informacione tehnologije kao uslugu. Sistem integratori, odnosno administratori računarskih sistema se pojavljuju kao „outsorcing" partneri, odnosno kao servis integratori za pružanje ugovorom unapred određenih internih i eksternih usluga koje korisnici plaćaju na mesečnom nivou. Svrha ovakvog načina pružanja usluge je da se kompanije bave onim što najbolje rade, a da poslove oko informacionih tehnologija prepuste onim kompanijama koje to najbolje rade, čime se smanjuju kapitalna ulaganja i postiže bolji efekat.

U narednim godinama se očekuje dvocifreni rast Cloud computing rešenja, prema Gartnerovom predviđanju očekuje se da čak 30% preduzeća do 2015. godine promeni namenu korišćenja IT resursa. Privatni korisnici za sada koriste Cloud

computing samo za čuvanje fajlova ili korišćenje vebmejla. Uopšteno, sve aplikacije koje se koriste na PC računarima bi trebalo ubuduće da se dobijaju kao usluga preko Cloud computing rešenja.

IBM koristi novorazvijenu cloud računarsku platformu koja nastoji da drastično smanji vreme potrebno za isporuku Cloud computing usluge. Platforma je razvijena tako da selekcija i implementacija Cloud computing usluga bude vrlo jednostavna a da se ujedno postižu vrhunske performanse i dostupnost raspoređivanjem skladištenja, mrežnih resursa i servera za korisničku primenu bez ljudskog dodira .[3]

U Srbiji se može naći široka paleta usluga u tom domenu. U toj oblasti značajna je saradnja zasnovana na VMW-are rešenjima. Telekom Srbija (zahvaljujući prisutnosti u regionu u Crnoj Gori i BiH) ima oko devet miliona pretplatnika i kao provajder signala mobilne telefonije, ali i širokopojasnog Interneta, idealni je partner. Uočena je poslovna potreba za javnim i privatnim cloud rešenjima koja nude fleksibilno korišćenje virtuelne infrastrukture, iznajmljivanje virtuelnih servera, odnosno serverskih i korisničkih aplikacija ili čitave platforme. Elementi ove usluge podrazumevaju povezivanje sa lokacijom infrastrukture sistema Cloud computing kompanije, pristup virtuelnim desktop i/ili serverskim uređajima, kreiranje i podešavanje virtuelnih elemenata po želji korisnika, kao i instalaciju i podešavanje odgovarajućih aplikacija. Uslugu prirodno prate i sistemi za podršku sigurnosti podataka, kao i mehanizmi za oporavak sistema od pada.

Usluge Cloud computing rešenja mogu da se svrstaju u pet kategorija.

- Osnovna infrastruktura: predstavlja virtuelizovani softverski sistem pomoću koga korisnici pokreću svoje aplikacije. Postoji minimalni veb standard koji se odnosi na postojanje sistemskog infrastrukturnog sloja.

- Softverska infrastruktura: predstavlja niz usluga koje se nalaze u paraleli sa tradicionalnim razvojnim tehnologijama. Sve pomenute usluge moraju posedovati ili koristiti arhitekturu koja se oslanja na veb tehnologije, a ujedno moraju i da poseduju izgled i dizajn kakav se traži u svetu.

- Programi: moraju pružati isporuku na globalnom nivou, preko arhitekture koja je bazirana na vebu ka veb pretraživačima ili ka programskim uslugama u Cloud computing rešenju. Sve ovo spomenuto predstavlja kreiranje arhitekture koja može da podrži više firmi.

- Poslovni procesi: poslovni proces sam za sebe se isporučuje kao Internet usluga.

- Upravljanje bezbednošću: se smatra uslugom koja obezbeđuje pristup, korišćenje i isporuku na svim nivoima usluga Cloud computing rešenja.

Cloud computing rešenja koja se primenjuju kod nas bazirana su na nekom od navedenih modela.

- Javna Cloud computing rešenja – su javno dostupni servisi koje provajderi cloud rešenja nude bilo kom korisniku preko Interneta.

- Privatna Cloud computing rešenja – su informacione mogućnosti kao usluga koju pružaoci cloud rešenja nude određenoj, odnosno izabranoj grupi korisnika. Pružaoci usluga cloud rešenja mogu da budu organizacije (jedna organizacija se pojavljuje i kao potrošač i kao pružaoc usluge) ili neka treća strana. Pružaoc koji nudi uslugu može da bude javni Internet ili privatna mreža, ali pristup mreži omogućen je samo autorizovanim korisnicima.

- Interno Cloud computing rešenje - skup privatnog cloud rešenja i internog cloud rešenja a ujedno je i IT rešenje koje se nudi kao usluga preko organizacija koje pružaju IT uslugu kako bi se lakše odvijalo poslovanje.

- Spoljašnje Cloud computing rešenje - predstavlja mogućnost koja se nudi kao usluga u poslovanju čiji resursi se ne nalaze u vlastitoj IT organizaciji. Spoljašnja cloud computing rešenja mogu biti javna ili privatna.

- Hibridno Cloud computing rešenje - jeste kombinacija javnog i privatnog *cloud-a* se oslanja i na unutrašnje i na spoljašnje IT resurse.

III. PRAVNE OBAVEZE

Period koji je iza nas obeležili su pokušaji da se precizno, pravno definišu pojmovi vezani za Cloud computing, kako bi se zaštitili pružaoci ali i primaoci usluge Cloud computing rešenja. Model koji se nameće kao moguće rešenje nije nov. Ukoliko se upotrebi model obračuna telefonskih usluga, možemo koristiti neke od opcija koje potpadaju pod današnji pravni okvir usluga Cloud computing rešenja. Stubovi ovog modela su: pravo da se vlasništvo nad sistemom zadrži, upotreba i kontrola nečijih vlastitih podataka, pravo na ugovor koji se tiče nivoa pruženih usluga koji nedvosmisleno određuje vlasništvo, načine i procedure za otklanjanje grešaka u uslugama i posledice, pravo i obaveza pružaoca usluge Cloud computing rešenja da obavesti korisnika usluge o promenama koje utiču na poslovne procese korisnika, pravo spoznaje pravnih okvira nadležnosti u kojima pružalac usluge obavlja svoje poslovanje, pravo da se zna koje bezbednosne procedure pružalac usluge Cloud computing rešenja poštuje i koristi. Cloud computing rešenje nosi sa sobom karakteristične rizike koji mogu da uspore prilagođavanje poslovnih sistema. Kao rezultat toga veliki broj javnih usluga koje pruža Cloud computing rešenje funkcioniše na isti način za sve potrošače (možemo reći da su svi ugovori tipski). Pretvaranje ove usluge u robu široke potrošnje (poznato kao komodizacija) uvodi rizike za potrošače, koji imaju malo moći u slučaju da pružaoci usluge ne isporuče uslugu koju su obećali. Da bi gore pomenuti rizici bili smanjeni, pružaoci Cloud computing rešenja i korisnici usluga moraju da se dogovore i da postave zajedničke ciljeve. Kada se usluge Cloud computing rešenja dovedu u operativni nivo poslovanja korisnika, pružalac usluge bi trebalo da ponudi bolje garancije korisniku, a naročito u delovima koji se tiču vlasništva nad podacima ali i u tehničkom domenu usluga. Danas pružaoci Cloud computing rešenja variraju u nivou usluga koje nude, a često ne nude zaštitu u celini.

IV. BEZBEDNOST U CLOUD COMPUTING OKRUŽENJU

IT infrastruktura organizacije je postala veoma teška i kompleksna za zaštitu, pogotovo što se bezbednost zanemaruje u trci za maksmalnim iskorišćavanjem potencijala Interneta. U 2012. godini broj novih virusa bio je veći nego za prethodnih dvadeset godina, da bi taj broj bio nadmašen već u prvoj polovini 2013[4]. Zbog toga se IT organizacije suočavaju sa velikim izazovom, s obzirom da se posao sve više oslanja na Internet. Sudeći po WASC-u , više od 87% Internet aplikacija je ocenjeno kao veoma ranjivo[5]. Kao moguće rešenje ovog problema javljaju se bezbednosni servisi bazirani na Cloudu, koji pružaju inovativan pristup zaštiti podatak a organizacije, dodajući globalno raspoređeni sloj odbrane. Ovaj sloj čini razliku u odnosu na centralizovane sisteme i znatno povećava nivo odbrane. Cloud bezbednosna rešenja dozvoljavaju kompanijama da se prilagode rizicima koji se konstantno menjaju, unapred izbegavajući predviđene rizike.

Podaci koji su osetljivi sve češće su dostupni na vebu, hostovani na Cloud baziranim servisima. U ovom dinamičnom i distribuiranom okruženju, mentalitet konvencionalne odbrane ne pruža dovoljne sigurnosne paradigme. Umesto toga, poslovni sistemi treba da prihvate distribuiranu prirodu Cloud computing rešenja, koristeći njene razmere i fleksibilnost u svoju korist prilikom sprovođenja strategije odbrane u dubinu. Odbrana u dubini podrazumeva razvijanje preklapajućih bezbednosnih slojeva koji koriste različite taktike zaštite protiv pretnji.

Skoro deceniju, softverske kuće koje se bave proizvodnjom sigurnosnih mehanizama čine Internet boljim, bržim i sigurnijim mestom za poslovanje. Veliki broj kompanija se oslanja na isključivo softverska rešenja kako bi osigurale i ubrzale svoje online transakcije, koristeći platformu koja obezbeđuje sigurnost na ivicama Cloud computing rešenja. Edge Platforma, kako se drugačije zovu rešenja koja se oslanjaju na mehanizme koji se nalaze na ivicama Cloud computing rešenja je dokazana platforma za pružanje inteligentne i skalabilne odbrane koja štiti od širokog spektra napada, bio to napad na DNS infrastrukturu organizacije, mrežni sloj ili internet aplikaciju. Obiman i fleksibilan skup sposobnosti može se prilagoditi različitim vrstama pretnji i napada na zahtev. Softverska rešenja omogućavaju korisnicima da u potpunosti uživaju u mogućnostima Cloud computing rešenja, održavajući kontinuitet poslovanja.

DDos napadi (eng. „Distributed Denial of Service“) su jedno od vizuelno najrazornijih oružja u sajber prostoru danas, jer parališu sistem preplavljujući ciljane delove infrastrukture nelegitimnim saobraćajem[6]. Avgusta 2009. napadi na Twitter, Facebook i Google privukli su veliku medijsku pažnju, ali je manje poznato da su i mnoge poslovne i državne organizacije iskusile iste napade. Posledice uspešnog napada mogu biti ne samo gubitak resursa i prihoda i poremećaj produktivnosti poslovanja, već i narušavanje ugleda brenda i gubitak poverenja kod korisnika. Podatak da je 2008. bilo 190.000 DDoS napada je već dovoljno obeshrabrujući, a kada se zna da su se najveći napadi za sedam godina ustostručili (sa 400 Mbps u 2001. na 40 Gbps 2007.), postaje još očiglednije koje su razmere ovog problema. Tako se, recimo, 4. Jula 2009. Vlada SAD suočila sa napadom koji je stizao sa 300.000 različitih IP adresa, napadajući istovremeno više sajtova saobraćajem stostruko većim od normalnog. Jedan od napadnutih sajtova je tog dana imao saobraćaj za koji bi mu u normalnim uslovima trebalo osam godina. DDoS napadi predstavljaju izazov, ne samo zbog veličine već i zbog raznolikosti. Ne postoji magično rešenje, ali najbolji pristup je višeslojni koji zavisi od specifične prirode napada.

Tačke koje treba identifikovati prilikom DDoS napada su :

- Da li napad dolazi od malog broja IP adresa ili iz određenog dela sveta;
- Da li je direktan ili reflektovan napad;
- Koji deo infrastrukture je napadnut;
- Koji sloj je ranjiv i na koji način je to iskorišćeno?

Raznolikost DDoS napada je ono što ih čini neodbranjivim tradicionalnim načinima odbrane. Strategije koje treba uzeti za ublažavanje DDoS napada su :

- Premeštanje centralizovane infrastrukture

Premeštanje centralizovane infrastrukture na Cloud platformu omogućava dodatni sloj zaštite povećavajući time generalnu skalabilnost i robusnost. Sa napadima se obračunava na obodima interneta, držeći ih podalje od infrastrukture jezgra. Potrebno je konfiguristati servere da prihvataju i prosleđuju samo validne HTTP/S zahteve ka izvoru. Ovaj pristup takođe obezbeđuje dodatno vreme za praćenje i analizu napada kako bi se obezbedile dodatne protivmere.

- Skrivanje izvora

Postiže se sakrivanjem od javnog Interneta. Sve zahteve krajnjih korisnika je potrebno filtrirati, tako da samo pouzdani serveri mogu da komuniciraju direktno sa izvornim serverom. Na ovaj način smanjuje se rizik od opasnosti po mrežni sloj.

- DNS zaštita

Predstavlja bitan sloj odbrane. DNS infrastruktura je kritična za sajt jer prevodi imena sajtova u IP adrese na kojima se sajtovi nalaze. DNS infrastruktura je najčešće i najslabija karika u mrežnoj strukturi poslovnog sistema. Mnogi poslovni sistemi se oslanjaju na samo dva ili tri DNS servera, što ih čini lakim plenom za DDoS napade.

Prebacivanje podataka na drugi server u toku napada može minimizirati negativne poslovne efekte. Jedan od mogućih rešenja jeste da se višak korisnika pošalje na alternativni sadržaj.

Jedna od najvećih prednosti visoko distribuirane arhitekture bazirane na Cloud computing rešenjima jeste sposobnost da brzo pokrene ciljane odbrambene tehnike sekući napade odmah kod izvora. Softverska rešenja, dostupna na tržištu, nude širok spektar mera za specifične situacije:

- Blokada ili preusmeravanje zahteva sa određene geografske lokacije;
- Autorizacija, odbijanje ili preusmeravanje saobraćaja na osnovu karakteristika kao što su brauzer ili jezik;

- Korišćenje sporih odgovora za isključivanje mašina koje napadaju;
- Preusmeravanje saobraćaja sa servera ili regija pod napadom;
- Ograničavanje stope po kojoj se zahtevi prosleđuju izvornom serveru;
- Smeštanje sumnjivog saobraćaja na mali broj servera;
- Provera kukija kako bi identifikovali preveliki broj novih korisnika;
- Slanje ilegalnog saobraćaja nazad ka mašinama koje ga iniciraju.

V. ODBRANA APLIKATIVNOG SLOJA

Sofisticiraniji napadi zaobilaze tradicionalni firewall i napadaju aplikativni sloj Internet aplikacije na portovima 80 i 443 koji su ostavljeni bez restrikcija u firewall zbog HTTP i HTTPS saobraćaja. Tehnike kao što su XSS, korišćenje prelivanja bafera i SQL ubacivanje se koriste prilikom napada na aplikativni sloj. Softverska rešenja odbranu aplikativnog sloja rešavaju pomoću WAFa (eng. Web Application Firewall). Krećući se po ivicama interneta softverska rešenja otkrivaju i blokiraju sav zlonameran saobraćaj iako su konfigurisana pravila za proveru protokola, input validaciju, bot i trojan identifikaciju i detekciju SQL curenja. Problem sa kojim se susreću trenutna softverska rešenja su kako razlikovati saobraćaj ka aplikacionom sloju od legitimnog saobraćaja, jer se prikazuje kao normalni veb aplikacioni zahtev.

S obzirom da je veličina i sofisticiranost Internet pretnji sve veća, poslovni sistemi moraju biti na oprezu prilikom zaštite digitalne infrastrukture i resursa. Efektna zaštita zahteva duboko odbrambeni pristup koji tradicionalnom dodaje prsten odbrane u vidu Cloud computing rešenja. DDoS napadi su samo jedan od primera sa čime se sve poslovni sistemi suočavaju, što ukazuje na stepen rizika kojem su svakodnevno izložene kompanije sa centralizovanim odbrambenim sistemom[7].

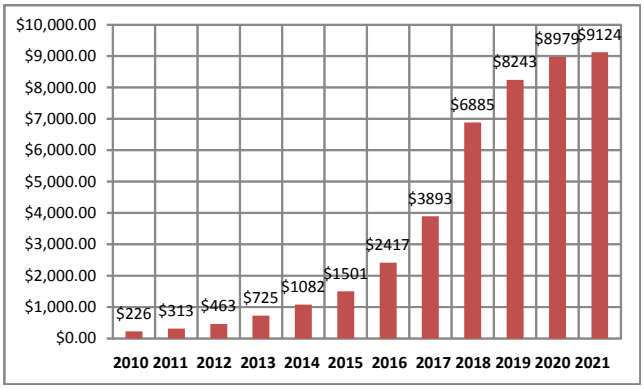
Tršište bezbednosnih rešenja za Cloud computing je tržište koje raste, ali je relativno malo u odnosu na ukupno tržište bezbednosti računara. Godine 2010-te Cloud computing bezbednosna rešenja su činila svega 2-3% ukupnog tržišta bezbednosnih softvera za računare. Predviđa se da Cloud computing bezbednost, uključujući SaaS, nadmašuje ukupno tržište bezbednosti i da će se povećati u veličini proporcionalno celini. Technavio Analysis procenjuje da će tržište bezbednosnih rešenja za Cloud computing u 2014. godini činiti 4% ukupnog tržišta bezbednosti računara. Štaviše, Forester predviđa da će 2015. godine tržište bezbednosnih rešenja za Cloud computing dostići vrednost od 1,5 milijardi, 5-6% ukupnog tržišta bezbednosti računara.

Ovakav uvid u istraživanja i predviđanja eminentnih institucija ukazuje na brz rast Cloud computing bezbednosti u odnosu na ukupno tržište. Na osnovu analize Cloud computing rešenja, brzog prihvatanja njegovog korišćenja, kao i kontinuiranog poboljšanja bezbednosti, moguće je da će tršište bezbednosnih rešenja za Cloud computing dostići 12% do 2018. i 20% do 2021. godine.

VI. RAZVIJANJE TRŽIŠTA BEZBEDNOSTI

Predviđanja o rastu tržišta bezbednosnih rešenja za Cloud computing su zasnovana na procenama vodećih istraživačkih kompanija kao što su Forbes, Forrester, and Gartner. Slika 1. predstavlja spajanje njihovih predviđanja, pokazuje koliko će kompanije trošiti novca na Cloud computing bezbednosna rešenja do 2021. godine. Vrednosti su date u milionima dolara. Rast tržišta je stabilan od 2010. godine, u proseku između 35 i 45% rasta svake godine, i nastaviće tim tempom do 2015. godine. Posle 2015. godine se očekuje da se rast poveća na oko 50% godišnje do 2020. godine. Nakon toga se očekuje da će se rast tržišta bezbednosnih rešenja za Cloud computing značajno usporiti[8].

Rast tržišta će se usporiti zbog nekoliko faktora. Prvo, većina poslovnih sistema koja želi da bude u Cloud sistemima će do 2020. god. na neki način već biti tamo. Drugo, SECaaS (eng. Security as a Service) će pružati dovoljno bezbednosnih proizvoda za rešavanje većine bezbednosnih problema do 2020.god. Dalje, bezbednost Cloud computing rešenja je u fokusu profesionalnih i akademskih istraživanja čime se ubrzava zrelost tržišta bezbednosti. Konačno, ukupno tržište Cloud computing rešenja će početi da sazreva oko 2020. Godine.



Slika 1. Tržište Cloud computing bezbednosnih rešenja

VII. ZAKLUČAK

Zaštita podataka je osnovni princip informacione bezbednosti. Sve rasprostranjene informacije bezbednosnih propisa i standarda, zahtevaju da osetljive informacije budu zaštićene na adekvatan način kako bi se očuvala poverljivost. Tajnost tih podataka je potrebna bez obzira gde da se podaci nalaze u lancu nadzora, uključujući i cloud okruženja.

Infrastruktura deljenja poziva na visok stepen standardizacije i automatizacije procesa što može poboljšati sigurnost eliminišući rizik od greške operatera i previda. Međutim, rizici nerazdvojni od masovne deljene infrastrukture znače da Cloud computing modeli moraju i dalje naglasiti značaj izolacije, identiteta i istinitosti.

LITERATURA

[1] Kočović, P. : "Osnovi primene kompjuterske tehnike", Fakultet za obrazovanje rukovodećih kadrova u privredi, Beograd 2010, Unpublished

[2] NIST Tech Beat : "Final Version of NIST Cloud Computing Definition", October 25, 2011, Published

[3] Chan,W., & Pili, H. : "Cloude computing: Preparing for future", Technology risk, Crowe Horwath, 2010, Published

[4] Symantec Corporation : "Internet security threat report", 2013, Published

[5] WASC Announcement : "Static Analysis Technologies Evaluation Criteria", 2013, Published

[6] The Department of Homeland Security's United States Computer Emergency Readiness Team : "Understanding Denial-of-Service Attacks", November 04, 2009, Unpublished

[7] MarkoTalijan : „Internet ogledalo", 2010.

[8] David Munyaka, Burman Noviansyah, Vibhor Goel, Andrew Yenchik, Steve Durham : "Cloud Computing Security", Telecommunications Management, 2012.

ABSTRACT

Constant efficiency increase requirements coupled with ICT resources potential cost reductions make the cloud computing concept becoming ever more present. Technological advantages, much quicker and easier shared resources access along different delivery channels are just some of the concept's extremely attractive preferences. Increasing cloud computing services demand brought upon urgent security issues resolution requirements related to offered data and services access. The present paper shall, along with brief cloud computing solutions overview, analyze the reliability jeopardizing security threats and ways of overcoming them.

CLOUD COMPUTING SOLUTION SAFETY ISSUES

Predrag Alargić
Tanja Kaurin