# POREĐENJE FORENZIČKOG POSTUPKA CLOUD OKRUŽENJA U ODNOSU NA DRUGE IZVORE PODATAKA

Jovana Samardžija*,
Bojan Bucalo,
Saša Adamović

Univerzitet Singidunum,
Beograd, Srbija

Rezime:

Cloud je jedan od bitnih napredaka u informacionim tehnologijama, koji pruža promene u kompjuterskim aktivnostima i pruža mnoštvo tehničkih i ekonomskih prilika. Mada se i dalje dosta korisnika ne usuđuje da svoje podatke postavlja na Cloud-u zbog same činjenice da je nešto nepoznato, kao i briga za samu sigurnost podataka. Razlika između klasične forenzike, recimo mobilnih uređaja, i Cloud-a je ta što je za forenziku mobilnih uređaja potreban sam fizički uređaj i pristup istom, dok sama decentralizacija Cloud-a to olakšava. U ovom radu će biti obrađeno da li je moguće vratiti podatke koji su održivi, kao i one koji su neodrživi. Biće prikazani problemi u samoj forenzici Cloud-a, kao i određena rešenja za iste uz pomoć analitičarima da bolje razumeju razlike primene koraka digitalne forenzike na podacima koji se nalaze na Cloud-u i one koji se nalaze na fizičkim uređajima.

Ključne reči:

forenzika Cloud, digitalna forenzika, sigurnost, forenzički alati, digitalni dokaz.

## 1. UVOD

Otkrivanje dokaza u forenzici Cloud-a je drugačije nego u tradicionalnoj forenzici jer ne postoje specifični alati za nju, ali postoji mnogo više pravnih regulativa jer se ne radi o fizičkom uređaju, i dokazivanje integriteta i autentičnosti je otežano. Podatak može biti vraćen od strane istraživača i provajdera, i u zavisnosti od toga kako je podatak prikupljen određuje se samo vraćanje podataka, kao i kako će biti prihvaćen na sudu kao digitalni dokaz. Tome najviše doprinosi činjenica da se u vlasništvu same korporacije ne nalazi infrastruktura Cloud-a, već se nalazi kod provajdera i određene zakonske regulative otežavaju taj proces odlučivanja ko će prikupljati podatke [8].

Cloud mogu da koriste pojedinci, korporacije i servis, a po istraživanjima [1] očekuje se rast tržišta od 30% do 2020. godine, dostižući vrednost od 270 milijardi dolara godišnje. Takođe, omogućuje da korisnik može da iznajmi usluge nad operativnim sistemom koji se nalazi na virtualnoj mašini, da koristi njegovu brzinu, fleksibilnost i pokretljivost jer može da joj se pristupi u bilo kom trenutku sa bilo kog mesta, dok sa druge strane provajder, odnosno dobavljač usluga, ima kontrolu nad fizičkim delom hardvera na koji je vezana ta virtualna mašina preko

Odgovorno lice:
Jovana Samardžija

e-pošta:
jovana.samardzija.17@singimail.rs



DOI: 10.15308/Sinteza-2018-38-43

Cloud servisa. Zbog tih usluga se povećava korišćenje samog Cloud-a od strane korporativnih organizacija, obrazovnih i vladinih institucija. Srazmerno povećanjem korišćenja Cloud-a u dobre namere povećava se i zlonamerna upotreba od strane napadača. Jednostavan proces registracije korisnika i neograničene računarske usluge koriste mnogi napadači kako bi izvršili krivična dela, i kada se izvrše jednostavno se samo odjave sa naloga.

U ovom radu biće obrađeno koliko se sam proces digitalne forenzike razlikuje od forenzike Cloud-a, koje su tehničke poteškoće i koji su predlozi rešenja.

## 2. CLOUD FORENZIČARI

Veliki broj forenzičara se složio da je teško prikupiti validne podatke u forenzici Cloud-a iz razloga što ne postoje alati koji mogu da urade forenziku na daljinu.

Istražitelji Dikstre i Shermana, 2012 [2] su ilustrovali kako mogu da se povrate podaci forenzikom na daljinu, ali sa manom da ti podaci mogu da budu veoma nepoverljivi, dok su Martini i Choo [6] predložili da se forenzika Cloud-a vrši tako što se preuzima slika virtuelnog diska proizvedena od virtuelnog diska mašine, ali ne postoji mogućnost da se izračuna *hash* vrednost preuzete slike i originala da bi se potvrdio integritet. Osim same slike diska, istražitelji koriste metapodatke i sistemske zapise da bi rekonstruisali zločin.

## 3. TEHNIČKE KARAKTERISTIKE

Ovde će biti obrađen sam Cloud sa svim njegovim različitim servisima i razvojnim modulima, kao i pojam digitalne forenzike i forenzike Cloud-a uz objašnjenje forenzičkih procesa.

*Cloud platforma*

Platforma za Cloud može da se definiše kao model za praktičan pristup mreži na zahtev koji poseduje veliki opseg konfigurisanih računarskih resursa, koje se tretiraju kao usluge i bivaju fakturisane prema korišćenju. Korisnik tim uslugama može da pristupi u bilo kom trenutku sa bilo kog mesta, preko bilo kog veb pregledača koji ima pristup internetu.

Prednosti platforme za Cloud:

- elastičnost: prilagođavanje potrebama kupca u broju računara, kao i u njihovoj konfiguraciji;
- povezivanje: mogućnost povezivanja na platformu bilo kada i bilo gde;
- vidljivost: mogućnost korisnika da imaju potpuni uvid u svoje podatke i u to kako su raspoređeni;
- naplata: mogućnost merenja korišćenja usluga i pravilna naplata po korišćenju.

Zbog dosta prednosti koje nosi Cloud, podstaknut je njegov drastični rast u proteklih par godina i kroz to su se odvojili načini pružanja usluga [9]:

- javni Cloud: računarska infrastruktura je dostupna preko interneta i svi su u mogućnosti da je koriste tako što sam vlasnik na virtualnom serveru dodeli IP adresu korisniku i tako prodaje Cloud usluge;
- privatni Cloud: isključivo u vlasništvu jedne organizacije, nalazi se iza više nivoa zaštite, organizacija ima uvid u svoje računarske resurse i svoje usluge dodeljuje ograničenom broju korisnika;
- Cloud u zajednici: sličan je privatnom Cloud-u, samo što ga umesto jedne organizacije koristi više organizacija koje poseduju određene sličnosti u vidu sigurnosnih pravila i regulativa;
- hibridni Cloud: kombinacija javnog i privatnog, u situacijama kada organizacija želi da zadrži za sebe određene aplikacije pa ih čuva u privatnom, ali su onda te aplikacije povezane na aplikacije koje se nalaze na javnom Cloud-u da bi unapredile njihove funkcionalnosti;
- distributivni Cloud: njegove usluge su raspoređene na nekoliko mašina koje sa nalaze na različitim lokacijama, ali su povezane na istu mrežu.

Vrste servisnih modela Cloud-a:

- softver kao usluga (Software-as-a-Service – SaaS): podrazumeva da korisnik plaća da bi dobio pristup aplikaciji koja se nalazi na serveru, i da može slobodno da je koristi, bez da mora da vrši neke modifikacije nad njom ili da poseduje specifičan hardver;
- platforma kao usluga (Platform-as-a-Service – PaaS): znači da korisnik iznajmljuje operativni sistem ili veb server i sa njim posluje;
- infrastruktura kao usluga (Infrastructure-as-a-Service – IaaS): omogućava korisniku da može da iznajmi virtuelne mašine sa konfiguracijom koje su njemu potrebne, i da ih koristi za svoje potrebe;

- radna površina kao usluga: pomaže korisniku da pristupi radnoj površini svog operativnog sistema preko interneta sa bilo kog mesta;
- skladištenje kao usluga: omogućava da korisnik svoje podatke čuva na fizičkim lokacijama na internetu i da ih koristi lokalno na svom računaru;
- baze podataka kao usluge: koriste se tako što se baza podataka instalira na Cloud-u i koristi se lokalno, čime se postiže visoka prilagodljivost i skalabilnost same baze podataka;
- sigurnost kao usluga: omogućava korišćenje određenih sigurnosnih usluga kao da su implementirane lokalno.

Rađeno je istraživanje u kome se procenjivalo kakvo mišljenje ima 126 ispitanika oko same definicije Cloud-a:

- 71% ispitanika se složilo da je „Cloud evolucija, ne revolucija"
- 62% ispitanika se složilo da je „Cloud je novi način isporuke računarskih resursa, a ne nova tehnologija"
- 31% ispitanika se složilo da je „Cloud samo redefinisan da uključuje sve što mi već radimo"
- 38% ispitanika je ostalo neutralno.

Rezultat istraživanja govori da Cloud nije nova tehnologija, ali da nije ni miks postojećih tehnologija i da su resursi novi, kao i da je nastalo kao rezultat prirodne evolucije računara [3].

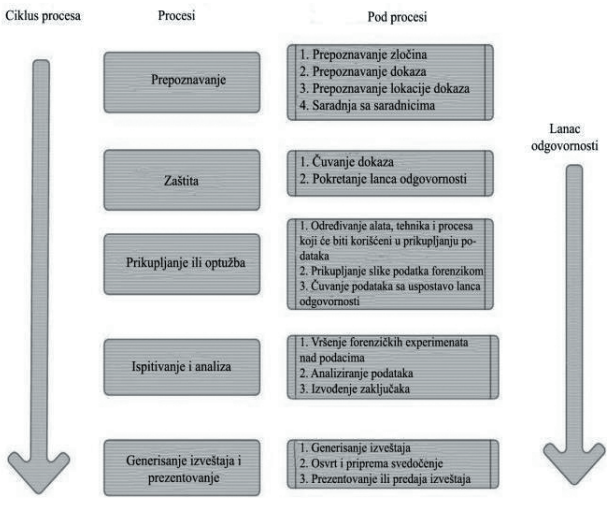
*Digitalna forenzika*

Digitalna forenzika je nauka koja ima za cilj primenu procesa prikupljanja, čuvanja, pronalaženja, analize, dokumentovanja digitalnih dokaza, odnosno podataka koji su skladišteni, obrađeni ili prenošeni u digitalnom obliku i prezentovanja digitalnih dokaza uz očuvanje integriteta originalnog dokaza. Ona svojim metodama i tehnikama prikuplja dokaze koji su u elektronskoj formi i koji mogu biti upotrebljeni kao legitimni dokaz na sudu.

Digitalna forenzika je 2008. godine definisana od strane američkog tima za hitnu digitalnu spremnost kao „disciplina koja kombinuje elemente zakona i računarske nauke da prikupi i analizira podatke iz računarskih sistema, mreža, bežične komunikacije i uređaja za skladištenje na način koji je prihvatljiv kao dokaz na sudu". Relativno je nova nauka, nastala krajem 70-ih godina prošlog veka i omogućava fizičku i logičku rekonstrukciju dokaza u istraživačkim procesima, i svoj ozbiljniji rast dostigla je 90-ih godina kada je krenula i velika zastupljenost računara.

Digitalna forenzika se bavi, pored računara, svim digitalnim uređajima koji imaju mogućnost skladištenja podataka i zato je prate brojni izazovi, kao što su brze promene strukture samih uređaja i sve bolji napadi na iste. Kao nauka najviše se bavi forenzikom računarskih sistema, gde se vrši naučno ispitivanje i analiza podataka koje se nalaze na hard disku, ssd-u, ali i drugim medijima gde se skladište podaci. Primenom alata za digitalnu forenziku određeni podaci koji su namerno obrisani ili sakriveni se mogu vratiti, i oni se analiziraju, i ukoliko je potrebno validni su na sudu kao digitalni dokaz. Digitalna forenzika može da se bavi i forenzikom računarske mreže, gde se skupljaju informacije o tome ko je napadač, odnosno haker. Tendencija je da se otkrije kako je napadač dobio pristup mreži ili sistemu i kojom URL lokacijom je pristupio. Takođe, može da se bavi forenzikom mobilnih telefona kao i forenzikom Cloud-a, koja će naknadno biti objašnjena.

Digitalna forenzika ima svoju tehnološku komponentu, odnosno alate u softverskom i hardverskom obliku, kao i svoju pravnu komponentu zbog koje moraju da se poštuju određeni principi, pravila i metodologije. Da bi digitalni dokaz bio validan i prihvatljiv na sudu, odgovorna lica koja sprovode istragu moraju dobro da poznaju obe komponente [7].




Slika 1. Proces digitalne forenzike 3

*Forenzika cloud-a*

Forenzika Cloud-a je unakrsna disciplina Cloud-a i digitalne forenzike [10]. Definisana je još i kao aplikacija digitalne forenzike koja se nalazi na Cloud platformi i sadržana je od naučnih principa, tehničkih praksi i obrade prošlih događaja u Cloud platformi kroz identifikaciju, prikupljanje, čuvanje, ispitivanje i izveštavanje o digitalnim podacima koji olakšavaju rekonstrukciju određenih događaja. Problemi sa nadležnošću i dupliranje podataka otežavaju samo praćenje lanca događaja, što dovodi do zaključka da forenzički procesi koji se obično koriste za fizičke uređaje ne mogu da se koriste za forenziku Cloud-a.

Cloud forenzika se sastoji iz tri komponente: tehničke, organizacione i pravne. Tehničke komponente su procedure i alatke koje se koriste za prikupljanje podataka u forenzici Cloud-a. Organizaciona komponenta obuhvata klijente, pravne savetnike i smernice. Pravna komponenta pokriva razvoj propisa i osigurava da forenzičke aktivnosti ne krše određene zakone i obezbeđuje poverljivost digitalnog dokaza.

*Tehnički zahtevi*

Integritet digitalnog dokaza mora biti sačuvan ukoliko treba biti prezentovan na sudu i najčešći način očuvanja tog integriteta je generisanje *hash* vrednosti [5].

- Kompatabilnost sa postojećim forenzičkim formatima, umesto kreiranja novih.
- Lako generisanje forenzičkih podataka
- Otvorenost i rasprostranjenost prema programerima koji treba da prošire forenzičke sposobnosti
- Prilagodljivost forenzičkih alata prema pojedincu koji koristi Cloud, u odnosu na one druge koji koriste isti Cloud.
- Praćenje postojećih praksi i standarda kada je to moguće u forenzici Cloud-a.

*Forenzičke procedure*

Forenzičke procedure se koriste nakon što se neki zločin već dogodio i u njima su unapred određeni koraci koji treba da se ispoštuju. U forenzici Cloud-a procedure su grupisane u tri oblasti: korisnička forenzika, forenzika Cloud-a i forenzika mreže.

*Korisnička forenzika*

Digitalni zločini se često dešavaju sa korisničke strane, ali dokazi se mogu naći i na korisničkoj i na serverskoj strani. Podaci kao što su istorija logovanja, privremeni podaci, registracije i kolačići mogu se naći na veb pregledaču i treba ih prikupiti što pre, da korisnik ne bi izvršio neke promene nad njima ili čak i samim sistemom, jer se tako gubi integritet podataka i ne može se rekonstruisati vremenski okvir događaja. Jedan od problema je i to što je većina podataka samo oni koji su najsvežiji, odnosno oni koji se nalaze u kešu računara [4].

*Forenzika Cloud-a (servera)*

Nemogućnost fizičkog pristupa podacima koji mogu da se nalaze isparčani na više različitih servera, koji su geografski udaljeni, otežava prepoznavanje, odvajanje i prikupljanje dosta nestabilnih podataka kao što su sistemska logovanja, aplikativna logovanja, korisničke informacije kroz proces forenzike Cloud-a.

*Forenzika mreže*

Forenzika mreže se bavi analizom saobraćaja i događaja u prošlosti, i u teoriji je moguća i u Cloud okruženju jer određeni slojevi TCP/IP protokola sadrže komunikaciju između virtualne mašine i Cloud-a, kao i virtualne mašine sa drugim servisima i u nekim slučajevima u tim kanalima mogu da se pronađu određena komunikaciona logovanja.

*Obrisani podaci*

Iz perspektive forenzičara obrisani podaci su bitan izvor dokaza. Kod forenzike digitalnih uređaja moguće je povratiti podatke sa alatima koji to omogućavaju, dok je to otežano sa Cloud-om. Postoji mogućnost da se napravi identična kopija sistemske memorije Cloud-a, odnosno da analitičar zamrzne stanje virtualne mašine i da iz toga izvuče informacije. Kada se tako gleda, onda je povraćaj obrisanih podataka moguć i sa Cloud-a samo ukoliko nisu neki podaci prepisani preko tih podataka i potrebno je da se instalira funkcija Snapshot i da se periodično prave slike kroz koje se dobijaju vredne informacije, ali i time što su periodične dobija se linija događaja.

Ukoliko se posmatra iz perspektive onog ko ima kriminalne namere, on će izvršiti svoj zločin koristeći Cloud, deaktivirati svoj nalog, obrisaće virtualnu mašinu i zbog propisa i regulativa o privatnosti na inicijativu

korisnika iza njega neće ostati nikakav trag, i kada forenzičar pokuša da nakon svega toga napravi sliku memorije i da proba da nađe nešto – neće uspeti ništa da dobije.

*Nedostatak podataka o registraciji korisnika*

Sama evidencija korisnika i njegovo prijavljivanje bi trebalo da se čuva u okviru dnevnika sa vremenskim okvirima, ali to zavisi kako je regulisao snabdevač usluga. Analizirajući sadržaj datoteka i pristupanjem vremenskim pečatima forenzičari mogu da donesu određene zaključke, ali bi im dnevnici pomogli da povežu sve u celinu, kao i da lakše mogu da prezentuju digitalne dokaze na sudu jer su svesni da nisu svi ljudi upoznati sa Cloud-om, šta on predstavlja, kako pamti svoje informacije i šta one tačno znače.

*Nedostatak specijalnih komercijalnih alata*

Podaci koje mogu da sakupe alati za digitalnu forenziku su metapodaci, promene u sadržaju određenih datoteka, sadržaj registra, obrisane particije, podaci o kreiranju i brisanju korisničkih naloga, dok za forenziku Cloud-a ne postoje sertifikovani i međunarodno priznati alati koji mogu da povrate te sve podatke u celosti.

Jedino sto može da se uradi sa aktivnim nalozima jeste da se prikupljaju podaci koji ostaju na strani korisnika i servera pravljenjem identične kopije memorije, gde mogu da se nađu podaci kao što su popis direktorijuma, registar, istorija pregledača, link datoteke i link reference koje ostaju i nakon što se obrišu, i sve to može da se predstavi kao validan dokaz na sudu.

*Pregled i analiza podataka*

Pregled podataka u fazi analize podrazumeva ocenjivanje prikupljenih podataka koji su podupreti nekim vremenskim okvirom dešavanja događaja. Gleda se njihova jačina, kada budu bili prezentovani na sudu, i da li će biti razumljivi.

## 4. REZIME

Postoje već određeni i standardizovani procesi za digitalnu forenziku, dok je forenzika Cloud-a nova oblast koja tek treba da se razvija. Nepoznata fizička lokacija podataka u Cloud-u i dupliranje podataka kroz različite virtuelne servere stvara prepreke u prepoznavanju dokaza, ali i njihovom očuvanju i prikupljanju. Sama decentralizacija Cloud-a pored tehničkih stvara i pravne poteškoće jer se počinilac i Cloud nekada ne nalaze na istoj teritoriji gde je potrebna podrška iz drugih zemalja, a još uvek nisu u potpunosti regulisani svi međunarodni okviri i tome treba obratiti pažnju.

Kada se radi o praćenju zločina, forenzičari moraju da prate svaku vezu u lancu kako bi prikupili dokaze i zato se teži ka tome da se odvoje korisnici na nivou naloga, a ne na nivou servera kako se ne bi narušila tuđa privatnost istražujući specifični nalog. Sve više korisnika enkriptuje svoje podatke kako bi ih još više zaštitili, što otežava identifikovanje dokaza sa počiniocem. Jedino što forenzičari mogu da rade jeste da rade *hash* nad svim podacima i da probaju da dođu do ključa za dešifrovanje podataka bez kršenja privatnosti.

Bitnu ulogu u budućnosti forenzike Cloud-a će imati pravilno sprovedena sigurnost na početku jer obezbeđuje podatke o tome ko poseduje taj nalog, kroz koje procese je prolazio i time se grade jaki dokazi. To će biti veoma teško za postići jer što su forenzičari bliži tome sa svojim alatima, to više narušavaju samu privatnost korisnika i kompanije koje nude usluge Cloud-a u želji da zadrže svoje korisnike i podižu nivo sigurnosti, što forenzičare vraća na početak.

## 5. ZAKLJUČAK

Cloud je kao usluga u potpunosti promenila način na koji se određene usluge tretiraju i prezentuju klijentima. U poslednjih par godina došlo je do naglog porasta upotrebe Cloud-a kao servisa i pretpostavka je da će nastaviti sa rastom. Sa druge strane, sa sve većom upotrebom sve više se javlja zabrinutost korisnika oko sigurnosti i privatnosti podataka, kao i velika mogućnost upotrebe servisa u kriminalne aktivnosti jer su ogromne računarske moći sa velikim skladištem, što omogućava sprovođenje određenih napada veoma brzo sa malo troškova, u odnosu na mogućnost dobiti. Takođe, nivo anonimnosti koji kriminalci mogu da imaju je visok jer oni mogu da izvrše napad, obrišu nalog i obrišu virtualnu mašinu sa svog računara i oni nikada ne mogu biti povezani sa tim zločinom.

Ono što može da se uradi jeste da se implementacija forenzike Cloud-a vrši na početku i da bude konstantna, pokušaj da se ne narušava privatnost drugih učesnika, već samo onog lica nad kim se vrši istraga. Takođe se gleda da se u budućnosti standardizuju određeni alati koji će moći u potpunosti da povrate sve podatke koji su se nalazili na Cloud servisu.

## LITERATURA

[1] A. Pichan, M Lazarescu, S. T. Soh, "Cloud forensics: Technical challenges, solutions and comparative analysis", 2015, pp.38-57.

[2] J. Dykstra, A. T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust and techniques", 2012, pp.S90-S98.

[3] K. Ruan, J. Carthy, T. Kechadi, I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results",2013, pp. 34-43.

[4] V. Roussev, I. Ahmed, A. Barreto, S. McCulley, V. Shanmughan, "Cloud forensicse-Tool development studies & future outlook", 2016, pp.79-95.

[5] J. Dykstra, A. T. Sherman, "Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform", 2013, pp.S87-S95.

[6] B. Martini, K. R. Choo, "An integrated conceptual digital forensic framework for cloud computing", 2012, pp.71-80.

[7] J. Samardžija, "Digitalna forenzika mobilnih telefona primenom uređaja Cellebrite UFED", Beograd, Srbija, ITS diplomski rad, 2018.

[8] S. Simou, C. Kalloniatis, E. Kavakli, S. Gritzalis, "Cloud Forensics: Identifying the Major Issues and Challenges", 2014, pp.271-284.

[9] <http://resources.infosecinstitute.com/overview-cloud-forensics/#gref>

[10] <http://cloudforensicsresearch.org/publication/Cloud_Forensics_An_Ov erview_7th_IFIP.pdf>