REPUBLIKA E SHQIPËRISË
UNIVERSITETI I TIRANËS
Fakulteti i Ekonomisë
Departamenti Statistikë dhe Informatikë e Zbatuar

Temë Diplome

Tema:

Hetimet e regjistrimeve te cloud-it: Zbulimet , të metat dhe drejtimi në të ardhmen.
(Cloud Log Forensics: Foundations, State of the Art and Future Directions)

Punoi

Arsid Selgjekaj

Udhëheqës:

Prof.Dr. Valentina Sinaj

Abstrakt:

Me zbulimin e internetit dhe teknologjisë, cloud computing është globalisht i pranueshëm për çdo shërbim në industri. Me këtë përshkallëzim të madh në zbatim, mjedisi cloud është i ekspozuar ndaj një sulmuesi me shumë sulme të mëdha. Pra, ekziston një emergjencë kërkesash për të lehtësuar hetuesit për të mbledhur, analizuar dhe prodhuar dëshmi nga mjedisi cloud, i cili mund të përdoret në raste gjykatë të ndryshme. Ditarët mbajnë të dhëna të dobishme lidhur me aktivitetet ose ngjarjet e sistemit, rrjetit. Ky informacion është shumë i shtrenjtë për të provuar sulmet në gjykatë raste. Pra, kërkohet mbrojtje dhe gjithashtu ruhet integriteti, konfidencialisht, siguria e shkrimet. Për të mbledhur dhe analizuar mesazhet e ditarit nga burime të ndryshme si router, switch, makinë virtuale, firewalls, sistem operativ. Këto shkrime kategorizohen me shprehje të rregullt dhe në dyqan në format të koduar të veçantë. Për të kapërcyer kostot e tematikës dhe për të përmirësuar sigurinë, një organizatë duhet të zhvendoset drejt cloud-it. Përdorimi i forenzikës së të dhënave të bazuar në cloud, hetuesi mbledh me lehtësi log-in dhe zhvillon hetimet. Në mjedisin e cloud-computing ata gjithashtu përdoren në forenzikë për të provuar sulmet dhe për të rritur konfidencialitetin. Ligjshmëria e kodeve kompjuterike Cloud Log Forencis zbut procesin e hetimit duke identifikuar sjelljen keqdashëse të sulmuesve përmes analizës së thellë të regjistrit të cloud-it. Sidoqoftë, atributet e kërkimit të log të cloud-it pengojnë arritja e qëllimit për të hetuar shkrimet e reve për ndjeshmëri të ndryshme. Kërkimi përfshin çështjet e aksesit në cloud-log, zgjedhjen e skedarit të duhur të logut të cloud, integritetin e të dhënave të logut të cloud dhe besueshmërinë e shkrimet e cloud-it. Prandaj, hetuesit ligjorë të skedarëve të logut cloud janë të varur nga ofruesit e shërbimit të cloud për të marrë aksesim në regjistrat e ndryshëm të cloud-it. Ky material shqyrton gjendjen e artit të CLF dhe nxjerr në pah sfida të ndryshme dhe çështje të përfshira në hetimin e të dhënave të regjistrit të cloud-it.Në këtë projekt janë shpjeguar mënyrat e regjistrimit, rëndësia e CLF, dhe cloud log-si-nje-sherbim. Për më shumë informacione, shpjegohen rastet studimore lidhur me CLF , të cilat nxjerrin në pah zbatimin praktik të hetimit të regjistrit të cloud për analizimin e sjelljeve me qëllim të keq. Kërkesat e sigurisë CLF, pikat e cenueshmërisë dhe sfidat janë identifikuar për të toleruar dyshimet e ndryshme të log cloud.

Falët kyçe: Cloud Log Forensics,Log, Virtual Machine,Cloud Computing, Hetime ligjore,Skedar.

Përmbajta

Lista e tabelave:

Lista e figurave:

Lista e shkurtimeve:

CLF---------- Cloud Log Forensics

IP---------- Adresa Ip

FISMA---------- Akti Federal i Menaxhimit të Sigurisë së Informacionit

PCI DSS---------- Standardi i Sigurimit të të Dhënave të Industrisë së Kartës së Pagesave

GLBA---------- Akti Gramm-Leach-Bliley

VM----------Virtual Machine

CS----------Zinxhirin e Identifikimit

CSP----------Cloud Service Provider

API----------Application Programming Interface

VMLA---------- Revista e Identifikimit të Veglave Virtuale

Kapitulli 1. Hyrje

1.1. Një përshkrim i përgjithshëm

Çdo ngjarje që ndodh në një sistem të teknologjisë informative të organizatës ose rrjetit është regjistruar me shënime të ndryshme në një skedar log. Procesi i regjistrimit të dosjeve të logaritjeve është i njohur si logging [Chuvakin et al. 2013]. Dosja e skedarit siguron informacion të dobishëm lidhur me ngjarjet e mëparshme që ndodhin në sistem dhe rrjet gjatë një hapësire kohore të specifikuar. Për shembull, një administrator i rrjetit mund të mësojë rreth përdorimit të bandës së rrjetit në një interval kohor duke analizuar kodin e rrjetit. Në mënyrë të ngjashme, përdoruesit e aplikacioneve përdorin kodin e aplikacionit për të identifikuar dhe rregulluar bug-et brenda një programi. Çdo hyrje në një regjistër skedari siguron informacion të rëndësishëm në lidhje me një ngjarje të veçantë në kohën e krijimit të skedarit.Fillimisht, skedari i log-ut(log file) përdoret për regjistrimin e problemeve [Flegel 2002]. Tani, log file ofron shërbime më funksionale, duke përfshirë monitorimin e sistemit dhe rrjetit, duke optimizuar performancën e tyre, regjistrimin e aktivitetit të përdoruesit, dhe duke hetuar sjellje me qëllim të keq [Kent dhe Souppaya 2014]. Shkrimet janë tani kryesisht përdoren për qëllime sigurie për shkak të sulmeve në rritje ndaj sistemit dhe rrjetit [Zuk 2011].Në organizata të mëdha, lloje të ndryshme të skedarëve të llogaritjeve krijohen në pajisje të ndryshme që përfshijnë çështjen e menaxhimit efektiv të shkresave për shkak të mungesës së burimeve. Për të kapërcyer problemin e menaxhimit të regjistrit, organizatat kanë filluar të lëvizin drejt cloud computing duke përdorur shërbimet e hyrjes cloud të njohur si log-as-a-service [Saurabh dhe Beedgen 2014]. Dosjet e regjistrit të krijuara në burime të ndryshme organizative dërgohen në cloud për ruajtje dhe analizë duke përdorur burimet e magazinimit të cloud dhe analizën e logut të serverave të cloud-it. Në mënyrë të ngjashme, organizatat kryesisht i zbatojnë aplikimet e tyre në llogaritjet cloud për të hetuar aktivitete me qëllim të keq. Regjistrimi në cloud përfshin skedarët e aplikacioneve , regjistrimet e rrjetit të cloud, regjistrimet e sistemit të cloud-it, firewall i cloud dhe kështu me radhë. Në këtë artikull, fjala "log cloud" është përdorur për t'iu referuar të gjitha shkrimet krijuar brenda një mjedisi të cloud computing. Në ditët e sotme, sulmet ndaj cloud computing po ndodhin më shpesh, gjë që krijon shqetësim midis përdoruesve dhe organizatave në lidhje me mënyrën më të mirë për t'i ruajtur të dhënat e tyre nga sulmues të ndryshëm [Khan et al.2014].

Procesi i analizimit të skedarëve të regjistrit të cloud në cloud computing ose përmes shërbimeve të analizës së palëve të treta quhet ligjërisht forensika e logut të cloud-it(CLF) [Thorpe et al. 2012]. CLF është një fushë e re e sigurisë së të dhënave që përdoret për të analizuar të dhënat brenda skedarëve të regjistrit të cloud për hetimin e sjelljeve me qëllim të keq. Megjithatë, skedarët e regjistrit të cloud janë të arritshëm vetëm tek një Ofrues i Shërbimeve të Cloud (CSP) përmes pronësisë së resurseve cloud. Për shembull, në softuerë-shërbime cloud (SaaS), një përdorues është i pajisur me softuer të zhvilluar për të drejtuar aplikacionet e saj. Çdo kërkesë gjeneron skedarë log gjatë ekzekutimit të saj në cloud që janë të paarritshme për përdoruesit [Ruan et al. 2011]. Edhe pse dosjet nuk janë të lidhur në mënyrë direkte me hetuesin, CPS-të ofrojnë akses në këtë regjistër me aprovim ligjor nga gjykata. CSP-të ofrojnë akses të kufizuar për hetuesit e palëve të treta për skedarët e regjistrit të cloud për shkak të privatësisë së të dhënave të përdoruesit dhe procedurave organizative të operimit standard (SOPs) [Birk dhe Wegener 2011].

Për më tepër, CFL-ja ka miratuar hapa të mëdhenj proceduralë për forenzikën digjitale si për mbledhjen, ruajtjen, analizimin dhe raportimin [Khan et al. 2014; Sang 2013]. Në hapin e grumbullimit, skedarët e regjistrit të cloud janë marrë nga burime të ndryshme cloud. Dosjet e ndryshme të regjistrit të cloud të grumbulluara nga burime të ndryshme të resurseve cloud mund të ndryshojnë në varësi të kërkesave organizative për të dhënat e regjistrit të cloud që përfshijnë një numër të shënimeve të regjistrit, limitin e skedarit, kohën për të hyrë në të dhëna dhe çfarë përmbajtjesh duhet të regjistrohen. Pas grumbullimit, skedarët e logut cloud regjistrohen në mënyrë të sigurt për të mbrojtur integritetin. Integriteti i të dhënave është ruajtur në CLF për arsyen për të siguruar prova kundër sulmuesve në gjykatë [Joo et al. 2014]. Hapi i ardhshëm është të kryejë analizë të dosjeve të logut të cloud për të prodhuar dëshmi të mundshme për të ndihmuar hetuesin të gjurmojë sulmuesin duke ri-gjeneruar përsëri aktivitetet me qëllim të keq. Analiza e kryer në shkrimet e cloud siguron një pamje të qartë të aktivitetit keqdashës të kryer nga sulmuesi gjatë sulmit. Analiza e skedarëve të regjistrit në cloud është shtylla kurrizore e CLF në identifikimin e sulmeve dhe ndihmën e administratorëve për të parandaluar lloje të ngjashme të sulmeve në të ardhmen. Së fundi, pas analizës së kryer në shkrimet e cloud, gjenerohet një raport ligjor për të regjistruar çdo ngjarje të kryer gjatë hapave individualë të CLF. Raporti përmban informacion gjithëpërfshirës në lidhje me tërë procesin e hetimit, por disa nga informacionet përfshijnë kur është kryer hetimi, procedura e përdorur për të mbledhur provat, se si u mbajt integriteti i dosjeve të regjistrit cloud, cilat ishin mjetet endryshme të analizës. Zakonisht, raporti përfundimtar përdoret kundër sulmuesit në një gjykatë për sjelljen e tij me qëllim të keq.

Për më tepër, gjatë dekadave të fundit, cloud computing u konsiderua si një vend i sigurt për të ruajtur dhe llogaritur të dhënat e përdoruesve dhe organizatave të ndryshme. Aktualisht, shfrytëzimi i resurseve të

ndryshme cloud, aplikacionet, kanalet e rrjetit dhe të dhënat e regjistrit kanë treguar se dobësitë e ndryshme gjenden në cloud-computing. Për të minimizuar dobësitë e gjetura në cloud, CSPs filluan të riorganizonin çështjet e tyre të sigurisë. CLF është një aspekt i sigurisë së cloud që ndihmon CSP për të fituar kuptueshmëri më të thellë në lidhje me hapat e kryera në sulmet e cloud-it. Rëndësia e CLF rritet kur skedarët e regjistrave të cloud-it ruhen në cloud-computing, bëhen viktima përmes sulmeve të ndryshme që përfshijnë modifikimin e të dhënave të regjistrit në skedarët e llogaritjeve, fshirjen e të dhënave të llogaritjeve, futjen e të dhënave të skedarëve të spoofed etj. CLF kryen inspektim të thellë të skedarëve të dosjeve të infektuara të cloud për të kuptuar sjelljen e dyshimtë të sulmit të kryer në skedarët e regjistrit të cloud. Qëllimi përfundimtar i CLF është të identifikojë shkaktarin rrënjësor të sulmeve të logut të cloud, i cili u ndihmon CSP-ve për të parandaluar përsëritjen e sulmeve të tilla.

Qëllimi i këtij kërkimi është që të ofrojë informacion mbi CLF dhe të ofrojë hulumtues me një kuptim të thellë përmes menaxhimit të regjistrit [Ray et al. 2013], mënyrat e hyrjes [Rafael 2013], shërbimet e ofruesve të log-like-a-service të cloud computing [Ellis 2013; Burton 2014; IBM 2014; Logentries 2014; Williams 2013], dhe, veçanërisht, studimet e rasteve të CLF [South 2013; Kastor 2015]. Për më tepër, sfidat e CLF identifikohen për të ndihmuar kërkuesit në eksplorimin e fushave të reja kërkimore dhe duke i motivuar ata të dalin me ide të reja, metoda, standarde dhe mjete për avancimin e hetimit të regjistrit në cloud-computing.

1.2. Qëllimi i punimit

Kontributet kyçe të kësaj teme theksohen si më poshtë:

- Njohuri të plota për sfondin e CLF: Ne japim informacione lidhur me hyrjet(logging), duke përfshirë llojet e tij dhe mënyrën e hyrjes, cloud computing, dhe forenzika dixhitale.

-Një përshkrim i shkurtër i log-si-një-shërbim i ofruar nga shitësit cloud: Unë ofroj njohuri rreth asaj se si dhe cilat tipare ofrohen nga shitësit e cloud tek konsumatorët në lidhje me menaxhimin e regjistrit të cloud-it.

- Një shpjegim i zbatimit praktik të CLF përmes studimeve të rasteve: Unë nxjerr në pah skenarët e botës reale që lidhen me klientët dhe shitësit e logave të cloud në vendosjen dhe zbatimin e CLF.

- Identifikimi i kërkesave të sigurisë së CLF, pikat e cenueshmërisë dhe sfidat më të rëndësishme të artit: Un diskutoj se çfarë duhet të jenë parametrat kryesorë të sigurisë për CLF, ku duhet të mbledhim dëshmi për hetimin dhe cilat janë sfidat për CLF ?

- Fushat e drejtimeve të ardhshme kërkimore: Unë ofroj fusha potenciale kërkimore për CLF për të kapërcyer sfidat aktuale. Pjesa tjetër e artikullit është e organizuar si më poshtë. Seksioni 2 ofron njohuri paraprake për hyrjet(logging) duke dhënë një pasqyrë të llojeve dhe mënyrave të tij. Përveç kësaj, përshkrimet e shkurtra në lidhje me cloud computing dhe forenzikën dixhitale ofrohen për të fituar njohuri për konceptin e saj kryesor. Në Seksionin 3, ne paraqesim rëndësinë e CLF dhe shpjegojmë gjendjen aktuale të artit. Seksioni 4 shpjegon shitësit të ndryshëm të cloud që ofrojnë shërbimin log-as-a-service. Në Seksionin 5, ne përshkruajmë studime të rasteve të ndryshme që lidhen me CLF. Seksioni 6 paraqet kërkesat e sigurisë CLF, pikat e cenueshmërisë dhe sfidat më të fundit. Së fundi, Seksioni 7 përfundon artikullin duke theksuar drejtimet e hulumtimit në të ardhmen.

1.3. Organizmi i punimit

Ky punim është ndarë në 5 kapituj. Kapitulli i pare është hyrja në të cilën tregohet se si ka nisur colud log forensics dhe në atë kohë si ishin impresionet e para të njerëzve. Cilat ihsin të vëçantat e këtij projekti dhe në fund të fundit për çfarë nevojitej ? Kapitulli i dytë tregon për regjistrimet se si ndodhin dhe cilat ishin disavantazhet dhe avantazhet e këtyre regjistrimeve. Mënyrat e regjistrimeve qe bëhen dhe diferencat mes tyre. Kapitulli i tretë na tregon një pamje më të qartë se çfarë është cloud log forensics dhe cilat janë detyrat dhe pjesët kryesore të saj dhe hetimet e ndryshme që ndodhin kundër hakerave. Kapitulli i katërt na tregon për rastet e ndryshme të studimeve që janë bërë në kompani të ndryshme në lidhje me cloud log forensics dhe çfarë kanë nxjerrë kompanitë nga këto studime. Kapitulli i pestë dhe i fundit na jep të dhëna se cilat janë pikat e dobëta të këtij projekti dhe a mundemi ne ti eliminojmë dhe si duhet të mbrohemi nga hakerat e ndryshëm që aksesojnë të dhënat tona. Në fund kemi përfundimet që kemi nxjerrë nga kjo detyrë dhe referancat.

Kapitulli 2. Regjistrimet e të dhënave

2.1. Regjistrimet

Procesi i regjistrimit të ngjarjeve në një skedar gjatë ekzekutimit të sistemit operativ, procesit të rrjetit, makinës virtuale ose aplikacionit quhet "hyrje(logging)" dhe skedari quhet "skedari log" [Kent dhe Souppaya 2014]. Dosja e regjistrit përmban hapat vijues të kryer gjatë një ekzekutimi përgjatë një afati kohor të specifikuar. Një skedar log-i përbëhet nga shënimet e regjistrit dhe çdo hyrje e regjistrit përmban informacion të dobishëm që lidhet me ngjarjet që ndodhin në sistem, rrjet, makinë virtuale ose aplikim. Skedarët log file ndryshojnë në lidhje me llojet dhe kërkesat e tyre. Për shembull, formati standard që përdoret nga web-server për të gjeneruar skedarët e skedarëve të serverit përfshin [Hosti identitet authuser data kërksesë statusi bytes]. " Hosti" është klienti që bën një kërkesë në web-server; "Identiteti" është RFC 1413 identifikues i klientit; "Authuser" është id-përdoruesi i përdorur në kërkesën për një dokument; "Data" është fusha e datës, kohës dhe fusha e kohës kur web-server përfundon përpunimin e një kërkese; "Kërkesë" është metoda e kërkuar nga klienti; "Statusi" përfaqëson një kod statusi HTTP; dhe "bytes"

është madhësia e një objekti që kthehet tek klienti nga web-server. Për një kuptim të qartë të formatit të regjistrit, Figura 1 përshkruan një format identifikimi të hyrjes duke theksuar fushat e tij të ndryshme. Çdo fushë log me vlerën dhe përshkrimin e saj është paraqitur në Tabelën I. Çdo organizatë ka qëllime të ndryshme për të gjeneruar skedarë loga-u varësisht nga kërkesat e saj. Dosjet e regjistrit fillimisht krijohen brenda organizatave me qëllim të zgjidhjes së problemeve, megjithatë, objektivat janë zgjeruar për shumë qëllime të tjera, duke përfshirë regjistrimin e veprimeve të përdoruesit, autentifikimin e përdoruesit, performancën e rrjetit, optimizimin, monitorimin e shëndetit të sistemit, privatësinë e të dhënave, forenzikën e kështu me radhë.

Logging është konsideruar si një mjet thelbësor për kontrollin e sigurisë që ndihmon hetuesit në identifikimin, përgjigjen dhe përjashtimin e çështjeve operacionale, incidenteve, shkeljeve dhe aktiviteteve mashtruese [Kent dhe Souppaya 2014]. Logging është përdorur kryesisht në sistemet e monitorimit për të mbledhur të dhëna për hetimin e sulmeve të ndryshme me qëllim të keq.

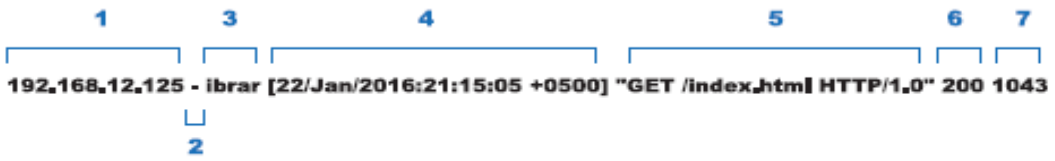

Fig. 1. Format of an access log file.

Fig. 1. Formati i aksesimit të një skedari regjistrimesh(S. Khan et al.)

Tabela I. Përshkrimi i formatit të Identifikimit të Aksesit

S.No	Fusha	Vlerat	Pershkrimi
1	Host	192.168.12.125	Adresa IP e përdoruesit HTTP i cili bën kërkimin e burimeve HTTP...
2	Rfc931	-	Identifikuesi përdoret për të përcaktuar klientin
3	Përdoruesi	ibrar	Emri i përdoruesit ose përdoruesi i përdorur për vërtetim
4	data:ora e zones	[22/Jan/2016:21:15:05 +0500]	Vula e datës dhe orës së kërkesës HTTP
5	Kërkesa	“GET /index.html	Kërkesa HTTP që

		HTTP/1.0”	përmban (a) HTTP metoda = GET, (b) Kërkesa HTTP resource = index.html, dhe (c) HTTP versioni i protokollit = 1.0
6	statusi i kodit	200	Kodi numerik përdoret për të treguar rreth statusit të kërkesës HTTP p.sh suksesi ose dështim
7	Bitet	1043	Fusha numerike përdoret për të nxjerrë në pah numrin e bytes e të dhënave të transferuara gjatë kërkesës HTTP

Burimi: S. Khan et al.

Shkrimet(logs) ndihmojnë hetuesit për të identifikuar burimet e mesazheve të gjeneruara nga pajisje të ndryshme në intervale të ndryshme kohore. Shumë shkrime të krijuara për arsye sigurie ndalojnë ndërhyrjet e ardhshme duke i zbuluar ato përmes modeleve dhe dukurive të ndryshme të vërejtura. Regjistrat e auditimit gjenerohen për të gjurmuar autentifikimin e përdoruesit të bërë në sistem ose rrjet [Prasad and Chakrabarti 2014]. Në mënyrë të ngjashme, pajisjet e sigurisë, siç janë sistemet e zbulimit të ndërhyrjeve dhe firewalls, regjistrojnë regjistra për të përmbajtur sulme të mundshme [Vaarandi dhe Pihelgas 2014]. Prandaj, shkrimet e ndryshme mund të përdoren për qëllime sigurie në varësi të kërkesave organizative. Disa shkrime sigurie gjenerohen në kohë reale duke mbledhur ngjarje gjatë kohës së ekzekutimit të sistemit dhe rrjetit, ndërsa disa shkrime sigurie gjenerohen periodikisht në intervale të rregullta kohore.

2.1.1.Tipet e logeve.

Rritja e dobësive, sulmeve dhe shkeljeve të të dhënave organizative detyrojnë personelin e sigurisë për të gjeneruar lloje të ndryshme të regjistrave. Çdo pjesë e një sistemi, aplikacioni, pajisjeje ose rrjeti që komunikon me përdoruesit ose sistemet, duhet të regjistrojë ngjarjet e komunikimit në një skedar log. Shembuj të regjistrave të ndryshëm përfshijnë

Tabela II: Llojet e ndryshme te loge-ve

Tipet e log	Përshkrimi	Shembuj
Log Aplikimi	Shkrimet që regjistrohen nga një aplikacion ose program. Zhvilluesit e aplikacioneve janë përgjegjës për të specifikuar se çfarë, kur dhe si të hyni në një ekzekutim të aplikacionit në një sistem.	Aplikime web, Programe database.
Log Sistemi	Regjistrat e sistemit gjenerohen nga një sistem operativ i cili është i paracaktuar dhe përmban informacion në lidhje me ngjarjet e sistemit, funksionimin, drejtuesit, ndryshimet e pajisjeve dhe shumë të tjera.	Syslog-ng, Log & Event Manager(Hyrja dhe Menaxhimi i eventeve).
Log Sigurimi	Ditarët përmbajnë informacione të lidhura me sigurinë për të përcaktuar sjelljen me qëllim të keq që gjendet në sistem ose rrjet. Për shembull, zbulimi i malware, karantina e skedarëve, koha e zbulimit me qëllim të keq dhe të tjerë.	Event Log Analyzer, Kontrolli i rasteve të Sigurisë Logging Event dhe shërbimet e Monitorimit.
Log Ngarkimi	Regjistrat e instalimit kapin ngjarjet që ndodhin gjatë kryerjes së instalimit të një aplikacioni.	Msiexec.exe
Log Interneti	Regjistri i rrjetit është një skedar log që përmban ngjarje të lidhura me rrjetin, domethënë përshkrimin e ngjarjes, prioritetin, kohën e ngjarjes dhe shumë më tepër.	Splunk, Log4j2.
Log i Serverave Web	Regjistri i ueb-serverëve regjistron të gjitha ngjarjet që ndodhin në web-server, si koha e aksesimit, adresa IP, data & ora, metoda e kërkesës dhe vëllimi i objektit (bytes).	Nihuo Web Log Analyzer.
Log Auditimi	Regjistri i auditimit përmban akses të paautorizuar të përdoruesit në sistem dhe në rrjet për të inspektuar përgjegjësitë e tij. Përfshin adresat e destinacionit, informacionin e identifikimit të përdoruesit dhe afatin kohor.	Regjistri i Auditimit të Sigurisë të WP, auditpol.exe.

Log të Makinave Virtuale	Një skedar që përmban të dhënat për çdo ngjarje të kryer në një makinë virtuale.	Kontrolli i regjistrit të makinës virtuale, kontrolluesi i JVM.

Burimi: S. Khan et al.

skedarët e aplikacioneve, regjistrat e sistemit, loget e sigurisë, regjistrimet e konfigurimit, shkrimet e rrjetit, loget e web-serverëve, regjistrat e auditimit, regjistrat e VM-së etj. Secili prej llojeve të regjistruara të lartpërmendura përshkruhet shkurtimisht në Tabelën II me shembuj. Regjistrat e aplikacionit krijohen nga zhvilluesit përmes futjes së ngjarjeve në program. Regjistrat e aplikacionit ndihmojnë administratorët e sistemit të dinë për situatën e një aplikacioni që ekzekutohet në server. Regjistrat e aplikacionit duhet të jenë të strukturuara mire në mënyrë që ata të japin informacion të rëndësishëm për të siguruar themelet për nivele më të larta të nxjerrjes, vizualizimit dhe bashkimit. Rryma e ngjarjeve të regjistrave të aplikacionit është e nevojshme për të parë dhe filtruar të dhënat që vijnë nga raste të shumta në aplikacion. Dosjet e skedarit të sistemit gjenden në sistemin operativ të përdorur për të regjistruar paralajmërime, gabime, modifikime dhe debug mesazhe. Për shembull, një mesazh paralajmërues për "përditësimin e drejtuesit të pajisjes" regjistrohet në regjistrimet e sistemit. Dosjet e regjistrit të sistemit zakonisht përmbajnë informacion në lidhje me të dhënat dhe kohën e krijimit të regjistrit; llojin e mesazhit, të tilla si debug, gabim, dhe kështu me radhë, mesazhe të gjeneruara nga sistemi të lidhura me ndodhjen; dhe proceset që janë prekur nga shfaqja e një ngjarjeje. Regjistrat e sigurisë përdoren për të siguruar aftësi adekuate në përcaktimin e aktiviteteve me qëllim të keq pas shfaqjes së tyre për t'i parandaluar ata që të rishfaqen përsëri. Regjistrat e sigurisë regjistrojnë informacione të ndryshme të paracaktuara fillimisht nga administratorët e sigurisë. Për shembull, shkrimet e firewall ofrojnë informacion lidhur me paketat e drejtuara nga burimet, adresat IP të refuzuara, aktivitetet e jashtme nga serverët e brendshëm dhe hyrjet e pasuksesshme. Regjistrat e sigurisë ofrojnë informacione të hollësishme që duhet të menaxhohen, kontrollohen dhe analizohen nga administratorët e sigurisë sipas kërkesave të tyre. Regjistrat e skedarëve të konfigurimit regjistrojnë çdo ngjarje gjatë kohës së instalimit. Ai ndihmon administratorin e rrjetit në njohjen e hapave vijues të kryera gjatë procesit të instalimit që mund të jenë të dobishme kur ka probleme me instalimin. Dosjet e skedës së konfigurimit gjenerojnë një përmbledhje të detajuar në lidhje me hapat e instalimit që ndihmojnë administratorët e sistemit në ndjekjen e lehtë.Regjistri i rrjetit përmban informacion të detajuar në lidhje me ngjarjet e ndryshme që kanë ndodhur në rrjet. Ngjarjet përfshijnë regjistrimin e trafikut me qëllim të keq, një rritje në shkallën e trafikut të rrjetit, pika e paketave, vonesat e bandwidthit, etj. Administratorët e rrjetit monitorojnë dhe troubleshoot e përditshme përmes analizimit logs të rrjetit për ndërhyrje të mundshme. Ekzistojnë pajisje të ndryshme të rrjetit nga të cilat mund të mblidhen shkrimet e rrjetit, duke përfshirë routers, rrjetet dhe vatrat e bazuara në host dhe sistemet e zbulimit të ndërhyrjeve. Web-server ruan regjistrimet e lidhura me faqet e internetit që ekzekutohen në web-server. Regjistrimet përmbajnë historinë për një kërkesë faqeje, adresën IP të

klientit, të dhënat dhe kohën, kodin HTTP dhe bytet që shërbejnë për kërkesën. Logs web-server janë të arritshme për administratorin ose webmaster, të cilët mund të kryejnë një analizë statistikore për të gjetur modelet e trafikut për një interval kohor të caktuar. Dosjet e regjistrit ruajnë aksesin e paautorizuar në sistem ose rrjet në mënyrë të njëpasnjëshme. Ai ndihmon administratorët e sigurisë në analizimin e aktiviteteve me qëllim të keq në kohën e sulmit. Zakonisht, informacioni kryesor brenda skedarëve të log-ut të auditimit përfshin adresat e burimit dhe të destinacionit, informacionin e identifikimit të përdoruesit dhe afatet kohore. Të dhënat e regjistrit VM regjistrojnë informata specifike për rastet që ekzekutohen në VM siç janë konfigurimi fillestar, operacionet dhe koha që përfundon ekzekutimin e tij. VM regjistron rekord për operacione të ndryshme, d.m.th numrin e instancave që konkurrojnë në VM, kohën e ekzekutimit të çdo aplikacioni dhe migrimin e aplikacioneve për të ndihmuar CSP në gjetjen e aktiviteteve të dëmshme që ndodhën gjatë sulmit. Numri në rritje i llojeve të ndryshme të logs(shkrimeve) krijon probleme për organizatat për të mbledhur, ruajtur dhe analizuar të dhënat e regjistrit brenda infrastrukturës ekzistuese. Problemet me të cilat përballen organizatat në menaxhimin e të dhënave të regjistrit përfshijnë ekspertë njerëzorë, kohën, koston, mjetet, burimet dhe menaxhimin e tyre. Ka shumë vështirësi për organizatat për të ndërtuar infrastrukturë të re, për të zhvilluar mjete dhe për të trajnuar fuqinë punëtore të tyre për të menaxhuar sasi masive të regjistrave. Si rezultat, kostot më të larta dhe konsumin më të madh kohor janë të nevojshme për të menaxhuar dosjet log me sasi të mëdha të të dhënave të regjistrit.

2.1.2. Mënyrat e Regjistrimit.

Logging(regjistrim) është procesi i regjistrimit të një ngjarjeje në kohën e ekzekutimit të sistemit. Kur një sistem po ekzekutohet në mënyrë korrekte, logging krijon një përshkrim të mbledhjes dhe ruajtjes së ngjarjeve të ndryshme në kujtesë. Megjithatë, gjenerimi i regjistrave ka kuptim kur sistemi shkon në fazën e dështimit shpesh ose ndjeshmëri të ndryshme ndikojnë në proceset në sistem. Për të hetuar probleme të tilla, kërkohet shkrimet për të identifikuar hapat vijues të ndjeshmërisë. Ka dy mënyra kryesore të logging që përcaktojnë se si duhet të ruhen shkrimet në kujtesë dhe çfarë duhet të mbulohen nga shkrimet për të hetuar dobësi të ndryshme. Secili prej mënyrave të logging është shpjeguar shkurtimisht dhe prot dhe kundrat e çdo modaliteti të logging janë ilustruar në Tabelën III me krahasimin e tyre në Tabelën IV.

Tabela III. Mënyrat e Logging, Avantazhet dhe Disavantazhet

Logging Mode (Mënyrat e regjistrimit)	Avantazhet	Disavantazhet
Logging në mënyrë rrethore	• Transaksion i shpejte mes regjistrave • Nuk kërkohet mirëmbajtje • I aplikueshëm për softuer, energji dhe dështimi i aplikimit • Kërkon ndërhyrje minimale njerëzore • Regjistrat e ripërdorur	• Mungesa e ruajtjes afatgjate • Mbishkruani shkrimet ekzistuese duke plotësuar hapësirën e fundme • Nuk ka kthim për skedarët e radhës të dëmtimeve

	• Rendimenti më i shpejtë • Nuk kërkon kohë për ndarjen, formimin, fshirjen, dhe arritjen e regjistrave	
Logging në mënyrë lineare	• Ripërtëritja e mediave • Zbatohet për softuer, energji, dështim në aplikim dhe dështim në media • Magazinim afatgjatë • Riktheni skedarët e radhës të dëmtimeve	• Kërkon mirëmbajtje • Proces i ngadalshëm • Asnjëherë nuk ripërdoren logs • Degradoni performancën për shkak të ndarjes periodike të regjistrave të rinj

Burimi: S. Khan et al.

Tabela IV. Krahasimi mes mënyrave të ndryshme të logging (identifikim)

Parametrat e krahasimit	Logging(Identifikim) në mënyrë rrethore	Logging në mënyrë lineare
Alokimi i regjistrave	Njëherë	Periodikisht
Administrimi i mëtejshëm	Më pak (i parëndësishëm)	Më shumë
Ripërdorimi	Po	Jo (Regjistrat lëvizen ose fshihen)
Fillo kthimin (Restart Recovery)	Po	Po
Rekrutimi i të dhënave të humbjes	Jo	Po (Riprodhimi i regjistrave)
Mbishkruan të dhënat e regjistrit	Po	Jo
Kapaciteti i ndarjes së regjistrit	Fundëm	Dinamike

Burimi: S. Khan et al.

2.1.2.1. Regjistrimi cirkular.

"Regjistri qarkor" i referohet pranisë së regjistrit në një formë rrethore. Ngjarjet e ndryshme ruhen në formën e një skedari logesh qarkore që ka një memorie të paracaktuar të alokuar të barabartë me kujtesën e disponueshme të sistemit siç tregohet në Figurën 2. Çdo hyrje e regjistrit ruhet në mënyrë sekuenciale në kujtesë dhe një herë memoria arrin fundin e saj, hyrja e parë e regjistrit automatikisht mbishkruhet nga log-i i krijuar rishtazi [Wyatt 2009]. Procesi vazhdon si një lloj unazë rrotulluese. Nuk ka frikë se shkrimet e mbledhura do të mbushin tepër hapësirën e kujtesës së fundme. Regjistrat qarkullues përdoren për të rifilluar rimëkëmbjen duke u kthyer në transaksionin operativ për shkak të dështimit të sistemit. Menaxheri i radhës rifillohet duke hyrë në dosjen e log-ut pa humbur të dhënat. Gjatë procesit të rifillimit, skedarët e log janë të marrë kundër dosjeve të radhës për të rikrijuar mesazhin e transaksionit. Ripërdorimi i dosjeve të regjistrit për kërkim bëhet përmes pikës së kontrollit [Khan et al. 2012]. Checkpointi prodhon sinkronizim midis të dhënave të radhës dhe skedarëve të regjistrit për të krijuar një pikë konsistence [Scales et al. 2013]. Pika e kontrollit tregon një pikë ku të dyja skedarët e regjistrit dhe të dhënat e radhës kanë të njëjtat të rekorede në të njëjtën kohë. Prandaj, shkrimet rrethore kanë më pak shpenzime administrative në drejtim të zvogëlimit të ndërhyrjes njerëzore. Të gjitha shkrimet menaxhohen automatikisht në një memorie të paracaktuar pa nevojën e memories shtesë për skedarët e zgjatur. Menaxhimi automatik i dosjeve të regjistrit kursen kohë duke zvogëluar futjen, fshirjen dhe arkivimin e regjistrave, gjë që shpejton procesin me xhiro të lartë. Megjithatë, mbishkrimi i të dhënave

ekzistuese shkakton rekorde të ruajtura paraprakisht, shkrimet që humbasin, të cilat mund të ndikojnë në procesin e rimëkëmbjes së përgjithshme. Dosjet e regjistrit në logging rrethore nuk arkivohen për ruajtje afatgjate për shkak të alokimit të tyre të kujtesës së fundme të tipit të unazës.

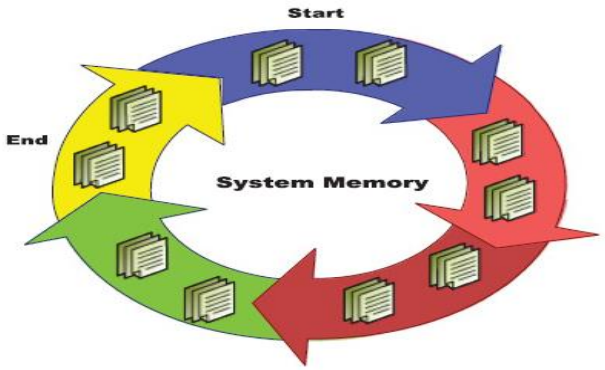

Fig. 2. Generalized circular logging diagram.

Fig. 2. Diagrami i përgjithshëm i regjistrimeve në formë rrethore(ACM Computing Surveys, Vol. 49, No. 1, Article 7, Publication date: May 2016.)

2.1.2.2. Regjistrimi linear.

Regjistrimi linear është procesi i ruajtjes së regjistrave në një hapësirë lineare të kujtesës [Turnbull 2005]. Procesi i rimëkëmbjes është i njëjtë me atë të regjistrit rrethues me më shumë shërbime të shtuara si queue manager(menaxher të stivës), i cili rifillon procesin

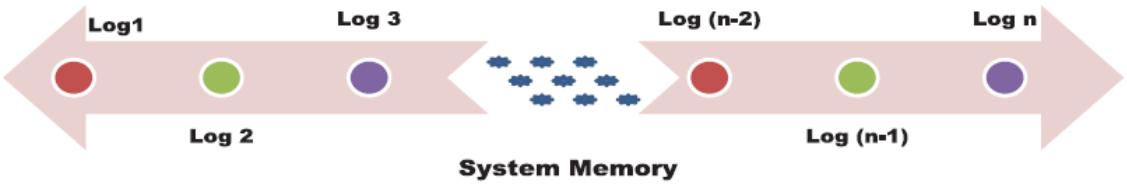

Fig. 3. Generalized linear logging diagram.

Fig. 3. Diagrami i përgjithshëm i regjistrimeve në formë lineare(ACM Computing Surveys, Vol. 49, No. 1, Article 7, Publication date: May 2016.)

në rastin e një skedari të dëmtuar. Regjistrimi linear nuk ka hapësirë të kufizuar të kujtesës, ndërkohë që kufiri i saj është drejtpërdrejt proporcional me kujtesën e sistemit siç tregohet në Figurën 3. Vendet e logut linear regjistrohen në mënyrë sekuenciale brenda një memorie pa mbishkruar shkrimet e mëparshme [Wyatt 2009]. Kur kujtesa është e plotë, shkrimet e mëparshme zhvendosen në një kujtesë

tjetër ose fshihen nga administratori, në varësi të situatës. Kujtesa nuk ka kufi për ruajtjen e regjistrave, kjo varet nga kapaciteti i disponueshëm i kujtesës. Regjistri linear regjistron ngjarjet e transaksionit, si dhe një kopje të mesazheve të vazhdueshme. Persistenca është një pronë e një mesazhi që përdoret për të ruajtur një mesazh në një disk, në bazën e të dhënave ose në një skedar log. Mesazhi i vazhdueshëm është rikuperuar edhe për menaxherin e radhës rifillohet. Logging lineare rimëkëmbin skedarët e radhës duke riprodhuar shkrimet lineare, e cila njihet edhe si rikuperim i medias. Prandaj, log logaritmi kryen si rikuperimin e transaksionit [On et al. 2012] dhe rimëkëmbjen e radhës. Ripërtrirja e transaksionit kryhet duke përdorur pikat e kontrollit dhe rikuperimi i radhës kryhet duke përdorur një kopje të mesazhit të vazhdueshëm. Regjistri linear ka avantazhin e përdorimit të regjistrave për ruajtjen afatgjatë, e cila përdoret për analiza sa herë që kërkohet. Megjithatë, shkrimet lineare përfshijnë mirëmbajtjen për të zhvendosur shkrimet nga një kujtesë në një pajisje tjetër ruajtëse kur kujtesa aktuale arrin kulmin. Zhvendosja e dosjeve të regjistrit ngadalëson proçesin dhe zvogëlon performancën duke alokuar në mënyrë periodike shkrimet.

Vlen të përmendet se zgjedhja e një modaliteti të duhur të logging(identifikimit) kërkon një pasqyrë të kërkesave aktuale. Bazuar në nevojën, mund të adoptohet një logging mode, e cila duhet të përmbushë kërkesat e ndërmarrjes. Regjistrimi qarkor kryen shkrime automatike me performancë të lartë, ndërsa sakrifikon rikuperimin e mesazheve të vazhdueshme nga një skedar i radhës së dëmtuar. Megjithatë, në rastin e logging lineare, hapësira në disk duhet të menaxhohet në mënyrë të përshtatshme në mënyrë që të mos konsumojë të gjithë hapësirën në dispozicion. Bazuar në diskutimin e lartpërmendur, duhet të vlerësojmë secilën prej mënyrave të logging bazuar në koston dhe rrezikun përpara zbatimit të tyre.

2.2. Cloud Computing

Cloud computing është një burim i lidhur i rrjetit për ofrimin e shërbimeve të ndryshme për përdoruesit duke përdorur një komunikim në internet në çdo vend dhe kohë [Armbrust et al. 2010; Gani et al. 2014; Qi et al. 2014]. Burimet në cloud që posedojnë ose jepen me qera nga CSP janë të integruara së bashku për të forcuar aftësinë e llogaritjes dhe ruajtjes [Buyya et al. 2008]. CSP(Cloud Service Providers) është një kompani që ofron shërbime të ndryshme për përdoruesit duke i dhënë akses burimeve cloud. Përdoruesit aksesojnë resurset cloud pa pasur njohuri indepth ose detajet e vendndodhjes dhe pronësisë së tyre. Përdoruesit ngarkohen vetëm në bazë të shfrytëzimit të resurseve cloud dhe një fenomen i tillë njihet si "payas-you-go" në cloud computing [Armbrust et al. 2010]. Një burim mund të përdoret nga shumë përdorues për të rritur efikasitetin dhe rendimentin dhe gjithashtu të zvogëlojë kohën e papunë të resurseve në cloud-computing.

Për më tepër, në ditët e sotme ka qindra CSP që ofrojnë shërbime të ndryshme për përdoruesit bazuar në nevojat e tyre, për shembull, Microsoft, Amazon, Azure, Google dhe të tjerë. Këto CSP mund të kategorizohen në tri kategori kryesore të shërbimit, të cilat njihen gjithashtu si "modele shërbimi" për cloud computing, të tilla si: (a) Infrastruktura-si-shërbim (IaaS), (b) Platform-si-shërbim (PaaS), dhe (c) Software-as-a-service (SaaS)

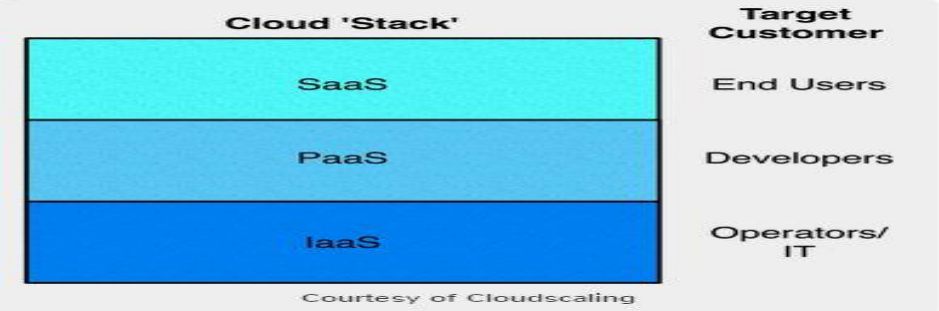

Fig. 6. Ofruesi i shërbimit të cloud-it(Sreenivas Makam's Blog – WordPress.com)

Tabela V. Shitësit Cloud duke ofruar shërbime të ndryshme

Shërbimet Cloud	Përshkrimi	Shitësit e Cloud
Ruajtje si-një-Sherbim (STaaS)	Siguron një sasi të madhe të magazinimit në arkitekturën e cloud për organizata të ndryshme për të arkivuar të dhënat e tyre. Ai ofron ekonomi të shkallës dhe ulje të kostos në drejtim të ruajtjes si krahasim me magazinat lokale në dispozicion.	Amazon S3, Windows Azure Ruatje
Rrjetëzimi-si-një-Shërbim (NaaS)	Për të optimizuar burimet duke ofruar shërbime të rrjetit përmes përdorimit të shërbimeve të tij të transportit. Mund të ofrojë shërbime virtuale të rrjetit për përdoruesit e ndryshëm të integruar me modelet e tjera të shërbimit.	Pertino
Çdo gjë-si-një-Shërbim (XaaS)	Një grup shërbimesh ofron përmes një rrjeti të internetit në infrastrukturën cloud. Për shembull, një CSP ofron shërbime përregjistrime, magazinimin, hetime dhe kështu me radhë.	Google, Microsoft, Hewlett Packard
Të Dhëna të shumta-si-një-Shërbim	Të ofrojë mjete statistikore ose informacione për të ndihmuar	1010data, IBM, AWS

(BPaaS)	organizatat në kuptimin e informacionit të madh të vendosur për të fituar përparësi konkurruese.	
Forenzikë-si-një-Shërbim (FaaS)	Hetoni ngjarje të ndryshme kriminale në internet duke përdorur mjete analitike të larta të integruara me burime informatike me performancë të lartë.	Jo një shitës i specializer akoma
Desktop-si-një-Shërbim (DaaS)	Ofrimi i ndërfaqes virtuale desktop me arkitekturën multi-qiramarrëse në një cloud përmes abonimit mujor të tarifave.	Wipro, Citrix XenDesktop
Grafik-si-një-Shërbim(GaaS)	Ofron teknologji grafike bazuar në cloud për të zbatuar aplikacionin e dizajnit grafik në fund të lartë duke përdorur shfletuesin HTML5.	NVIDIA
Testimi-si-një-Shërbim (TaaS)	Një aktivitet testimi që lidhet me organizatën kryhet në cloud dhe jo nga punonjësit në hapësirën e punës.	Oracle, Njohës

Burimi: S. Khan et al.

[Armbrust et al. 2010]. Në modelin IaaS, përdoruesve u jepet akses në burimet virtuale të cloud computing për të zbatuar aplikimin e saj, por që janë përgjegjës për sigurinë, mirëmbajtjen dhe mbështetjen e aplikacionit të vet [Mell and Grance 2011]. Shembujt përfshijnë Amazon Web Service (AWS), Google Compute Engine (GCE), Rackspace dhe Microsoft Azure. Modeli PaaS përdoret nga zhvilluesit për të zhvilluar aplikacione të reja mbi infrastrukturën e ofruar nga CSP-të. Në PaaS, CSP ndihmon programuesit / zhvilluesit duke ofruar gjuhë të hapura / pronësi, konfigurimin bazë fillestar për komunikim, monitorim, shpërndarje të aplikacionit, shkallëzueshmëri të një aplikacioni, dhe kështu me radhë [Buyya et al. 2008]. Shembujt për PaaS përfshijnë AWS Elastic Beanstalk, Force.com, Apprenda, dhe Heroku. Megjithatë, në SaaS, CSP ofron softuer të plotë për përdoruesit për ekzekutimin e tij. Programi / aplikacioni arrihet nëpërmjet një ueb portali ose arkitekture të orientuar nga shërbimi [Buyya et al. 2009]. Përdoruesit mund të hyjnë në çdo softuer të listuar nga CSP pa shqetësime rreth konfigurimit dhe instalimit të tij. Shembujt e SaaS përfshijnë aplikacionet Google, Gmail, Microsoft 365, Salesforce dhe Cisco WebEx. Për më tepër, shërbime të tjera ofrohen nga CSP për të argëtuar përdoruesit për të përmbushur kërkesat e tyre përmes përdorimit të resurseve cloud. Disa nga shërbimet e ofruara nga CSP-të janë të renditura në Tabelën V. Shumë prej CSP-ve tani kanë filluar të ofrojnë shërbime log-as-a-

service për klientët e tyre duke mbledhur të gjitha llojet e të dhënave të regjistrit [Ellis 2013; Burton 2014; Oppenheimer 2009; Lindvall 2014]. Të dhënat e regjistrit të gjeneruara në aplikacione, servera, pajisje dhe rrjete të ndryshme normalizohen dhe filtrohen për reformatimin përpara përpunimit të mëtejshëm. Të dhënat e regjistrit të mbledhura nga organizata të ndryshme analizohen në resurset cloud për qëllime të ndryshme hetimore. Analiza e regjistrit në cloud jep informacion të dobishëm për klientët, duke përfshirë integrimin e të dhënave, shikueshmërinë e menjëhershme të regjistrit, monitorimin në kohë reale, përshtatjen e formatit të identifikimit, diagnozën e lehtë dhe të thjeshtë, karakteristika të pasura grafike të përdoruesit (GUI), analiza e shkaktarit të rrënjës etj.

2.3. Forenzika Dixhitale

Forenzika dixhitale është procesi për të identifikuar artefakte dixhitale për të hetuar sjelljet e sulmuesit me qëllim të keq [Chung et al. 2012]. Sjelljet keqdashëse të sulmuesit komprometojnë kredencialet sekrete të përdoruesit duke shfrytëzuar privatësinë e tij duke monitoruar, ndryshuar, fshirë dhe kopjuar të dhënat në pajisje të ndryshme [Casey 2009]. Origjina e sulmuesve duhet të hetohet për të parandaluar sjelljet keqdashëse nga shfrytëzimi i të dhënave legjitime të përdoruesve. Disa modele digjitale të procesit të forenzikës ligjore janë propozuar për të kryer hetime në aspekte të ndryshme kërkimore që përfshijnë ushtrinë, biznesin, zbatimin e ligjit dhe industritë e ndryshme. Megjithatë, hulumtuesit e ndryshëm kanë propozuar modele të ndryshme të forenzikës digjitale. Megjithatë, Instituti Kombëtar i Standardeve dhe Teknologjisë (NIST) ka paraqitur katër faza të përgjithshme të forenzikës digjitale në raportin e tyre [Kent et al. 2006], të tilla si grumbullimi, ekzaminimi, analiza dhe raportimi.

Faza e grumbullimit është faza fillestare e forenzikës digjitale në të cilën dëshmitë dixhitale janë mbledhur nga artefakte digjitale. Kjo fazë është jetike përsa i përket mbledhjes së duhur të dëshmive megjithatë, marrja e gabuar e provave do të anojë pjesën tjetër të procesit digjital. Në fazën e ekzaminimit, zakonisht shuma masive e të dhënave të grumbulluara përpunohen për të identifikuar të dhëna të mira ligjore që duhet të hetohen për prova të vlefshme. Integriteti i të dhënave duhet të ruhet duke ruajtur origjinalitetin e saj. Faza e analizës përdoret për të analizuar të dhënat për të identifikuar ndjeshmëritë e ndryshme dhe sjelljet keqdashëse të sulmuesit në të dhënat e ruajtura të mbledhura nga faza e provimit për të përcaktuar shkakun rrënjësor të sulmit. Në shumicën e rasteve kërkohet analizë e drejtpërdrejtë për të kapërcyer intensitetin e sjelljes me qëllim të keq duke identifikuar shkakun rrënjësor të sulmit të shpejtë [Carrier 2006]. Mjetet e njohura të forenzikës digjitale si Sleuth Kit, Encase dhe Toolkit Ligjore (FTK) përdoren për të identifikuar provat e nxjerra nga regjistri dhe dosjet e përkohshme dhe të fshirë, si dhe email, cache, cookies dhe metadata të paraqitura në pajisje të ndryshme. Së fundi, në

fazën e raportimit rezultatet e analizës janë përpiluar në një formë të dokumentit ligjor i cili duhet të paraqitet në gjykatë kundër sulmuesit. Raporti përmban informacion në lidhje me metodën e përdorur për analizën, përzgjedhjen e mjeteve dhe procedurave, veprimet e nevojshme të ndërmarra në secilën fazë të hetimit, rekomandimet për përmirësimin e procesit të ligjor. Formaliteti i raportit varion varet nga situata e hetimit që ndodh.

Dosja log luan një rol thelbësor në forenzikën digjitale për të zbuluar veprimet e fshehura të sulmuesit duke regjistruar hapat e tij vijues [Chung et al. 2012]. Ai ndihmon hetuesit në zbulimin dhe nxjerrjen e informacionit të vlefshëm, modelimin dhe analizimin e ngjarjeve të ndryshme të kryera gjatë sulmit. Përveç kësaj, hetimi i dosjeve të regjistrit ofron njohuri të vlefshme duke ofruar modele të sjelljes së përdoruesve keqdashës gjatë ndërveprimit të tyre me sistemin, rrjetin dhe aplikacionin. Korrelacioni i dosjeve të regjistrit konsiderohet një metrik i rëndësishëm në hetimin e dosjeve të regjistrit në sistemet e shpërndara siç janë cloud-computing. Korrelacioni i skedarëve të regjistrit përmban ngjarje të ndryshme të përfshira në përcaktimin e marrëdhënieve ndërmjet fragmenteve të të dhënave, analizimin e të dhënave të fshehura dhe identifikimin e domethënies së skedarëve nga sistemi, rrjeti, aplikacioni dhe skedarët e logut të filtruar. Rindërtimi i të dhënave nga dosjet e llogaritjeve dhe arritja në përfundim konsiderohet gjithashtu një pjesë e aktiviteteve të korrelacionit. Si rezultat, dosjet e regjistrit rrisin besueshmërinë dhe pranueshmërinë e provave në një proces dixhital.

Kapitulli 3. Cloud Log Forensis

3.1 Shërbime ligjore

Përveç shërbimeve të ndryshme të regjistrit, informatika cloud ofron shërbime ligjore duke hulumtuar të dhënat e regjistrit për të identifikuar dobësi të ndryshme dhe sjellje me qëllim të keq [Taylor et al. 2011]. Të dhënat e regjistrit të mbledhura nga CSP-të ruhen në një memorie të vazhdueshme, të sigurt për të hetuar mjete dhe algoritme të ndryshme analitike për të përcaktuar dhe sjellje me qëllim të keq.

Përdoruesit mund të hyjnë në të dhënat e tyre të regjistrit në kohë reale duke ditur tendencat e të dhënave dhe sjelljen e tyre me informacione të hollësishme. Për të siguruar të dhënat e regjistrit në një cloud, një CSP përdor metoda të ndryshme të enkriptimit të të dhënave origjinale të regjistrit të padukshëm për

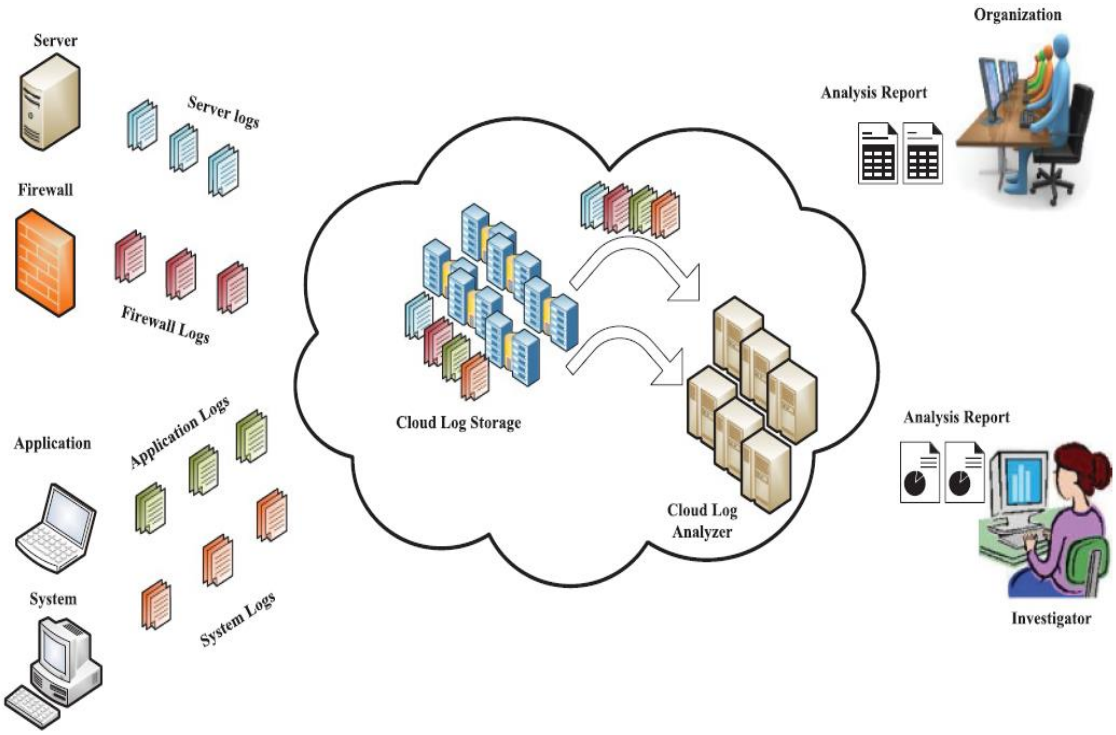

Fig. 4. Generalized cloud log forensics diagram.

Fig. 4. Diagrami i përgjithshëm i cloud log forensics(ACM Computing Surveys, Vol. 49, No. 1, Article 7, Publication date: May 2016.)

ndërhyrësit kur ata përpiqen të fitojnë akses. [Sundareswaran et al. 2012]. Megjithatë, CSP-të duhet të krijojnë një nivel besueshmërie për të kënaqur përdoruesit për sigurimin e të dhënave të tyre të regjistrit në cloud-computing. Burimet kompjuterike të performancës së lartë, servera të mëdha të ruajtjes, qindra mjete analitike, fuqi njerëzore ekspertësh, një rrjet komunikimi të shpejtë dhe një përgjigje në kohë reale i bëjnë përdoruesit të ndihen rehat duke përdorur log-as-a-service cloud për të dhënat e tyre të regjistrit. Ndonjëherë një organizatë e di se kur dhe ku ka lindur një kërcënim, por mungesa e burimeve nuk i mundëson asaj që të analizojë plotësisht situatën mirë, e cila pastaj bëhet e kushtueshme. Sot, ofruesit e shërbimeve të log-as-a-service ofrojnë shërbime të përshtatshme për konsumatorët, duke përfshirë forenzikë, për të mirëmbajtur të dhënat e tyre të logaritjeve duke iu përgjigjur analitikës, dokumentacionit, statistikave, trendeve, tabelave dhe grafikëve brenda interfaces GUI të përdorshme. Sipas Gartner 2015 Magnet Quadrant për Sigurinë e Informacionit dhe Menaxhimin e Ngjarjeve (SIEM),

Splunk dhe LogRhythm janë konsideruar liderët e tregut në të dhënat e inteligjencës së sigurisë që gjithashtu ofron shërbime të menaxhimit të logëve të plotë për klientët e tyre.

Cloud computing jo vetëm siguron shërbime forenzikë për skedarët e log-ut të mbledhura nga jashtë cloud, por gjithashtu përfshin shërbime forenzike për skedarët e log-ut të mbledhura nga pajisjet, sistemi, sistemet operative, makinat virtuale, rrjetet dhe resurset e tjera brenda cloud. Për shembull, ekzekutimi i një aplikacioni që ekzekutohet në një server aplikacioni regjistrohet nga CSP ose një imazh i një makine virtuale në një burim regjistrohet dhe ruhet në një burim magazinimi cloud nga një përdorues i makinës virtuale. Koncepti i përgjithësuar i CLF është ilustruar në Figurën 4. Për më tepër, çdo model shërbimi cloud ka kritere të ndryshme për logging në varësi të aksesit të të dhënave. Për shembull, një përdorues në një IaaS lehtë mund të mbledhë dhe të kontrollojë të dhënat e makinës virtuale, ndërsa një përdorues që ekzekuton një aplikacion në një SaaS nuk mund të hyjë në regjistrat e aplikacioneve për shkak të kufizimit të siguruar nga CSP [Sang 2013]. Në cloud-in, shkrimet gjenerohen kryesisht nga CLF-ja dhe hetuesve u ofrohet akses i kufizuar në to. Vartësia nga CSP bën procesin e hetimit të identifikimit të problemeve rrënjësore të dobësive, përgjatë një linje kohore të caktuar më të komplikuar për hetuesit. Hulumtuesit tani kryesisht fokusohen për të minimizuar varësinë nga CLF-ja në hetimin e të dhënave të regjistrit të cloud computing.

Rëndësia e CLF po rritet për shkak të numrit të problemeve që lidhen me hetimin e regjistrit në cloud [Birk 2011]. Probleme të tilla përfshijnë decentralizimin, aksesueshmërinë, ruajtjen, mbajtjen, disponueshmërinë dhe formatet e logaritmeve të rastit të dosjeve të regjistrit. Hetuesi ligjor përballet me problemin e decentralizimit të dosjeve të logit për shkak të serverëve të shumtë [Shams et al. 2013]. Mbajtja e regjistrit është gjithashtu një problem për hetuesin ligjor në kuptimin e asaj se sa kohë duhet të ruhet një skedar log për të qenë i dobishëm për analizën loh [Popovic dhe Hocenski 2010]. Megjithatë, politika e mbajtjes së regjistrit varet nga politikat e CSP dhe SLA me përdoruesit, organizatat dhe ndërmarrjet. Në mënyrë të ngjashme, natyra e paqëndrueshme e resurseve cloud (të tilla si makinat virtuale të caktuar për përdoruesit për një periudhë të caktuar kohore) i bën skedarët e logit të disponueshme për periudha kohore më të shkurtra.

3.2. Logjika e re e forenzikës: gjendja e artit

Në këtë seksion, unë klasifikoj forensikën e gjendjes aktuale të cloud-it në tri grupe kryesore si më poshtë: hetimi, sinkronizimi dhe siguria. Secili grup krahasohet më tej me karakteristika të ndryshme që përfshijnë objektivin, metodën, zgjidhjen, konfigurimin, mjetet dhe regjistrat e synuar. Karakteristikat objektive theksojnë qëllimin kryesor të zgjidhjes së propozuar; karakteristikat e metodës shpjegojnë aksesin e përdorur në zgjidhje; karakteristikat e zgjidhjes na drejtojnë drejt një rezultati; karakteristikat e

konfigurimit përshkruajnë infrastrukturën e përdorur për të testuar zgjidhjen e propozuar; karakteristikat e mjeteve tregojnë për aplikimin dhe paketën e përdorur në eksperiment; dhe karakteristikat e regjistrave të synuar tregojnë llojet e regjistrave të përdorur për eksperimentet. Bazuar në karakteristikat e lartpërmendura, literatura e hulumtimeve të ndryshme CLF është renditur në Tabelën V.

3.2.1. Hetimi.

Hetimi është qëllimi kryesor i CLF për të gjetur dobësitë e pranishme në skedarët e regjistrit të cloud. Aktualisht, hulumtime të ndryshme janë kryer për të hetuar skedarët e regjistrit të cloud. Sigurimi i informacionit të rëndësishëm e bën procesin e hetimit të shpejtë dhe efikas. Në Thorpe et al. [2013a], struktura e orientimit të shërbimeve CLF (SOA) është propozuar për të rindërtuar ngjarje të ndryshme që ndodhin në hostët e VM, platformat e cloud-it dhe aplikacionet. Rindërtimi i ngjarjeve ndihmon ekipin e sigurisë për të identifikuar aktivitetet e dëmshme të kryera nga sulmuesi gjatë sulmit të tij. Në Patrascu dhe Patriciu [2014], është propozuar një arkitekturë forensike cloud log për monitorimin e aktiviteteve të përdoruesve në cloud-informatikë.

Tabela VI. Klasifikimi i Ligjit për Regjistrin Cloud

Klasifikimi	Objektivat	Metoda	Zgjidhja	Vendosja (Setup)	Mjetet	Logs target	Referencat
Investigimi	Të sigurohet një qasje proaktive për të siguruar gjenerimin e loguve për hetim ligjor.	Zbatimi i regjistrave të aplikacionit në MSA.	Instalime me tre nivele në krye të infrastru--kturës së cloud.	Testbed	Django, JavaScript, Apache, MySQL	Regji-strat e apliki-meve	[Marty 2011]
	Hetimi i regjistrave të cloud bazuar në arkitekturën e orientuar drejt shërbimit ligjor.	Skenari i ndërveprimit të aktorit cloud.	Kuadri ligjor i auditimit cloud.	Shpjegimi teorik	N/A	Regji-stra të ndrys-hëm	[Thorpe et al 2013a]
	Zgjidhja për të ndihmuar hetuesit për të monitoruar aktivitetet e përdoruesit në cloud-computing.	Arkitektura e cloud logging.	Shtresa e bazuar ligjore.	Testbed	Apache HTTP server, PostgreSQL	Regji-trat VM	[Patrascu and Patriciu 2014]
	Për të monitoruar aksesin në	Flogger: Një regjistrues	Logging i ciklit të jetës në	Testbed	PostgreSQL 9.0, MonetDB	VM regjis-tra,	[Ryan et al.

	skedarë dhe transferimet në kuadër të cloud computing nëpërmjet centralizimit të regjistruesve.	me bazë File-centric.	të dy VMs dhe PMs.			regjis-trat e maki-neriv e fizike	2011a]
Sinkronizimi	Vendosni sinkronizimin e logaritmit VM.	Kufizimet formale.	Hartimi i transfor-mimit.	Qendra e të dhënave VMWare essx3i	N/A	Regji-strat VM	[Thorpe et al 2011c]
	Sinkronizimi i regjistrave VM në zona të ndryshme kohore të tilla si mjedisi VM jo-nacionale.	Mekanizmi formal i përkohshëm.	Auditori Global Log VM.	Qendra e të dhënave VMWare essx3i	N/A	Regji-strat VM	[Thorpe et al 2011d]
	Sinkronizimi i ngjarjeve të regjistrit në sistemin e shpërndarjes forenzike llogarit mjedisin e databazës së cloud.	Parametratë formale.	Përbërja e sinkroniz-uar e ngjarjeve të regjistrit.	Qendra e të dhënave VMWare essx3i	Kontrollue si global i logaritmëv e të makinës virtuale	Regji-strat e Siste-mit Hype-rviso r	[Thorpe et al 2012b]
Sigurimi	Transferoni shkrimet e sigurta nga një VM në një tjetër VMto për tu mbrojtur nga ngatërrimi	Zëvendësim i i bibliotekës në VM.	Shkrimi i kodit shtesë në bibliotek-ën libc.	Testbed	N/A	Regji-strat VM	[Sato and Yamauchi 2013]
	Mundësoni fshehtësinë dhe privatësinë e të dhënave të përdoruesit të cloud.	Përshkrimi skematik.	Procesi i fundit i testimit të evidencë-s dhe verifikim-it.	Prototip	OpenStac k, Snort	Regji-strat e VM, Regji-stri i akses-sit në rrjet	[Shams et al. 2013]
	Ekzekutoni pyetjet në shkrimet e cloud pa ndikuar në	Skema e kodimit homomorfik.	Gjenerat-or i tageve anonime.	Prototitp	Gjeneruesi i regjistrit: Vetë i zhvilluar	Regji-stra të ndrys-hëm	[Prabha et al 2014]

	konfidencialitetin dhe privatësinë.						
	Për të aplikuar mekanizëm të sigurt të logging në çdo mekanizëm të log.	Gjuhësia Forenzike e Njohur (FAL).	Regjistrimi i sistemit dhe aplikimit.	Zhvillimi i programimit	Zhvillimi i përpiluesit FAL duke përdorur LISA	Regji-stra-të ndrys-hëm	[Shams et al 2014]

Burimi: S. Khan et al.

Arkitektura e bazuar në shtresa përdoret për të parë çdo ngjarje në shtresa të ndryshme duke e ndarë monitorimin e përgjegjësive ndërmjet shtresave që ndihmon në gjetjen e trazirave me qëllim të keq, gjatë procesit të hetimit. Në Ryan et al. [2011a], një skedar-qendror i makinës fizike (PM) dhe logger me bazë VM (Flogger) është propozuar për të monitoruar operacionet e skedarëve në cloud-computing. Flogger mbledh shkrimet nga PM dhe VM për të dhënë informacion mbi skedarët e aksesuar në cloud. Informatat gjithëpërfshirëse të regjistrit të siguruara nga Flogger ndihmojnë në identifikimin e prejardhjes së dosjeve të përdorura nga përdoruesit e dëmshëm përmes analizimit të ngjarjeve në skedarët e regjistrit.

3.2.2. Sinkronizimi.

Sinkronizimi i skedarëve të logut cloud ofron qëndrueshmëri në log të dhëna të vendosura në vende të ndryshme në cloud-computing. Konsistenca e të dhënave të regjistrit në skedarë të ndryshëm ndihmon hetuesit ligjorë për të kontrolluar ndryshimet e bëra nga sulmuesi gjatë sulmit. Dosjet e regjistruara të paqëndrueshme mund të japin rezultate të njëanshme në hetim dhe nuk do të çojnë në burimin e vërtetë të sulmit. Hulumtime të ndryshme janë kryer në sinkronizimin e dosjeve të logut të cloud për të ofruar një platformë të besueshme për CLF.Në Thorpe et al. [2011d], një auditor global logjistik i makinës virtuale i bazuar në softuer është zhvilluar për të sinkronizuar shkrimet virtuale të serverëve në zona të ndryshme kohore në një mjedis jo-VM. Auditori përdorte modele të të dhënave të përkohshme të bazuara në pikë dhe në bazë të intervalit për të diskutuar sinkronizimin në skedarët e regjistrit që ndihmojnë në hetimin për skedarët e logut me qëllim të keq dhe migrimin e të dhënave në zona të caktuara kohore të cloud-computing. Sinkronizimi i përbërjes së ngjarjeve në regjistrat e VM nga burime të ndryshme cloud bëhet përmes operatorëve binarë si disjunksioni, lidhja dhe sekuenca. Si rezultat, ngjarjet e përziera të regjistrave të ndryshëm VM ofrojnë informacion të mjaftueshëm për të identifikuar burimet reale të sulmit.

3.2.3. Sigurimi.

Përdoruesit keqdashës janë më të interesuar në kalimin e të dhënave në logun cloud për shkak të ngjarjeve të regjistruara që mund të gjurmojnë në origjinën e sulmeve [Khan et al. 2016]. Sigurimi i dosjeve të regjistrit cloud nga përdoruesit keqdashës është një sfidë drastike. Burimet e shumëfishta dhe

heterogjene, infrastrukturat e shpërndara, rrjetet virtuale, kontrollet e decentralizuara dhe sasi masive të të dhënave në cloud-in e bën më të vështirë për të siguruar skedarët.Në Sato dhe Yamauchi [2013], VM logs files transferohen në një mënyrë të sigurt nga një VM në një VM tjetër duke modifikuar bibliotekën "libc" në operacionin Linux dhe FreeBSD sistemet. Zakonisht, skedari log VM mblidhet nga introspekti VM që nuk është i optimizuar për mbrojtjen e regjistrit. Sapo kërkesa e VM-së për skedarin e skedarit, Monitor Virtual Machine (VMM) nxjerr shkrimet nga hapësira e kernelit dhe e dërgon atë te demoni SYSLOG. Sulmet malware të nivelit kernel nuk mund të ndryshojnë skedarët e regjistrit në demonin SYSLOG. Prandaj, zgjidhja e propozuar ndihmon CLF-në për të hetuar regjistrimet VM në një vend të sigurt dhe të besuar. Në Shams et al. [2013], një hetim i sigurtë i ofrohet hetuesve ligjorë, duke siguruar konfidencialitetin dhe integritetin e regjistrave VM. Integriteti i regjistrave të VM mbahen duke përdorur Dëshmin e Kalimit të Kaluar (PPL) dhe Zinxhirin e Identifikimit (LC). PPL-ja siguron një skemë të dukshme për të parandaluar përdorimin keqdashës të ndryshimit të skedarëve të regjistrit, ndërsa LC-ja mban verifikimin e sekuencës së saktë për skedarët e logut cloud që ofrohet nga CSP.Megjithatë, operacioni cloud mund të kryhet në të dhënat e regjistrit të koduar pa shfrytëzuar konfidencialitetin dhe privatësinë e të dhënave legjitime të përdoruesit [Khan et al 2015]. Hetuesit ligjorë konfirmohen për origjinalitetin e dosjeve të logut, sepse dosjet e logit janë të koduara para se t'i dërgojnë ato. Ndihmon në identifikimin e burimit të vërtetë të sulmeve përmes analizimit të regjistrave të ndryshëm nga cloud në zbulimin e ngjarjeve me qëllim të keq.Integriteti i skedarëve të logut cloud lejon CLF që të ketë dëshmi të sakta të nxjerra nga dosjet origjinale të regjistrit. Për më tepër, duke përdorur FAL(Gjuha informuese forensic), struktura e vet log mund të përcaktohet dhe të analizohet në skedarin e logut të bazuar në strukturën e përcaktuar të log-ut. Ky tipar ndihmon hetuesit ligjorë për të kapërcyer problemin e heterogjenitetit të formave të regjistrave të hasura gjatë procesit të hetimit.

3.3. Log-si-një-shërbim: Menaxhimi i logut

Regjistrat janë të dhënat për kapjen e ngjarjeve të ndryshme që ndodhin në një sistem, rrjet, ose proces përgjatë një afati kohor të specifikuar [Chuvakin et al. 2013]. Çdo rekord në regjistër specifikon informacionin që lidhet me hapat vijues që ndodhin gjatë kohës së sistemit, rrjetit ose ekzekutimit të procesit. Rritja në shkrimet e ndryshme i bën organizatat të miratojnë menaxhimin e regjistrit për trajtimin e duhur të regjistrave brenda infrastrukturës ekzistuese. Megjithatë, rritja e numrit dhe frekuencës së regjistrave e vështirësojnë një organizatë për të menaxhuar regjistrimet brenda kontekstit të burimeve të pakta, stafit administrativ dhe aksesin e sigurisë.

Mundësia më e mirë për të përballuar problemet e lartpërmendura është përdorimi i shërbimeve të "cloud-as-a service" të cloud computing [Abbadi 2014]. Në ditët e sotme, shumë organizata përdorin shërbimet e regjistrit të një CSP për të thjeshtuar menaxhimin e tyre të regjistrit. Log-as-a-service CSP ndihmon

organizatat në menaxhimin e regjistrave, të tilla si integrimi i të dhënave të regjistrit operacional nga vende të ndryshme, shikimi i çastit të regjistrit, monitorimi i regjistrave në kohë reale, të dhënat e kërkimit dhe të filtrave dhe shumë më tepër. Organizatat përdorin shërbime log-as-a-service thjesht duke kaluar shkrime të ndryshme për një CSP për menaxhimin brenda infrastrukturës së cloud. Fotografi log janë transferuar në cloud në mënyra të ndryshme në varësi të log management e CSP. Për shembull, Log entries (hyrjet log) u ofron klientëve mundësi të shumta për të dërguar të dhënat e tyre të regjistrit në serverin e cloud-it, domethënë, hyrjet me bazë agjenti, dërgimi SYSLOG, hyrjet e bazuara në aplikacione dhe hyrjet me bazë tokësore. Regjistrimi i bazuar në aplikacione kryhet përmes regjistrimit të aplikacioneve të siguruara për mbledhjen e regjistrave duke përdorur gjuhë të ndryshme programimi. Token-based logging ofron raste të shumta log nga vende të ndryshme në një enë të vetme në ndërfaqen e përdoruesit Logentries. Kjo metodë përdoret për organizatat e mëdha që duhet të regjistrojnë të dhëna nga vende të ndryshme të shpërndara. CSP siguron analiza të ndryshme të regjistrit për organizatën duke përdorur burime të larta llogaritëse, mjete të fuqishme analitike potenciale dhe resurse cloud. CSP përdor burime të larta llogaritëse duke kombinuar mijëra kompjuterë në qendra të dhënash të ndryshme. Për shembull, Amazon ka përdorur 26,496 bërthama CPU, 106TB of memory dhe një ndërlidhje 10Gbit Ethernet për të ndërtuar një grumbull të lartë llogaritës. Në mënyrë të ngjashme, mjetet analitike potenciale të larta si sumo logic, tracker ngjarjesh, Scalyr dhe të tjerë përdoren nga CSP për të kryer analizë të hollësishme të logaritjeve në ofrimin e informatave të dobishme për klientët e tyre. Log-as-a-service kursen kohën, kosto dhe ekspertët e kërkuar nga një organizatë për të analizuar të dhënat e regjistrit. Seksioni i mëpasshëm shpjegon disa nga CFL-të që ofrojnë shërbim log-as-a-service për përdoruesit dhe organizatat nga perspektiva të ndryshme. Një përshkrim i shkurtër në lidhje me krahasimin e log-si-shërbim të CSP është përshkruar në Tabelën VII.

Krahasimi i CFL-ve që ofrojnë shërbimin log-as-a-service është bërë sipas parametrave të ndryshëm që theksojnë kompetencën bazë të secilit. Parametra

Tabela VII. Përshkrimi i Parametrave të Përdorura për Krahasimin e Zgjidhjeve të Shërbimeve Log-As-A-Service

Krahasimet	Përshkrimi
Forensik(Hetuesit)	Institucionet e hetimit të ofruara nga CSP për të analizuar skedarët e regjistrit për dobësi të ndryshme.
Aksesi	Përdoruesit lirisht kontribuojnë në log-as-a-services nëpërmjet aksesit në kodet me kod të hapur ose janë të kufizuar nga CLF-të që të kenë licenca të komercializuara.

Çmimi	Tregon ose log-as-a-services janë ofruar falas nga CSPs për klientët e tyre ose ata të paguajnë një shumë për të siguruar shërbimet e hyrjes(logging).
Platforma Mobile	Platforma e lëvizshmeLog-si-shërbime të ofruara nga PGP-të është i arritshëm në pajisjet mobile duke përdorur aplikacione mobile.
Regjistrimi i personalizuar	Një strukturë e ofruar nga CLF-të për përdoruesit e saj për të modifikuar përmbajtjen e dosjeve të regjistrit bazuar në kërkesat e tyre.
Regjistrimi i përplasjeve	Crash loggingServices dhënë nga CSPs për të rivendosur fotografi log nga gjendja e saj e mëparshme e shpëtuar pas crashes e dosjeve të log.
Dashboard	Dashboard GUI i siguruar nga CSPs për të lehtësuar përdoruesit në aksesin e analytics log përmes grafiku, grafikët, dhe rezultatet statistikore.
Formati i Regjistrimit (Log Format)	Formati i identifikimit CSP siguron formate të logaritjeve të vetme ose të shumëfishta për të bërë skedarë të regjistrit.
Enkriptimi	Të dhënat log janë të siguruara në skedarët log
Siguria	Kanali i sigurt i ofruar për përdoruesit nga CSP-të për të hyrë në dosjet e regjistrit në cloud.
Avantazhet	Përfitimet kryesore të ofruara nga PGP-të për përdoruesit në aspektin e shërbimeve të log.
Kapaciteti	Limiti i volumit i siguruar nga CSP për të regjistruar të dhënat në skedarët e regjistrit.
Suporti i OS	Një sistem operativ i përdorur nga CSP-të në sigurimin e log-as-a-services për përdorues të ndryshëm.
Instalimi	Niveli i përpjekjeve kërkohet nga përdoruesit për të konfiguruar log-as-a-services të marra nga CLF.

Burimi: Unë

e krahasimit përfshijnë forenzikë, akses, çmim, platformë mobile, regjistrimi i personalizuar, regjistrimi i përplasjeve,dashboard, format log, encryption, sigurinë, avantazhet, kapacitetin, mbështetjen e OS dhe instalimin, të cilat përshkruhen shkurtimisht në Tabelën VI. Parametri ligjor tregon strukturën e hetimit të ofruar nga CLF-të për përdoruesit e tyre në lidhje me regjistrimet e regjistrit. Siç tregohet në Tabelën VII, CLF-të ofrojnë hetime ligjore për zbulimin e ndonjë ndërhyrjeje dhe cenueshmërisë që gjendet në regjistrimet e ndryshme të regjistrit. Parametri i aksesit tregon nëse log-as-a-service është një burim i hapur ose nëse ajo është dhënë nën një markë tregtare të pronarit. Parametri i çmimit i ndihmon përdoruesit të dinë nëse shërbimi i log-si-një-shërbim i ofruar nga CSP paguhet ose falas (gjykim i lirë). Parametri i platformës mobile tregon sistemet operative të lëvizshme të mbështetura nga CSP-të e ndryshme për shërbimin e tyre log-as-a-service si iOS ose Android. Parametri i identifikimit me porosi tregon se përdoruesit mund të vendosin se çfarë duhet të përfshihen në skedarin e skedarit për të përmbushur kërkesat e tyre [Samudra 2005]. Prandaj, përdoruesit e ndryshëm mund të kenë fusha të

ndryshme të regjistrit në dosjet e tyre të regjistrit. Në mënyrë të ngjashme, parametri i regjistrimit së përplasjeve përcakton objektin e regjistrimit që kap gjendjen aktuale të sistemit para se sistemi të ulet (crashes) [Yang et al. 2014]. Regjistrimi i Crash është shumë i dobishëm në një situatë ku sistemi shpesh rrëzohet. Parametri dashboard tregon GUI të siguruar nga CSP për të parë analizën e të dhënave të regjistrit në një mënyrë të lehtë dhe të thjeshtë. Parametri i formatit të identifikimit tregon se çfarë lloje të aksesi në formatin e regjistrit lejohen nga CSP që të regjistrojnë të dhënat. Për shembull, ofron një format të vetëm të regjistrimit ose formatin e personalizuar sipas kërkesave të përdoruesve, ku përdoruesit mund të krijojnë formatin e tyre të regjistrimit. Parametri i enkriptimit tregon algoritmet e enkriptimit të aplikuara për të regjistruar të dhëna për ta mbrojtur atë nga sulmues të ndryshëm. Në mënyrë të ngjashme, parametri i sigurisë tregon aksesin e siguruar nga CSP në të dhënat e regjistrit të përdoruesve në cloud.Parametri i avantazheve tregon shërbimet e kompetencës bazë të CLF-së në ofrimin e shërbimeve të menaxhimit të regjistrit për përdoruesit. Parametri i kapacitetit thekson vëllimin e të dhënave të regjistrit të menaxhuara nga PGJS. Parametri i mbështetjes OS tregon sistemet operative të mbështetura nga CSP për log-as-a-service. Parametri i instalimit tregon nivelin e vështirësisë në instalimin dhe konfigurimin e klientit CSP log-as-a-service.

3.3.1. IBM Smart Cloud Analytics

Analiza IBM Smart Cloud është një kornizë e analizës së regjistrit që përdor IBM cloud për të analizuar të dhënat operacionale të një ndërmarrjeje të integruar me burime të ndryshme [Ellis 2013]. Ndihmon në identifikimin, izolimin, analizimin dhe zgjidhjen e problemeve operacionale të lidhura me regjistrimet(logs), dokumentet mbështetëse, ngjarjet dhe parametrat. Për më tepër, ai redukton kohën e përpunimit të nevojshme për të kryer analiza rrënjësore duke zbatuar kërkimin, filtrimin dhe vizualizimin e shpejtë të të dhënave në një ndërfaqe të vetme aplikimi. Regjistrat e ndryshëm, duke përfshirë loget e Internetit, shkrimet e Windows, Syslogs dhe Shkrimet Delimiter Separated Value (DSV), janë të integruara me shërbime logjike të rëndësishme për të kryer analiza të sakta dhe të shpejta. Analiza analitike e IBM SmartCloud përfshin më shumë karakteristika që e bëjnë atë një nga ofruesit kryesorë të log-as-a-service në treg, me përmirësimin e disponueshmërisë së shërbimit, kohën e reduktuar të riparimit, mesazhet paralajmëruese dinamike, ndarjen e çështjeve që lidhen me fusha specifike , kërkimi i shpejtë i indeksit dhe rezultatet e kërkimeve të vizualizuara.

3.3.2. Papertrail

Papertrail siguron log-as-a-service për përdoruesit përmes shfletuesit, API, dhe ndërfaqen e linjës së komandës [Lindvall 2014]. Objektivi kryesor i Papertrail është që të sigurojë menaxhimin e regjistrit të pritur për të dhëna të ndryshme të regjistrit të integruar nga burime të ndryshme, duke përfshirë SYSLOG,

skedarët e skedave të tekstit, apache, MySQL, ngjarjet e dritareve, routers dhe firewalls. Dosjet e tekstit trajtohen nga Papertrail duke përdorur sisteme skedari që janë të paarritshëm përmes linjës së komandës, webit ose email-it. Të dhënat e kërkuara në skedarët e regjistrave të tekstit janë të izoluara dhe shpërndahen në aplikacione, sisteme dhe direktori të shumta për qëllime të përpunimit të menjëhershëm dhe të sigurisë. Papertrail aprovon sigurinë e të dhënave të regjistrit duke siguruar encryption TLS dhe verifikimin e bazuar në certifikim për hostin e destinacionit. Në fund të çdo dite, Papertrail automatikisht arkivon mesazhet e logut dhe meta të dhënave në Amazon S3 dhe ofron një zgjedhje opsionale për përdoruesit për të ruajtur një kopje në vendin e ofruar.Shkrimet e krijuara nga Papertrail janë në formatin e ngjeshur Gzip me vlera të ndara në tab, për shembull: "Tape / Papertrail / logs / 98765 / dt = 2014-12-24 / 2014-12-24.tsv.gz." Tape "Është emri i vendit," 98765 "është log id, dhe" dt = 2014-12-24 "është data, ku" 2014- 12-24.tsv.gz "është zgjerimi i skedës së ngjeshur Gzip me datën e specifikuar .

3.3.3. Logentries

Logentries është një kompani cloud nga Irlanda që ofron shërbime softuerike për të bërë menaxhime të regjistrimeve dhe analiza bazuar në kërkesat e ndryshme të përdoruesit [Burton 2014]. Objektivi kryesor i Logentries është që të japë rezultate të analizës në kohë reale me më pak vonesa në kohë dhe kënaqësi më të madhe të përdoruesve. Logentries mbledh regjistra të ndryshëm dhe i analizon ato përmes sistemeve të softuerit duke përdorur hapa para-përpunimi si filtrimi, korrelacioni dhe vizualizimi i të dhënave të regjistrit. Kërkimi intuitiv i regjistrit të Logentries ndihmon përdoruesit përmes shkrimit të fjalëve të thjeshta, shprehjeve të rregullta dhe frazave. Logentries ofrojnë një strukturë të zbulimit të anomalisë për të përcaktuar ndryshimet që ndodhin brenda parametrave të pyetjeve të kërkimit kohë pas kohe. Shërbimet e shumëfishta grafik të Logentries ndihmojnë përdoruesit të krijojnë një pamje të vetme. Ato ndihmojnë përdoruesit, hetuesit ligjorë dhe pronarët e ndërmarrjeve për të parë shumë rezultate të kërkimit në një ndërfaqe të vetme me të dhëna të organizuara dhe të strukturuara.

3.3.4. Splunk Storm

Splunk Storm është një softuer i menaxhimit të regjistrit i bazuar në cloud që ndihmon përdoruesit në monitorimin, diagnostikimin dhe zgjidhjen e problemeve të aplikacioneve të ndryshme në cloud, të ekzekutuara në platforma të ndryshme, duke përfshirë AWS, Google App Engine, Heroku, Rackspace dhe të tjerë [Baum 2014]. SplunkStorm mbledh të dhënat e makinës të gjeneruara nga serverat, faqet e internetit, aplikacionet, si dhe të dhënat e rrymës së klikimit, të dhënat e thirrjes, transaksionet në internet dhe aktivitetet e ndryshme të rrjetit. Të dhënat e mbledhura janë të renditura për të identifikuar dhe zgjidhur llojet e ndryshme të çështjeve të aplikimit. Shërbimet e SplunkStorm ndihmojnë përdoruesit të kryejnë kërkime mbi të dhënat historike dhe aktuale të makinës, ngjarjet specifike të filtrave, lidhin

transaksionet e komponentëve të ndryshëm të aplikimit, përcaktojnë analizën e trendeve të parametrave të ndryshëm operacionalë, ndajnë projektet e tyre me miqtë dhe kolegë, dhe të gjenerojë raporte për zgjidhjen e çështjeve brenda të dhënave. SplunkStorm është shfrytëzuar më së miri nga zhvilluesit për sa i përket gjenerimit të analizave statistikore për aplikacione, duke analizuar ngjarje të ndryshme përmes regjistrimeve semantike, kërkimeve dhe aplikimeve të shtrydhjes, dhe defekteve të performancës. SplunkStorm gjithashtu ndihmon në monitorimin e disponueshmërisë dhe performancës së aplikimit, monitorimin e aktiviteteve të përdoruesit dhe identifikimin e modeleve të rrezikut për kërcënime të ndryshme si rrjedhjet e të dhënave dhe sulmet e dhunës.

3.3.5. Loggly

Loggly është një ofrues shërbimi për menaxhimin e logut të cloud që bazohet në Shtetet e Bashkuara që synon të ofrojë akses të lehtë me analizë të centralizuar të të dhënave të regjistrit tek klientët e tyre [Oppenheimer 2009]. Loggly mbledh të dhënat e regjistrit direkt nga burime të ndryshme ose pajisje, domethënë routers, firewalls, serverë, pajisje ruajtëse dhe hostë të ndryshëm, dhe gjeneron një raport të vizualizuar në kohë reale. Loggly ndihmon përdoruesit për të kontrolluar statusin e aplikacioneve, faqeve të internetit dhe shërbimeve të tyre dhe si veprojnë sipas bazave të ndryshme kohore. Nuk është një punë e lehtë për një kompani për të mbledhur dhe analizuar miliona ngjarje në baza ditore, të cilat mund të kërkojnë infrastrukturë të madhe. Loggly madje ndihmon klientët për të parë analizat e trendit të të dhënave të tyre të regjistrit për të kërkuar çështje të ndryshme dhe ngjarje duke hyrë në ndërfaqen e vizualizuar nëpërmjet shfletuesit të internetit. Shërbimet e thjeshta dhe të thjeshta të menaxhimit të logit e bëjnë Loggly një mundësi më atraktive midis kompanive të ndryshme të aplikimit në cloud. Si rezultat, në fund të vitit 2014, Loggly kishte regjistruar më shumë se 750 miliardë ngjarje, kishte përpunuar më shumë se 250 skeda TB, dhe kishte më shumë se 21,000 llogari aktive.

TabelaVIII. Krahasimi i ofruesve të shërbimit të logave të ndryshëm

Krahsimi	IBM SmartCloud Analytics	Papertrail	Logentries	Splunk Strom	Loggly
Forensik(Hetuesit)	Po	Po	Po	Po	Po
Aksesi	Pronësi	Pronësi	Pronësi	Pronësi	Pronësi
Çmimi	Pagesë, 90 ditë prove falas	Pagesë, 60 ditë prove falas	Pagesë, 30 ditë prove falas	Pagesë	Pagesë, 30 ditë prove falas
Platforma Mobile	N/A	iOS, Android	Android	iOS	iOS, Android
Regjistrimi i personalizuar	N/A	Po	Po	Po	Po
Regjistrimi i	N/A	N/A	Po	Po	Po

përplasjeve					
Dashboard	Po	Po	Po	Po	Po
Formati i Regjistrimit (Log Format)	Modifikuar	Modifikuar	Modifikuar	Modifikuar	Modifikuar
Enkriptimi	Advanced Encryption Standard (AES)(Enkriptimi Standart i avancuar)	TLS Enkriptim	Diffie-Çelës Hellman Shkëmbim	Advanced Encryption Standard (AES)	TLS Enkriptim
Siguria	SSH me bazë në çelës Vërtetim	Verifikimi i bazuar në certificate	Secure Socket Layer	Zgjidhja e palës së tretë (Meldium, Bitium)	HTTP/S duke përdorur APIRESTf-ul
Avantazhet	Analiza e shkakut të rrënjës, Zgjidh çështjet	Alarmet e menjëhershme, arkivat afatgjata	Zbulimi i Anomalisë, grafikët shumëpalëshe, pultet(dashboard) e përbashkët	Disponueshmëri-a, Privatësia dhe siguria e të dhënave	Regjistrimi i lehtë pa instalimin e agjentit, thjeshtimi i analizës së regjistrit
Kapaciteti	Pa limit	500GB	Pa limit	200GB	Pa limit
Suporti i OS	Red Hat Enterprise Linux Server	Unix/Linux	Windows,Linux, Mac	Windows,Linux	Windows, Linux, Mac
Instalimi	Medim	I lehtë	I lehtë	Medium	Medium

Burimi: S. Khan et al.

Kapitulli 4. PËRDORIMI I RASTEVE TË STUDIMIT TË NJË CLOUD LOG FORENSICS

4.1. Rastet e Studimit

Studimet e rasteve konsiderohen si një strategji hulumtimi për të hetuar një mjet, projekt, proces, sistem, shërbime, dhe kështu me radhë, në mënyrë empirike për të përcaktuar efektin në një situatë të jetës reale [Gerring 2007]. Këtu, në këtë seksion, unë shpjegoj katër raste studimesh që lidhen me CLF të ofruara nga CSP të ndryshme, duke siguruar lehtësira për hetimin e regjistrave të ndryshëm për dobësitë. Tabela VII nxjerr në pah tiparet kryesore të secilës CLF të përmendur në rastet studimore në drejtim të dhënies së CLF. Çdo studim i rastit krahasohet me karakteristika të ndryshme si: (a) lloji i studimit të rastit, (b) fokusimi, (c) teknologjia cloud, (d) lloji i regjistrit, (e) përparësia dhe (f) rezultati.

Karakteristikat e tipit të log-it përmbajnë vlera të ndryshme të shënjuar dhe të përdorura në studimet e rasteve për hetim që përfshijnë logot e webit, regjistrat e sistemit dhe aplikacioneve, shkrimet e serverit HTTP, regjistrat neto të rrjedhës dhe regjistrimet e aksesit. Karakteristikat e përparësisë përmbajnë vlera

të karakteristikave shtesë të marra duke përdorur një akses që përfshin shkallëzueshmërinë, qëndrueshmërinë, tolerancën e gabimit, fleksibilitetin, kosto-efikasitetin dhe koston e mundësive. Vlera e "shkallëzimit" tregon se teknologjia e tanishme e përdorur në studimet e rasteve mund të zgjatet për sasi të mëdha të dosjeve të regjistrit. Vlera e "qëndrueshmërisë" tregon se sistemi aktual mund të funksionojë edhe në shtetet me qëllim të keq që ndodhin gjatë hetimit të dosjeve të regjistrit. Vlera e "tolerancës së gabimit" tregon se sistemi i parashikuar për hetimin e dosjeve të regjistrit mund të funksionojë në kohën e dështimit të tij. Vlera e "fleksibilitetit" tregon integrimin e teknologjive të ndryshme të përdorura me sistemin e hetimit aktual të regjistrit. Vlera "efiçente për kosto" tregon zvogëlimin e kostos së operimit për një sistem hetimi log. Vlera e "kostos së mundësive" tregon përfitime alternative në dispozicion me më pak kosto. Për më tepër, karakteristikat e rezultateve kanë dy vlera si më poshtë: (a) suksesi dhe (b) i moderuar. Vlera e "suksesit" tregon se studimi i rastit është zbatuar me sukses, duke arritur objektivin e saj, ndërsa "i moderuar" tregon se studimi i rastit është zbatuar pa arritur plotësisht objektivat e tij.

4.1.1. Sistemet e Pagesave Heartland

Sistemet e Pagesave Heartland (HPS) janë një kompanitë me procesorët e pestë më të madh të pagesave në Shtetet e Bashkuara të cilët përpunojnë më shumë se 11 milionë transaksione në ditë, me një vlerë monetare prej rreth 80 miliardë dollarësh në vit [Jug 2013]. Përveç pagesës, proçesori HPS ofron shërbime të tjera të shumëfishta, si listat e pagave, tregtia elektronike, urdhërimi celular, pagesat shkollore, huadhënia etj., në industri të ndryshme, përfshirë restorantet, mikpritjen, naftën, shitjen me pakicë dhe arsimin. Bazuar në shërbimet e shumta financiare të biznesit, HPS u shfrytëzua vazhdimisht përmes sulmeve të ndryshme të hetimit të cenueshmërisë. Ishte një sfidë e madhe për HPS për të hetuar dobësitë në një sasi të madhe të të dhënave të regjistrit të mbledhura gjatë transaksioneve financiare. Në vitin 2009, HPS u vra në shënjestër me një sulm SQL injection që vodhi 130 milionë numra të kartave të kreditit dhe debitit të përdoruesve të ndryshëm nga burimet e rrjetit dhe informatikës. HPS u gjobit 60 milionë dollarë nga Visa Corporation dhe operacioni i saj u pezullua për 6 javë, të cilat i kushtonin një numri klientësh besnikë. Si rezultat i ndëshkimit të madh financiar dhe humbjes së konsumatorëve, HPS vendosi të forcojë sigurinë e saj duke u fokusuar në analizimin e aktiviteteve në rrjetin dhe infrastrukturën informatike për të gjetur shkakun rrënjësor të modeleve me qëllim të keq në fazën e hershme të shfaqjes së saj.HP ArcSight ofron një shërbim të ultë të shpejtë të forenzikës që bashkon kërkimin, njoftimin, analizën dhe raportimin në tërë tekstin përgjatë gjithë të dhënave të makinës së ndërmarrjeve të dhëna në skedarët e regjistrit. Përveç kësaj, sigurimi i Sistemit të Informacionit të Sigurisë dhe Menaxhimit të Eventeve (SIEM) nga arkivuesi i HP ArcSight përshpejton skedarin e forensikës duke ulur afatin kohor për t'iu përgjigjur shpejt aktiviteteve të dëmshme dhe duke kufizuar koston e fuqisë punëtore duke u fokusuar në burimin e alarmit në vend që të përdorin skuadra të shumta për t'u mobilizuar dhe për të hetuar ngjarjet e dyshimta. Duke përdorur logger HP ArcSight, hetuesit HPS kanë përcaktuar kërcënime të ndryshme të sigurisë duke analizuar shkrimet e ndryshme të infrastrukturës në kohë reale, e cila është parandaluar para se të prekë viktimën. Hetuesit HPS kanë përfituar duke përdorur logger HP ArcSight për të mbledhur të dhënat log nga një numër i burimeve të shumta, për të lehtësuar vendosjen e forensikës log, forenzika ultra të shpejtë nëpërmjet kërkimit të plotë tekst, monitorimin e vazhdueshëm, opsionet fleksible të magazinimit log me një raport të lartë compression (dmth., 10: 1), dhe në kohë reale analizën e një numri të madh të dosjeve log. Prandaj, HPS ka mbrojtur dhe rritur biznesin e saj në mënyrë të konsiderueshme duke përdorur logger HP ArcSight dhe ka fituar shumë çmime të industrisë, të tilla si shefi i Sigurimit Zyrtar (CSO) të vitit (2013) për John South në SC Magazine.

4.1.2. Ofruesi i Shërbimeve Financiare Monex

Kompania Monex është ofrues i shërbimeve financiare në internet, me seli në Tokio, Japoni, që ka disa degë të tregtimit të letrave me vlerë në internet. Monex ofron shërbime tregtare financiare për më shumë se 1.5 milionë klientë në Japoni [Kastor 2015]. Rrjeti aplikacion i përdorur për shërbimet financiare është zhvilluar në një rafte zhvillimi të Windows me një aplikacion .Net front-end dhe një bazë të dhënash MySQL. Monex varet nga të dhënat e regjistrit të aplikacionit për të identifikuar sjelljen keqdashëse të sulmit në kohë kur gjërat nuk funksionojnë siç pritej. Sfida me të cilën përballet Monex ishte të analizonte sasi të mëdha të të dhënave të regjistrit në kohë reale për të përcaktuar shkaktarin kryesor të sulmit. Monex nuk mundi të arrinte një mekanizëm hetimi efikas dhe të shpejtë për të përballuar sasi të mëdha të të dhënave të regjistrit në kohë reale. Monex filloi të përdorte DFE, një shërbim i ofruar nga Loggly, një ofrues i menaxhimit të regjistrit të cloud. DFE ofron një përmbledhje të plotë strukturore të të dhënave tuaja të regjistrit që ndihmon në dallimin midis ngjarjeve të përbashkëta dhe anomalive, si dhe për të siguruar një mënyrë të shpejtë dhe të saktë për t'u filtruar në regjistra të caktuar. Hetuesit e sigurisë Monex përfitojnë nga DFE për të kryer analiza automatike të regjistrave, analizë të thellë të logaritmit, kontrolle të shëndetit dhe identifikim të rrënjës. Për më tepër, llogaritja e ngjarjeve në kohë reale të DFE ndihmon hetuesit e sigurisë të Monex për të kuptuar më mirë shkallën e problemit dhe për të përcaktuar vendndodhjen ku ekziston problemi. Kjo çon në një reagim të shpejtë dhe efikas të kërcënimit ndaj pjesës korrekte të sistemit.Si rezultat, Monex fitoi pasqyrë relevante në të dhënat e regjistrit për të hetuar ngjarjet e dëmshme të pranishme në sistem shumë më shpejt dhe me saktësi. Zbulimi i shpejtë i ngjarjeve me qëllim të keq në të dhënat e regjistrit nëpërmjet DFE-së e bëri Monex më produktiv duke u fokusuar në kompetencat e tij kryesore në vend që të analizonte regjistrimet për burime të dëmshme.

4.1.3. Intesa Bank

Banka Intesa është një bankë udhëheqëse në Serbi që ka më shumë se 1.7 milionë klientë. Banka përpunon më shumë se rreth 11 milionë ngjarje në ditë të mbledhur nga skedarë të ndryshëm log nga pajisje të ndryshme të rrjetit, pajisjet e sigurisë dhe bazat e të dhënave [Stanojević 2013]. Si një institut financiar, Banka Intesa beson se është e sigurtë nga dobësitë duke shfrytëzuar rekorde të ndryshme të klientëve përmes sulmeve të ndryshme. Banka Intesa kërkoi shërbime të centralizuara të menaxhimit të regjistrit për të siguruar një analizë të plotë të aktiviteteve të përdoruesit dhe rrjetit. Banka Intesa donte të lidhte informacionin e mbledhur nga pjesë të ndryshme të infrastrukturës bankare dhe të kryejë një hetim, duke përdorur analizën rrënjësore, duke rezultuar në përgjigjet ndaj ngjarjeve të dyshimta dhe kërcënimeve të mundshme. Banka Intesa shfrytëzoi shërbimet e regjistruesit të HP ArcSight për të kërkuar regjstrimet e mbledhura për kërcënime të mundshme që shkaktojnë dëme në infrastrukturën bankare. Logger HPArcSight ofron shërbime të forenzikës log për llogari të plotë të Bankës Intesa duke analizuar dosjet e ndryshme të regjistrit, duke përfshirë ngjarjet kritike në kohë reale, njoftimet e ndryshme, korrelacionin e informacionit të regjistrit, monitorimin e të dhënave dhe të përdoruesve, monitorimin e aplikacioneve dhe inteligjencën e kërcënimeve. Informacioni për forenzikën e log-it ndihmon hetuesit e sigurisë të Banca Intesa të dinë se kush është në rrjet, cilat të dhëna janë aksesuar dhe cilat veprime janë kryer mbi të dhënat. Informacioni i marrë nga forenzika log ndihmon hetuesit e sigurisë të bankës të kontrollojnë veprimet e dëmshme të kryera nga përdoruesit keqdashës përpara se ata të vazhdojnë të dëmtojnë infrastrukturën bankare.

4.1.4. Yelp Content Analytics System

Yelp është një korporatë me një faqe interneti që boton përmbledhje të burimeve të turmave në lidhje me lokalet e bizneseve [Stoppelman 2004]. Në dekadën e parë, Yelp përhapi biznesin e saj në 29 vende me më shumë se 120 tregje. yelp ka më shumë se 130 milionë përdorues mujorë të cilët vizituan faqen e internetit për qëllime të ndryshme, duke përfshirë rishikimet e biznesit, azhurnimin për informacionet e kontaktit të biznesit, gjenerimi i planeve të biznesit, azhurnimi i pervojave të jetës personale, dhe shumë më tepër. Për të hyrë në një sasi aq të madhe, të dhënat janë të vështira dhe, më tej, kërkon analizën e të dhënave për të përcaktuar sjellje me qëllim të keq. Yelp filloi të përdorte Amazon S3 dhe Amazon Elastic Map Reduce (Amazon EMR) për të kapërcyer problemet e lartpërmendura. Yelp raportoi se 1.2TB të të dhënave të regjistrit ruhen në Amazon S3 në baza ditore. Yelp përdor Amazon EMR për të përpunuar të dhënat e regjistrit për të analizuar përmbajtjet e dyshimta. Amazon EC2 ndihmon Yelp-in në kryerjen e analizave të regjistrit për të përcaktuar përmbajtjen e dyshimtë dhe, për rrjedhojë, kursen përdoruesit e pafajshëm. Si rezultat, Yelp kursen kostot e pajisjeve paraprake duke përdorur Amazon EMR për analizimin e të dhënave të regjistrit dhe, për më tepër, fokusohet në kostot e mundësive për të fituar më shumë me kosto më të ulët me konceptin "paguani vetëm për atë që përdorni".

Kapitulli 5. FORENZIA E CLOUD LOG: KERKESAT E SIGURISË, PIKAT E VULNERABILITETIT DHE SFIDAT

5.1. Ruajtja e të dhënave

Bërja masive e regjistrit në vende të shumta rrit kërkesën për hapësirën e ruajtjes në një organizatë. Një organizatë me resurse të pakta nuk është në gjendje të akomodojë një sasi të madhe të regjistrave, gjë që e inkurajon atë për të migruar në ruajtjen e cloude-ve [Shiraz et al. 2015]. Megjithatë, ruajtja e të dhënave të rëndësishme në burimet e palëve të treta në cloud computing krijon një rrezik për një organizatë sa i përket mbrojtjes së të dhënave. Informacioni publik i disponueshëm publik shton më shumë rrezik për mbrojtjen e të dhënave në aspektin e aksesit të lehtë dhe të thjeshtë të resurseve cloud [Ramgovind et al. 2010]. Një sulmues mund të punësojë burime të shumta në cloud dhe të përdorë burime për gjenerimin e sulmeve duke hyrë në bazat e të dhënave të regjistrit për të fshirë dhe ndryshuar skedarët e të dhënave të regjistrit. Për të minimizuar

Tabela IX. Ligjërata për Regjistrin Cloud: Kërkesat e Sigurisë

Kërkesa për sigurinë e forensikës së regjistrit në cloud	Përshkrimi
Konfidencialiteti	Të sigurojë një siguri për shkrimet e cloud të krijuara nga burime të ndryshme përmes parandalimit të aksesit së paautorizuar.
Integriteti	Për të ruajtur regjistrimet e cloud nga ndryshimi ose modifikimi i personit të autorizuar ose të paautorizuar, kryen një veprim me dashje ose pa dashje.
Disponueshmëria	Për të garantuar shkrimet e cloud të disponueshëm për analizë në formën origjinale ashtu siç është krijuar dhe ruajtur.
Autenticiteti	Për të siguruar që përdoruesi i duhur të ketë akses

	në të ketë akses të autorizuar në loget e reve që ruajnë në re.
Privatësia	Ruajtja e të dhënave të përdoruesit nga rrjedhja gjatë gjenerimit, mbledhjes, ruajtjes dhe analizimit të regjistrave të reve në cloud.

Burimi: Unë

kërcënimet nga shfrytëzimi i regjistrave të cloud-it në cloud, CSP duhet të mbrojë dosjet e regjistrit të përdoruesve dhe duhet të sigurojë CLF gjithëpërfshirëse dhe adekuate. Në mënyrë të ngjashme, një raport i përpiluar ligjor në fund të procesit të hetimit i dërgohet organizatës. Niveli i besimit është rritur në mes të CLF-së dhe organizatës në drejtim të kryerjes së proceseve adekuate ligjore për skedarët e logut cloud. Në këtë seksion, CLF klasifikohet në tri pjesë duke përfshirë kërkesat e sigurisë, pikat e cenueshmërisë dhe sfidat. Kërkesat e CLF tregojnë parametrat e sigurisë të nevojshme për logun e cloud që do të hetohen për prova të vlefshme (origjinale). Pikat e cenueshmërisë CLF përfshijnë vende ku mund të ndodhin sulme për të shfrytëzuar skedarët e logut të cloud brenda ose jashtë cloud-it. Në pjesën e fundit të këtij seksioni, sfidat e CLF janë të anketuara. Megjithëse janë propozuar disa zgjidhje për disa nga sfidat, për shkak të sasisë së vogël të konsideratës që u është dhënë këtyre sfidave, kërkohen më shumë përpjekje kërkimore për të siguruar rezultate adekuate dhe praktike.

5.2. Ligji i Regjistrimit Cloud: Kërkesat e Sigurisë

Kërkesat përfshijnë konfidencialitetin, integritetin, disponueshmërinë, origjinalitetin dhe privatësinë. Çdo kërkesë e sigurisë CLF është përshkruar në paragrafët e mëvonshëm dhe të theksuara me një përshkrim në Tabelën X.

Konfidencialiteti. Konfidencialiteti merret me ruajtjen e të dhënave të përdoruesit në cloud log files. Të dhënat e ndjeshme(sensitive) në skedarët e regjistrit të cloud nuk duhet t'u zbulohen asnjë individi. Individi mund të jetë një sulmues ose një tjetër CSP. Në analizimin e dosjeve të logut të cloud, atje mund të jenë të dhëna të ndjeshme në dispozicion rreth përdoruesit, duke përfshirë fjalëkalimin, numrin e kartës së kreditit, përmbajtjen e postës elektronike dhe të tjera. Informacioni i tillë i ndjeshëm krijon shqetësime të sigurisë për një person që heton shkrimet e cloud dhe ngjashëm për një person që hyn në regjistrimet e clous-it në mënyrë të ligjshme ose ilegale.

Integriteti. Integriteti konsiderohet një parametër jetik për skedarët e logut të cloud në lidhje për të siguruar prova kundër sulmuesve. Integriteti merret me jo-ngatërrime ose mos modifikimi i skedarëve të logut të cloud pasi ato krijohen dhe ruhen në cloud [Yun et al. 2014]. Ruajtja dhe tranzitimi i regjistrit të rremë të papërshtatshëm mund të krijojë ndjeshmëri ndaj shkatërrimit dhe ndryshimit të integritetit të logut cloud. Si rezultat, krijohen probleme të ndryshme, duke përfshirë aktivitete të padëmshme me qëllim të keq, manipulim të provave, fshehje të përdoruesve keqdashës etj. Për shembull, ka rootkit të dizajnuara në mënyrë specifike që ndryshojnë të dhënat e skedarit të logut për të modifikuar ekzekutimin dhe instalimin e rootkit. Si rezultat, gjatë procesit CLF, një hetues ose CSP duhet të ofrojë dëshmi për gjykatën pas hetimit se i tërë procesi është kryer në bazë të dosjeve origjinale të regjistrit të cloud, në vend se ato të manipuluara.

Disponueshmëria. Disponueshmëria merret me të dhënat e regjistrit të cloud që duhet të jenë të disponueshëm sa herë që kërkohet [Yin 2014]. Në cloud-computing, skedarët e regjistrit të cloud përsëriten në më shumë se një vend për hir të sigurisë dhe besueshmërisë. Sidoqoftë, problemi i disponueshmërisë lind kur sulmuesi ka akses në një skedar logi të cloud derisa të përsëritet në burime të ndryshme. Aksesueshmëria e skedarëve të regjistrit të cloud tek sulmuesit mund të rezultojë në fshirjen e dosjeve të logut për të fshehur identitetin e tyre. Në mënyrë të ngjashme, disponueshmëria ndikohet gjithashtu nga politikat e ruajtjes së të dhënave të një organizate. Për shembull, një regjistër ka një limit maksimal të specifikuar që tregon volumin e të dhënave të regjistrit. Kufiri duhet të jetë në kapacitete të tilla si 500 megabajt ose mund të jetë në numra të tillë si 100,000 ngjarje. Sapo të arrihet kufiri, shkrimet mbishkruhen ose hyrjet e regjistrave ndalohen, gjë që shkakton humbjen e të dhënave. Prandaj, rezulton në minimizimin e disponueshmërisë së skedarëve të regjistrit të cloud.

Autenticiteti. Çështja e origjinalitetit merret me lejen e aksesit për skedarët e regjistrit të cloud. CSP-ja duhet të sigurojë që dosjet e logeve cloud të arrihen vetëm nga individë të autorizuar që kanë objektiva të justifikueshme siç është hetimi. Ndonjëherë, një skedar log cloud arrihet nga një hetues ose një punonjës i CSP-së, megjithatë ajo mund të fshijë ose ndryshojë një pjesë të skedarit të log-ut që ndikojnë në të gjithë procesin e CLF.Mundësia e aksesit në skedarët e logut të cloud të autorizuar nuk do të zbulonte informacionin e përdoruesve të tjerë që do të zvogëlonte besimin e përdoruesve në aksesin në të dhënat e tyre. Aksesueshmëria e plotë në skedarët e regjistrit të cloud duhet të mirëmbahet në formën e një raporti nga CSP që inçizon secilin dhe çdo akses në skedarët e skedave të ruajtura në cloud-informatikë.

Privatësia. Privatësia merret me sigurimin e të dhënave të regjistrit të përdoruesit në çdo fazë të CLF nga gjenerator në fazën e analizës. Në cloud-computing, çdo burim fizik ka makina të shumta virtuale që kanë aplikacione të shumëfishta të përdoruesve në të njëjtën kohë, dhe fenomenet e tilla njihen si multi-tendancy në cloud computing [Jahdali et al. 2014]. Regjistrat e gjeneruar në një mjedis me shumë banorë përmbajnë të dhëna të shumta të përdoruesve në të njëjtën kohë. Ambienti shumë-qiramarrës i cloud-it bën hetimin të vështirë për të izoluar të dhëna nga burime të ndryshme [Simou et al. 2014]. Probabiliteti i aksesit në të dhënat e regjistrit të një individi të pafajshëm, ndërsa aksesi në skedarët e të dhënave të regjistrit të përdoruesve të dëmshëm rritet. Si rezultat, në CLF, privatësia është një kërkesë kryesore dhe një sfidë për hetuesit ligjorë që të mbesin të paprekur.

5.3. Ligji për Cloud Forensika: Pikat e Vulnerabilitetit

CLF mbështetet fuqimisht në veçoritë e rëndësishme të sigurisë për të dhënat e regjistrit si konfidencialiteti, integriteti dhe disponueshmërisë. Një hetim i të dhënave të regjistrit duhet të ruajë të dhënat e ndjeshme të përdoruesit të paraqitur në logun e cloud-it ndërsa analizon atë për ndjeshmëri të ndryshme. Në mënyrë të ngjashme, një hetim duhet të rezistojë heqjen dhe modifikimin e çdo lloj të dhënave që regjistrohen në mënyrë që të mos kompromentoni integritetin e të dhënave. Megjithatë, disponueshmëria

Tabela X. Ligji për Cloud: Forensika: Pikat e Vulnerabilitetit

Pikat e mundshme të cenueshmërisë për sulmet me log	Përshkrimi	Konfidencialiteti	Integriteti	Disponueshmëria

në cloud				
Gjenerimi i regjistrit	Sulmi në loget e cloud-it ku gjenerohen shkrimet. Ai përfshin makinën virtuale, aplikacionin, hostin, serverin dhe të tjerët.	Jo	Jo	Po
Mbledhja e regjistrit	Sulmi mbi sistemin dhe burimet ku shkrimet janë mbledhur nga vende të ndryshme në cloud.	Po	Po	Po
Rrjeti	Sulmi në kanalin e rrjetit midis gjeneratorit të gjenerimit të regjistrit dhe sistemit / agjentit të koleksionistit të regjistrit ose ndërmjet agjentëve të mbledhjes së regjistrit dhe burimeve të ruajtjes së regjistrit.	Po	Po	Po
Ruajtja e regjistrit	Sulmi mbi burimet e magazinimit ku shkrimet janë ruajtur nga agjentët e mbledhjes së regjistrit dhe burimet e tjera të ruajtjes së cloud.	Jo	Jo	Po
Analiza e regjistrit	Sulmuesi shfrytëzon burimet në të cilat kryhet analizë e llogaritjeve për të hetuar dobësi të ndryshme të gjetura në shkrimet.	Jo	N/A	Po

Burimi: S. Khan et al.

e të dhënave të regjistrit është gjithashtu e rëndësishme për shkak të nevojës për analiza të qëndrueshme të regjistrit me identifikimin e saktë dhe në kohë të dobësive. Dobësitë e ndryshme gjenerohen nga sulmuesit në shkrimet cloud për të kryer aktivitete keqdashëse me qëllim të shkatërrimit të gjurmëve të tyre të sulmeve, modifikimin dhe fshirjen e të dhënave të regjistrit, devijimin e procesit të hetimit në drejtime të tjera në mënyrë që t'i fshehin ato, nxjerrjen e të dhënave të ndjeshme etj. . Tani, fokusi ynë në këtë seksion është të shpjegojmë pikat e mundshme të pambrojtura në infrastrukturën e regjistrimeve cloud. Ne e kemi ndarë infrastrukturën e regjistrimit cloud në pesë pjesë për të nxjerrë në pah qartë gjithë procesin e sulmit në logun cloud në lokacione të ndryshme të regjistrit. Pikat potenciale të cenueshmërisë në infrastrukturën e regjistrimit cloud janë gjenerimi i regjistrit, mbledhja e regjistrit, rrjeti, ruajtja e regjistrit dhe analiza e logaritmave. Secila nga këto pika të pambrojtura në infrastrukturën e regjistrimeve cloud është përshkruar dhe ilustruar në Tabelën X.

Gjenerimi i regjistrit. Dosjet e regjistrit gjenerohen përmes mjeteve të ndryshme dhe skedarëve të konfigurueshëm, për shembull, ProcMon.exe, skedari vmware.log dhe aLogcat para-konfiguruar për kapje kërkojnë informacione nga serverat, rrjeti, pajisjet dhe aplikacionet. Dosjet e regjistrit të përditësimeve përditësohen me përmbajtjen e regjistrit me kalimin e kohës kur sistemi, procesi dhe rrjeti fillojnë ekzekutimin e tij në cloud. Në cloud-in, CSP ndërton skedarë logesh në vende të ndryshme në cloud për të regjistruar ngjarje të ndryshme, duke përfshirë makinat virtuale, pret, serverat, rrjetet dhe aplikacionet e ndryshme, në mënyrë që të regjistrojnë ngjarje të ndryshme përgjatë një afati të caktuar kohor. Çdo njësi e lartpërmendur krijon një skedar regjistrimesh në varësi të konfigurimit të brezit të paracaktuar të përcaktuar nga CSP. Për më tepër, në infrastrukturën e madhe të cloud-computing, është e vështirë për të gjetur vendin e saktë ku gjenerohen regjistrimet. Sulmuesi mund të shkatërrojë aplikacionin ose sistemin e krijuar nga logi duke fshirë skedarët e konfigurimit, duke injektuar kodin keqdashës, duke e detyruar atë të kryejë keqfunksionime, duke e zhvendosur atë nga objektivi. Sidoqoftë, konfidencialiteti dhe integriteti i të dhënave të regjistrit cloud në një situatë të tillë nuk është një çështje për shkak të qëllimit të sulmuesit për të shkatërruar ose fshirë dosjet e ekzekutimit të aplikacionit për gjenerimin e regjistrit ose sistemit, në vend që të shikojnë përmbajtjen e dosjeve të logut cloud.

Mbledhja e regjistrimeve. Dosjet e regjistrimeve grumbullohen nga koleksioni i log cloud ose agjent cloud nga burime të ndryshme në cloud computing. Pas gjenerimit të skedarëve të ndryshëm të regjistrit të cloud, koleksioni i regjistrit cloud mbledh skedarët e logut cloud për të ruajtur ato në burime të ndryshme cloud computing. Megjithatë, sapo sulmuesi të ketë akses në lokacionet e grumbullimit të regjistrave, ai / ajo lehtë mund të shfrytëzojë skedarët e logeve të cloud. Në këtë pikë, skedarët e regjistrit të cloud janë në dispozicion të sulmuesit për të fshirë ose modifikuar duke hequr gjurmët e sulmit ndërsa kompromenton konfidencialitetin, integritetin dhe disponueshmërinë. Mbledhësi i regjistrimeve mbledh kryesisht log fotografi në formatin zip, të cilat mund të konvertohen lehtësisht nga sulmuesi në formatin log të zakonshëm për kuptueshmëri.

Rrjeti. Rrjeti, i njohur edhe si transit, përdoret për të kryer skedarë të regjistrit të cloud, mbledhësit log në burimet e magazinimit log. Mënyra më e lehtë për sulmuesit që të sulmojnë është ndërhyrja në mes të kolektorëve të logave cloud dhe resurseve të ruajtjes së logut cloud , sesa thyerjes së pengesave të sigurisë për secilin. Rrjeti është amedium për të lidhur dy burime, sisteme ose pika të përgjithshme që nuk i përkasin asnjë prej palëve. Konfidencialiteti është kompromet uar për shkak të rrjedhjes së të dhënave, ndërsa integriteti është kompromet uar për shkak të modifikimit dhe ndryshimit të të dhënave në rrjet. Në

mënyrë të ngjashme, disponueshmëria mund të ndikohet nga fshirja e disa ose të gjitha dosjeve të logut cloud derisa kalon nga mbledhësit e logave cloud në ruajtjen e regjistrit cloud.

Ruajtja e regjistrit. Magazinimi i regjistrit është vendndodhja / burimi ku ruhen skedarët e logut të cloud të analizohen në fazën e ardhshme të CLF, të tilla si analiza e logut cloud . Siguria e skedarëve të regjistrit cloud të ruajtura në resurset cloud varet nga siguria që u është dhënë atyre në aspektin e formatit të regjistrit, kodimit, aksesit së autentifikimit dhe të tjerave. Formati i regjistrit që përdoret për të ruajtur skedarët e regjistrit të cloud në ruajtje mund të ndryshojë nga formati i logaritmeve të përdorura në gjenerimin e regjistrit dhe grumbullimin e regjistrit. Sulmuesi mund të ketë akses në disa nga skedarët e logut cloud në mbledhjen e të dhënave të cloud dhe tani ai dëshiron të ketë akses në më shumë informacione nga shkrimet në vendin e magazinimit, por ai mund të jetë i kufizuar duke bërë kështu për shkak të formave të ndryshme të regjistrit cloud. Sidoqoftë, përsa i përket aksesit në ruajtjen e regjistrit cloud, një sulmues mund të fshijë skedarët e regjistrit cloud, duke kompromet uar disponueshmërinë. Konfidencialiteti nuk është një çështje për shkak të skedarëve të regjistrit të koduar dhe as nuk është integriteti për shkak të vështirësive në shikimin e të dhënave të skedarëve në cloud.

Analiza e regjistrimeve. Analiza e regjistrit është procesi për të kryer analiza në skedarët e logut cloud që grumbullohen nga ruajtja e logut të cloud. Analiza e regjistrit cloud identifikon sulmuesit përmes analizimit të skedarëve të regjistrit të cloud. Sulmuesit duan të mbajnë veten të fshehur nga hetimi, gjë që i detyron ata të sulmojnë burimet / aplikacionet e analizës së regjistrit për të hequr prova të sulmit të tyre. Sidoqoftë, në infrastrukturën e madhe të informatikës cloud, gjetja e vendndodhjes së saktë ku bëhet analiza e regjistrimeve cloud është një detyrë e vështirë, e cila detyron

Tabela XI. Logjika e re për forenzikë: Sfidat

Logjika e re për forenzikë: Sfidat	Zgjidhja e propozuar	Përshkrimi
Të dhënat e regjistrit në cloud si të dhëna të mëdha	Mekanizmi i filtrimit të të dhënave	Për të regjistruar vetëm të dhëna të rëndësishme në skedën e të dhënave të regjistrit të cloud.
Aksesi në regjistrin cloud	Varësia nga ofruesit të shërbimit në cloud.	PGJS-ja duhet të sigurojë shkrimet cloud për hetuesit e ndryshëm për shkak të kontrollit të tyre në regjistrat e ndryshëm cloud. Megjithatë, integriteti i të dhënave duhet të sigurohet nga hetuesit.
Siguria e regjistrit cloud	Metodat e duhura të aksesit Kriptimi i skedarëve të logut cloud dhe çelësin kriptografik Replikimi i skedarëve të regjistrit të cloud	Logs cloud duhet të arrihen vetëm nga individë të autorizuar përmes metodave të ndryshme të aksesit. Të dy të dhënat e regjistrit cloud dhe çelësi i kodimit janë të koduara për shkak të sigurisë më të mirë dhe më të besueshme të regjistrit të cloud. Regjistri i të dhënave i skedës së re përsëritet në burimet e shumta të ruajtjes cloud.
Regjistrat e decentralizuar cloud	Analizë e centralizuar e regjistrit	Të kontrollojë dhe menaxhojë të

		gjithë serverët e shpërndarjes së analizës së të dhënave të shpërndara.
Formati i regjistrimit të standardizuar cloud	Formati i logit të vetme cloud	Çdo log cloud i gjeneruar në vende të shumta në cloud-computing duhet të ketë një format të vetëm të logut cloud, me shënime të mbushura sipas kërkesës.
Drejtësia e analizës së logut cloud	Mjet automatik i analizës së regjistrit cloud	Një mjet i përdorur për të analizuar automatikisht logat cloud me ndërhyrje minimale njerëzore.

Burimi: S. Khan et al.

sulmuesit të bëjnë më shumë përpjekje për të gjetur një vend të saktë për të sulmuar. Decentralized CLF ndihmon hetuesit për të kryer analiza në vende të shumta dhe parandalon sulmuesit që të shfrytëzojnë skedarët e logeve cloud në kohën e analizës. Konfidencialiteti dhe integriteti nuk janë shfrytëzuar nga sulmuesit gjatë sulmeve të tyre, ndërkohë që disponueshmëria e skedarëve të logave cloud është prekur në bazë të fshirjes së tyre.

5.4. Logjika e re për forenzikë: Sfidat

Për të analizuar shkrimet e ndryshme të blloqeve të mbledhura nga burime të ndryshme në cloud-informatikë nuk është një detyrë e lehtë [Damshenas et al. 2012]. Infrastruktura e shpërndarë, mjedisi i virtualizuar, burimet me shumë banorë, aplikacionet e mëdha të drejtimit, miliona përdorues në cloud, reagimi në kohë reale (sipas kërkesës) dhe shumë faktorë të tjerë e bëjnë CLF-në shumë sfiduese. Sfidat më të fundit janë prezantuar dhe shpjeguar në seksionet e mëvonshme me qëllim të ofrimit të fushave të reja kërkimore për hulumtuesit dhe agjencitë hetuese për të zhvilluar modele, standarde dhe korniza të reja për procesin CLF. Sfidat e CLF shoqërohen nga propozimi i zgjidhjeve për të ndihmuar studiuesit në zgjidhjen e problemeve. Tabela XI thekson sfidat e fundit të CLF me zgjidhjet e propozuara.

Të dhënat e regjistrit në cloud si të dhëna të mëdha. Siç u përmend më herët, gjenerimi i sasive masive të të dhënat e regjistrit cloud në burime të ndryshme shkakton një problem për hetuesit e CLF në analizimin të dhënat e regjistrit cloud. Problemi ka të bëjë me konceptin e quajtur "të dhëna të mëdha", dmth vëllimit të të dhënave, varietetit dhe vlerës [Hashem et al. 2015]. Vëllimi tregon madhështinë sasia e të dhënave të regjistrit cloud të gjeneruara në vende të shumta në cloud-informatikë, të cilat shkakton vështirësi për hetuesit në mjediset në kohë reale [Zibin et al. 2013]. Për më tepër, siguria është një çështje për ruajtjen e të dhënave të logut të madh në vende të shumëfishta në cloud. [Popa et al. 2011]. Megjithatë, nëse ndonjë pjesë e magazinimit të regjistrit cloud është shfrytëzuar nga sulmuesi, atëherë do të ndikojë në tërë procesin e hetimit, duke rezultuar në integritetin e reduktuar të të dhënave të regjistrit cloud. Në mënyrë të ngjashme, një shumëllojshmëri e të dhënave të regjistrit cloud nga burime të ndryshme me formate të ndryshme të regjistrit e bëjnë CLF më të vështirë në drejtim të përdorimit të një akses të vetëm të kanalit të logut cloud (Oliner et al. 2012]. Çdo log cloud i krijuar në vende të ndryshme të cloud-computing ka objektivin e vet për të cilin është krijuar. Për shembull, shkrimet e rrjetit cloud krijohen për të regjistruar

modele të ndryshme të paketës [Pranverë 2011], ndërsa shkrimet e sistemit të reve përdoren për të regjistruar ndryshime të ndryshme shtetërore.

Aksesueshmëria e Regjistrave Cloud. Gjenerimi i skedarëve të regjistrit të cloud në cloud-informatikë mjediset nuk është aq e vështirë, por aksesi në to me kërkesat e duhura është i vështirë [Shams et al. 2013]. Çdo regjistër cloud duhet të arrihet nga individë të autorizuar që kanë një objektiv të qartë. Për shembull, një zhvillues i aplikacioneve do të kërkojë regjistrime cloud të një aplikacioni për të rregulluar gabimet në kodin e aplikimit. Ngjashëm, një administrator i rrjetit kërkon që shkrimet e rrjetit të përcaktojnë rrjedhën e paketave. Çdo log cloud duhet të arrihet nga grupi i individëve përgjegjës, sipas kërkesave të tyre [Trenwith dhe Venter 2014]. Asnjë grup tjetër nuk mund të hyjë në një regjistër tjetër cloud pa arsye të vlefshme dhe aprovim nga autoritetet ligjore. Çdo hetues ligjor duhet të ketë akses të plotë në loget e kërkuara cloud për hetimin e sulmeve me qëllim të keq brenda të dhënave të regjistrit. Aksesi i përshtatshëm në regjistrat cloud do të rezultojë në CLF të duhur. Për më tepër, në shumë raste, CLF-ja nuk lejon ndonjë agjenci të palës së tretë ose hetuesin ligjor që të ketë akses në regjistrat cloud për arsye sigurie dhe privatiteti [Ruan et al. 2012]. CLF-ja mund të ndihmojë hetuesit në marrjen e aksesit në regjistrat cloud nëpërmjet lejes ligjore të caktuar nga gjykata. Megjithatë, shfaqet një problem kur CSP-ja bëhet e pabesueshme për shkak të modifikimit të regjistrave cloud që u ofrohen hetuesve. Integriteti i të dhënave duhet të sigurohet nga hetuesit kur ata marrin log nga cloud nga CSP për të identifikuar aktivitetet (origjinale) me qëllim të keq të sulmuesit që janë regjistruar në kohën e krijimit të regjistrit cloud. Për të monitoruar çdo paragjykim të CLF-së, ndërhyrja njerëzore duhet të minimizohet duke zhvilluar një mekanizëm automatik që i dërgon hetuesit cloud tek hetuesit e ndryshëm të autorizuar duke i verifikuar ato përmes mekanizmave të ndryshëm të hashingut. Sapo hetuesit të konfirmojnë se shkrimet cloud të pranuara nga CLF-ja janë të pa modifikuara, ata mund të fillojnë hetimet e tyre.

Siguria e Regjistit Cloud. Siguria e dosjeve të regjistrit të Cloud është e rëndësishme për CLF për shkak të konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave (CIA) [Ryan et al. 2011b]. Hetuesi ligjor duhet të sigurojë që të dhënat e hetuara në regjistrin cloud nuk janë ndryshuar nga askush pas gjenerimit të tyre. Sulmuesi mund të shfrytëzojë skedarët e logut cloud në hapësirën e ruajtjes së të dhënave ku regjistrohen rregjistrat dhe në rrjetin cloud ku të dhënat kalojnë nga një vend në tjetrin dhe ngjashëm në serverin e analizës së logeve cloud ku të dhënat e regjistrit kontrollohen për veprime me qëllim të keq. Çdo shkelje e menaxhimit të regjistrit cloud në terma të CIA-s do të ndikojë në të gjithë CLF duke prodhuar rezultate të njëanshme. Kryesisht, ofruesit e log-as-a-service kryejnë encryption në skedarët e logit cloud dhe i ruajnë ato në burimet e ruajtjes cloud. [Sundareswaran et al. 2012]. Sidoqoftë, sapo një sulmues të ketë gjetur çelësin privat për të dekriptuar skedarët e regjistrit të cloud, ata kryejnë më tej aktivitete me qëllim të keq, siç janë fshirja e gjurmëve të sulmeve, modifikimi në të dhënat e regjistrit cloud dhe kështu me radhë. Për të siguruar CIA-n e dosjeve të logut cloud,CLF-ja duhet të sigurojë akses të duhur duke zbatuar individët për të dhënë fjalëkalime në nivele të ndryshme të aksesit së tyre. Ngjashëm, kodimi i skedarëve të regjistrit të cloud si dhe një çelës kriptografik do t'i detyrojnë sulmuesit të bëjnë më shumë përpjekje në aksesin dhe modifikimin e përmbajtjes së regjistrave cloud. Disponueshmëria e skedarëve të regjistrit të cloud mund të sigurohet duke mbajtur kopje kopjimi të resurseve të ndryshme të ruajtjes cloud. Sidoqoftë, duhet të garantojmë më tej që të gjitha kopjet e një skedari të logut cloud janë sinkronizuar me njëri-tjetrin gjatë aksesit në ndonjë nga kopjet gjatë hetimit të skedarëve të regjistrit të cloud. Për të siguruar skedarë të ndryshëm të regjistrit cloud nga sulmuesit në cloud është një nga sfidat më të mëdha për hetuesit, ndërsa preformon CLF.

Regjistrat e decentralizuar cloud. Në cloud computing, shkrime të ndryshme cloud janë gjeneruar në shtresa të ndryshme duke u ruajtur në serverët e shpërndarjes së analizave të shpërndarjes. Shtresat cloud siç janë sistemi operativ, aplikacionet, rrjetet dhe bazat e të dhënave kanë skedarët e tyre të logaritjeve me formate të ndryshme të regjistrit (Shams et al. 2013]. Përdorimi i regjistrave të ndryshëm në cloud në secilën shtresë të një mjedisi cloud kompjuterik është një detyrë sfiduese për hetuesit ligjorë në lidhje me mbledhjen, ruajtjen, analizimin dhe regjistrimin e të dhënave të regjistrit [Shams et al. 2013]. Çdo log në shtresat e ndryshme të cloud computing mund të sigurojë informacion jetik për procesin ligjor dhe duhet të arrihen për prova të rëndësishme. Megjithatë, një aplikacion i vetëm që ekzekutohet në një makinë virtuale mund të ketë disa regjistra të ruajtura në serverë të analizave të shumta të regjistrave të vendosur në cloud të ndryshme, duke ngadalësuar procesin CLF për shkak të aksesit, vonesat në rrjet, serverët e aksesuar, disponueshmëria e kështu me radhë. Hetimi i logeve të decentralizuara cloud për aktivitete me qëllim të keq në një situatë në kohë reale është sfiduese. Situata bëhet më sfiduese kur shkrimet cloud janë analizuar për serverët e analizës së logut cloud të vendosura në qendra të ndryshme të të dhënave cloud të ndryshëm të kontrolluar nga CSP të ndryshme. Për të sinkronizuar të gjithë serverat e shpërndarjes së analizave të shpërndarjes cloud kërkojnë gatishmërinë e të gjitha CSP-ve për të bërë analizën e logut të cloud më të menaxhueshme dhe transparente.

Formati i standardizuar i regjistrit cloud. Për shkak të skedarëve të ndryshëm të regjistrit cloud që gjenerohen në një mjedis cloud informatikë ka shumë formate të log-cloud që varen nga kërkesat. Për shembull, shkrimet e aplikacionit për cloud kanë formatin e tyre të logit për të regjistruar informacione, ndërkohë që shkrimet e rrjetit cloud kanë formatin e tyre për të regjistruar informacionin e paketës. Nuk është paraqitur asnjë format i vetëm i standardeve cloud për të përfaqësuar shkrime të ndryshme cloud brenda një formati të vetëm [Marty 2011]. Formati i vetëm i regjistrit cloud mund të ndihmojë hetuesit të hetojnë me lehtësi loget cloud derisa kanë përqendrim të plotë objektivat e tyre kryesore si analiza e logut cloud. Nga ana tjetër, është e mundur të humbasë disa lloje informacioni në regjistrimin e regjistrave cloud që mund të jenë thelbësore për identifikimin e aktiviteteve të dëmshme nga një sulmues. Për më tepër, është e mundur që aplikimi i aplikacionit cloud në cloud-1 të ketë një format log, ndërsa i njëjti aplikim cloud që konkurron në një cloud tjetër të tillë si cloud-2 përdor një format të logut tjetër të cloud. Formatet e shumta të regjistrave cloud për aplikimin e njëjtë cloud e bëjnë procesin e hetimit më të paqartë dhe kompleks për hetuesit për të analizuar të dhënat e regjistrit cloud në një situatë në kohë reale. Si rezultat, një format i logaritmit të standardizuar cloud është thelbësor për kryerjen e CLF të saktë dhe të besueshëm. Zgjidhja e propozuar e lartpërmendur mund të zbatohet më lehtë kur një organizatë regjistron vetëm atë që ata besojnë se është e rëndësishme për ta. Prandaj, shënimet e shënimeve të regjistrit do të reduktohen dhe do të lehtësojnë automatizimin e regjistrimeve cloud duke prodhuar një format të vetëm log.

Drejtësia e Analizës së Identifikimit të Regjistruar. Sfida kryesore për kryerjen e hetuesve cloud nga CLF po verifikon drejtësinë e procesit të analizës së logeve cloud. Në shumicën e rasteve, analiza e regjistrit cloud bëhet nga stafi i vogël administrativ, si më pak prioritet i jepet për të analizuar regjistrimet cloud. CSP-të fokusohen më pak në analizën e logut cloud për shkak të besimit se ajo ofron pak përfitime, duke pasur parasysh prodhimin e vogël duke analizuar sasi të mëdha e të dhënave dhe duke marrë një sasi të madhe të kohës. Megjithatë, ky nuk është rasti. Koha e shpenzuar në hetimin e regjistrit cloud u ndihmon CSP-ve të kuptojnë rrjedhën e punës së informacionit të regjistruar si dhe të identifikojnë dobësitë e regjistruara brenda logeve cloud për t'i ndihmuar ata në zbulimin dhe parandalimin e dobësive në të ardhmen. Megjithatë, si mund ta kuptojë përdoruesi i cloud se analiza e regjistrit të kryer nga CSP është e

vlefshme, që do të thotë se analiza kryhet pa ndonjë ndryshim ose modifikim të të dhënave të regjistrit cloud? Në mënyrë të ngjashme, si mund të verifikohet analiza e kryer në shkrimet e reve është origjinale ose analiza përmban të gjitha informacionet e regjistruara që duhej të ishin të pranishme? CLF duhet t'i përgjigjet pyetjeve të lartpërmendura për të siguruar që procesi i hetimit është i drejtë dhe i qartë përpara përdoruesit të cloud dhe gjykatës. Mjetet e analizës së logut cloud automatik duhet të zhvillohen për të analizuar skedarët e logut cloud të gjeneruara në burime të ndryshme në cloud-informatikë. Nëse vetëm një individ është i përfshirë në kryerjen e analizës së logeve cloud , a ka më shumë shanse të humbasë informacionin e dobishëm gjatë analizës me qëllim ose pa qëllim, duke e bërë të gjithë procesin hetues të anshëm? Probabiliteti i padrejtësisë në kryerjen e analizës së logeve cloud duke përdorur mjete automatike CLF mund të minimizohet duke zvogëluar ndërhyrjen njerëzore. Ngjashëm, CLF automatike duhet të mbledhë skedarë të logut cloud nga resurset e ruajtjes së regjistrit të cloud, duke siguruar integritetin e të dhënave përmes përdorimit të metodave të ndryshme të sigurisë së të dhënave.

Përfundime dhe drejtimet në të ardhmen

Së pari, unë paraqes rezultatet përfundimtare të nxjerra nga pjesët e artikullit. Më pas, unë paraqes drejtimet e ardhshme për CLF për të udhëhequr kërkuesit, CSP-të, hetuesit, ligjvënësit dhe shitësit e rënë për t'i ndihmuar ata të përpunojnë këto çështje të hapura për ta bërë CLF më realiste dhe të zbatueshme.

Përfundime

Integrimi i logeve cloud me hetimet ligjore digjitale ka prodhuar një fushë të re kërkimi, që është, CLF në sigurinë cloud kompjuterike. Kohët e fundit janë kryer punë të ndryshme kërkimore në CLF që kanë propozuar zgjidhje. Për shembull, Shams et al. [2013] propozoi një arkitekturë të sigurt të regjistrimeve cloud që mbledh informacion nga shkrimet e shpërndara për të gjeneruar një imazh të vetëm të operacionit duke ofruar hetime të thella. Në Marty [2011], një kolektor dhe përpunues i vetëm i regjistrit futen për të siguruar të dhëna të besueshme dhe të sigurta për hetuesit në mënyrë të standardizuar. Menaxhimi i centralizuar i regjistrit ul kohëzgjatjen e kohës për përdoruesit dhe organizatat. Përveç të gjitha hulumtimeve të kryera në CLF, ende ka çështje të ndryshme që do të adresohen për të bërë një implementim të vërtetë të CLF. Një opsion i përshtatshëm është të gjenerohet shkrimet për secilën dhe çdo ngjarje që ndodhin në cloud-computing për të regjistruar të gjitha sjelljet me qëllim të keq. Megjithatë, shkrimet cloud janë krijuar në vende të ndryshme, duke rezultuar në një numër të madh të skedarëve të regjistrit të cloud që kërkojnë menaxhimin e duhur të regjistrit cloud . Menaxhimi i regjistrit cloud është i domosdoshëm për të siguruar që shkrimet cloud janë të ruajtura në burime të sigurta me informacione adekuate për periudha të caktuara kohorePër shembull, nuk ekziston ndonjë politikë e aksesit në lidhje me aksesin në skedarët e regjistrit cloud nga resurset e llogaritjes së resurseve cloud, nuk ka mekanizëm integrues të të dhënave për skedarët e logut cloud, ekziston një mungesë e privatësisë së të dhënave të përdoruesit në skedarët e logut cloud dhe kështu me radhë. Për të kapërcyer problemet e lartpërmendura të CLF, ofruesit e log-as-a-shërbimit duhet të punojnë në një sërë rekomandimesh që përfshijnë: (a) krijimin e një politike të standartizuar dhe grupeve të standardizuara të procedurave, (b) krijimin dhe mirëmbajtjen e një (d) caktimin e fuqisë punëtore të ekspertëve për menaxhimin e logeve cloud, (e) dhënien e prioriteteve për regjistrimet operacionale cloud, (f) zhvillimin e

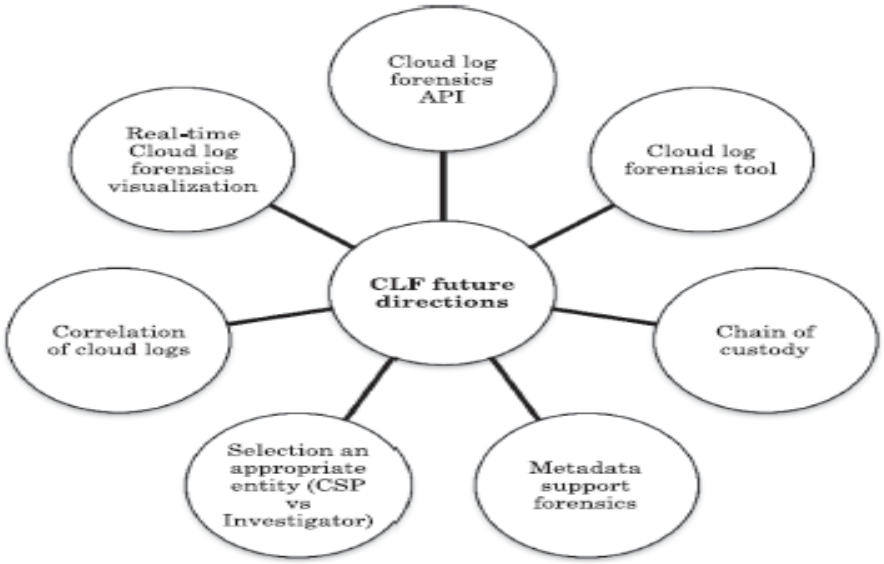

Fig. 5. Future directions for cloud log forensics.

Fig. 5. Drejtimet e ardhshme per cloud log forensics(ACM Computing Surveys, Vol. 49, No. 2, Article 8, Publication date: May 2016.)

një procesi operacional të standardizuar për regjistrimet cloud, dhe (g)) duke korreluar shkrimet e shpërndara cloud me një menaxhim qendror të regjistrit cloud.

Drejtimet në të ardhmen

Në këtë seksion paraqiten drejtime të reja kërkimore në kontekstin e CLF. Megjithatë, CLF është ende në fazën e hershme të hulumtimit për të ofruar mundësi të shumta për punën e ardhshme teknike dhe ekonomike për të zbutur sfidat që lidhen me të menaxhimin e dorës së parë. Çdo drejtim i ardhshëm siç tregohet në Figurën 5 do të sjellë fokusi i akademikut, industrialistëve, shitësve dhe PSK-ve për të hulumtuar thellë zgjidhje për CLF për t'i bërë ato të zbatueshme në kuadër të cloud computing.

*Regjistrimi iligjit cloud API.*Aktualisht, informatika cloud ofron API të ndryshme për të ndihmuar klientët të bashkëveprojnë me resurset cloud për shërbime të ndryshme duke përfshirë ruajtjen dhe llogaritjen. Megjithatë, CLF i mungon API të standardizuara për të ndihmuar hetuesit të aksesojnë në të dhënat e regjistrit cloud për analizimin e ngjarjeve me qëllim të keq që ndodhën në kohën e sulmit. Në Patrascu dhe Patriciu [2014], propozohet API për forenzikë cloud, që është përdoret për të mbledhur të dhënat e regjistrit nga VM në shtresën e virtualizimit. API për forenzikë cloud të propozuar mungon në aftësinë për të ofruar të dhënat e regjistrit midis VM-ve të ndryshme, të cilat mund të jenë jetike për sulmet e kanalit të VM-së. Prandaj, është e nevojshme të zhvillohen API unike dhe të sigurta për CLF për të siguruar të lehtë dhe lidhjet e sigurta për hetuesit për të analizuar të dhënat e regjistrit cloud brenda dhe jashtë saj. Si rezultat, përdoruesit e cloud-it do të ndihen më të rehatshëm në aksesin në të dhënat e tyre në cloud, ndërsa aksesi përmes API-ve të sigurta CLF në cloud. Prandaj, API-të e reja të regjistruara të cloud-it për forenzikë janë të nevojshme për hetim të plotë dhe të saktë të të dhënave të regjistrit cloud.

Zinxhiri i Kujdestarisë. Zinxhiri i Kujdestarisë (CoC) i referohet regjistrimit të shteteve në vijim gjatë një ngjarjeje pa humbur asnjë informacion për shkak të modifikimit dhe fshirjes. KQV është e rëndësishme për të kuptuar të gjithë procesin duke lidhur secilin ngjarje në tjetrën për nxjerrjen e informacionit të dobishëm. Në CLF, CoC është definuar si ndryshe atributet që përfshijnë dëshmi të verifikueshme, lokacionet e regjistrave, pozicionet e ruajtjes së regjistrit, metodat e aksesit në regjistër dhe procesi i grumbullimit të regjistrave që shpjegon dhe verifikon çdo hap, domethënë nga mbledhja e dosjeve të regjistrit deri tek paraqitja e dëshmive të evidencave në gjykatë. Në përgjithësi, CoC duhet të sigurojë në cloud llogaritje se si skedarët e regjistrit u krijuan, ruheshin, analizoheshin dhe paraqiteshin në gjykatë.

Forenzika për Mbështetjen e Metadatave. Metadata e shkronjave cloud luan një rol jetësor në sigurimin dëshmi mbështetëse për çdo shkelje në cloud-computing. Metadata e regjistrave cloud mund të përfshijë krijimin e skedarëve të llogaritjeve, aksesit, modifikimin, zhvendosjen e resurseve dhe madhësinë e saj. Informacioni mbi të dhënat jep informata të dobishme për hetuesit në analizimin e logeve cloud lehtë. Për shembull, një skedar log cloud u krijua në një kohë të caktuar dhe meta të dhënat e tij u ruajtën me statusin e tij aktual të informacionit. Më vonë, në qoftë se skedari i logut cloud migron në një burim tjetër brenda të njëjtit cloud ose në një cloud tjetër, ai do të ndryshojë informacionin e meta të dhënave për shkak të aksesit, migrimit dhe formimit të regjistrit pas faktit. Në mënyrë të ngjashme, në rastin e akseseve të shumëfishta në skedarin log të cloud nga përdorues të shumëfishtë, ndryshohet metoda e informacionit në lidhje me logun cloud, gjë që krijon paragjykim në CLF sa i përket gjetjes së saktë të individit / përdoruesit përgjegjës për aksesin në regjistrat cloud. Metadata e skedarit të logut cloud mund të shkarkohet nga hetuesi për të analizuar të dhënat kur ai është aksesuar ose modifikuar më vonë nga një individ tjetër për të krijuar dëshmi të pasakta në lidhje me hetimin e një shkeljeje në cloud-computing.

Miniera e të dhënave efikase dhe teknikat na kërkojnë që në mënyrë efikase të marrim informacion të dobishëm nga një metadata e madhe e regjistrimeve cloud me një përgjigje në kohë reale.

Përzgjedhja e një subjekti të përshtatshëm (CSP vs Hetues). Shumica e resurseve cloud brenda territorit të cloud computing janë në kontrollin e CSP, që rezultojnë nga pronësia e saj. Në procesin e hetimit të regjistrimeve cloud , një hetues duhet të ketë akses në të dhënat e regjistrit cloud për të analizuar ngjarjet me qëllim të keq. Kërkesa bëhet e domosdoshme kur kërcënimet duhet të hetohen në kohë reale për shkak të rrezikut të ashpër të sulmit. Sfida lind kur një sulm duhet të hetohet në të dhënat e regjistrit cloud në kohë reale, dhe aksesi i vetëm në regjistrat cloud është me CSP. Menaxhimi i duhur i reagimit të forenzikës na kërkon të identifikojmë me inteligjencë qëllimin e hetimit dhe të bëjmë një veprim të menjëhershëm për të kontaktuar CSP ose hetuesin e logut cloud. Për pyetjet hetimore, CSP mund të marrë të dhëna të regjistrit cloud për të analizuar situatën menjëherë në bazë të aftësive të tij të hetimit në vend të dërgimit të të dhënave te hetuesi, gjë që kërkon shumë kohë. Megjithatë, në shumicën e rasteve, një hetues i ekspertëve duhet të hetojë shkrimet cloud për ngjarje me qëllim të keq që nuk mund të analizohen nga CSP. Vendimi për të identifikuar një njësi përgjegjëse (CSP ose hetues) për të pasur akses dhe për të hetuar të dhënat e regjistrit cloud kërkon një kuptim të sjelljes së sulmit dhe situatës. Kjo platformë e propozuar siguron një përfitim për skemat e aksesit në bazë të rregullave dhe skemave të mbrojtjes së të dhënave në cloud-computing. Në Santos et al. [2009], një platformë e besuar cloud computing është propozuar për IaaS për të siguruar një mjedis ekzekutimi të mbyllur kuti për të ekzekutuar një VM mysafir para se të kërkohet zyrtarisht nga përdoruesi.

Korrelacioni i Regjistrave Cloud. Menaxhimi transparent i cloud computing fsheh ekzekutimin e një aplikacioni nga përdoruesi me qëllim të sigurimit të një ndërfaqeje të thjeshtë për përdorim. Ngjashëm, loget e rrotës së aplikacioneve të përdoruesve që përdoren në burimet cloud janë fshehur nga përdoruesit e cloud-it dhe informacioni përfshin atë, kur, ku dhe si bëhet regjistrimi. Në cloud computing, një regjistrim mund të krijohet në një cloud, ndërsa ajo është ruajtur në një cloud tjetër. Formatet e ndryshme të regjistrit dhe të dhënat e kohës krijojnë një sfidë për të ndërlidhur skedarë të ndryshëm të të dhënave të një aplikacioni të njëjtë të ruajtur në burime të ndryshme të cloud. Sinkronizimi i kohës brenda një regjistri cloud është një sfidë e madhe për forenzikën, veçanërisht në cloud-computing.

Vizualizimi i të dhënave të forenzikës së të dhënave në cloud në kohë reale. Detajimi i detajuar i ekzekutimit të një aplikacioni është i fshehur nga përdoruesit e cloud-it për shkak të kompleksitetit të tij në resurset cloud. Secili përdorues cloud e sheh procesin e aplikimit thjesht si ndërveprim me ndërfaqen me cloud, ndërsa hapat aktual të ekzekutimit kryhen në mënyrë të përsosur. Ngjashëm, CLF kryhet në regjistrat cloud të gjeneruara nga vende të ndryshme të tilla si aplikacionet e përdoruesit, rrjetet, sistemet, burimet dhe pajisjet e sigurisë pa dhënë informacion mbi ekzekutimin e detajeve në hapat e hetimit të përdoruesve të saj. Aktualisht, një përdorues cloud është më shumë i ndërgjegjshëm për të njohur çdo ngjarje që lidhet me të dhënat brenda cloud-computing. Si rezultat, CLF duhet të sigurojë që të dhënat legjitime të përdoruesit nuk do të aksesohen ose ndryshohen gjatë hapave të hetimeve gjatë analizimit të të dhënave të regjistrit cloud. Opsioni më i mirë është të regjistrojë çdo hap të hetimit dhe ta paraqesë atë në një formë të vizualizuar. Vizualizimi i CLF do ta bëjë procesin e hetimit të thjeshtë dhe të kuptueshëm për përdoruesit e rinj dhe do të përzënë vendim për veprimet e ardhshme. Prandaj, rritja e sasia e të dhënave të regjistrit të cloud-it të gjeneruar në cloud-computing kërkon një mjet vizualizimi për të ofruar analiza parashikuese, përshkrimi dhe recetë për të dhënat e regjistrit cloud për të ndihmuar hetuesit në një hetim në kohë reale.

Mjete për forenzikë të regjistrit në cloud. Të dhënat e regjistrit konsiderohen si një nga pjesët më të rëndësishme të provave kundër sulmeve të dëmshme gjatë hetimit të sulmit në cloud-computing. Të dhënat e regjistrit brenda skedarëve të regjistrave të cloud të vendosura në burimet e shpërndara të cloud-it duhet të analizohen në kohë reale, e cila është një sfidë e madhe. Për të kryer analiza në të dhënat e regjistrit të cloud-it, kërkohet një mjet automatik CLF për të mbledhur skedarët e regjistrit cloud nga vende të shpërndara dhe për t'i hetuar ato për nxjerrjen e provave të vlefshme. Në Thorpe et al. [2011a], Revista e Identifikimit të Veglave Virtual (VMLA) është propozuar si mjet për forenzikë të logut cloud për të siguruar një ndërfaqe grafike për afatet kohore të ngjarjeve të logaritmit të hypervisorit VM të mbledhura nga sisteme të ndryshme operative fizike. Objektivi primar i VMLA është që të ndihmojë hetuesin të dijë se cilat ngjarje të VM, përfshirë modifikimin, aksesin dhe krijimin, ndodhën në sistemin fizik operativ. Megjithatë, deri më tani, asnjë mjet i standardizuar CLF nuk është zhvilluar për të mbledhur dhe analizuar skedarët e regjistrit të cloud të vendosura në burime të ndryshme cloud. Pengesat për zhvillimin e mjeteve të CLF rriten për shkak të infrastrukturës së shtresës, shpërndarjes dhe mjediseve të virtualizuara, burimeve të shumta, rrjeteve dhe burimeve të përbashkëta, miliona përdoruesve dhe kontrollit të centralizuar të informatikës cloud. Për të kapërcyer pengesat e sipërpërmendura, profesionistët e industrisë duhet të bashkërendojnë me CSP dhe personelin ligjor për të zhvilluar mjete të reja CLF pa shkelur marrëveshjet në nivel shërbimi midis përdoruesit të cloud dhe CSP, si dhe ligjet e juridiksionit.

Referencat

1. Burton. 2014. Real-time log management and analytics at any scale. (2014). Retrieved November 16,2015, from https://logentries.com/.
2. Chuvakin, K. Schmidt, and Chris Phillips. 2013. *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*. Syngress, 460 pages.
3. Gani, G. M. Nayeem, M. Shiraz, M. Sookhak, M. Whaiduzzaman, and S. Khan. 2014. A review on interworking and mobility techniques for seamless connectivity in mobile cloud computing. *J. Network Comput. Appl.* 43 (2014), 84–102.
4. Holovaty. 2014. Django Makes It Easier to Build Better Web Apps More Quickly and with Less Code.(2014). Retrieved November 16, 2015, from https://www.djangoproject.com/.
5. Oliner, A. Ganapathi, and W. Xu. 2012. Advances and challenges in log analysis. *Commun. ACM* 55,2 (2012), 55–61.
6. Patrascu and V. V. Patriciu. 2014. Logging framework for cloud computing forensic environments. In *Proceeding of the IEEE 10th International Conference on Communications (COMM)*. 1–4.
7. Patrascu and V. V. Patriciu. 2015. Logging for cloud computing forensic systems. *Int. J. Comput. Commun. Control* 10, 2 (2015), 222–229.
8. Prasad and P. Chakrabarti. 2014. Extending access management to maintain audit logs in cloud computing. *Int. J. Adv. Comput. Sci. Appl.* 5, 3 (2014), 144–147.
9. Rafael. 2013. Secure log architecture to support remote auditing. *Math. Comput. Model.* 57, 7 (2013),1578–1591. Mizerany. 2014. Put this in your pipe and smoke it. (2014). Retrieved November 16, 2015, from http://www.sinatrarb.com/.
10. Mollamustafaoglu. 2014. We make alerts work for you. (2014). Retrieved November 16, 2015, from https://www.opsgenie.com/.
11. R. Carrier. 2006. Risks of live digital forensic analysis. *Commun. ACM* 49, 2 (2006), 56–61.
12. C. Yun, J. Y. C. Chang, B. B. C. Chiu, D. Y. Shue, Y. Kaneyasu, and J.W.Warfield. 2014. Ensuring integrity of security event log upon download and delete. (2014). *U.S. Patent No.* 8,856,086.
13. Oppenheimer. 2009. Loggly reveals what matters. (2009). Retrieved November 16, 2015, from https://www.loggly.com/.
14. Rong, S. T. Nguyen, and M. G. Jaatun. 2013. Beyond lightning: A survey on security challenges in cloud computing. *Comput. Electr. Eng.* 39, 1 (2013), 47–54.
15. J. Scales, M. Xu, and M. D. Ginzton. 2013. Low overhead fault tolerance through hybrid checkpointing and replay. *U.S. Patent No.* 8,499,297 (2013).
16. Birk. 2011. Technical challenges of forensic investigations in cloud computing environments. In *Workshop on Cryptography and Security in Clouds*. Zurich, Switzerland, 1–6.
17. D. Birk and C. Wegener. 2011. Technical issues of forensic investigations in cloud computing environments.
18. In *Proceeding of the IEEE 6th International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE)*. Washington, DC, USA, 1–10.
19. Casey. 2009. *Handbook of Digital Forensics and Investigation*. Academic Press, San Diego, CA, 600 pages.
20. Lindvall. 2014. How Papertrail makes life easier. (2014). Retrieved November 16, 2015, from https://papertrailapp.com/.
21. Rocher. 2005. A powerful Groovy-basedWeb application framework for the JVM. (2005). Retrieved November 16, 2015, from https://grails.org/.
22. Samudra. 2005. Extending Log4j to create custom logging components. In *Logging in Java with the JDK 1.4 Logging API and Apache Log4j*. Apress. 235–284.

23. A. Jahdali, A. Albatli, P. Garraghan, P. Townend, L. Lau, and Jie Xu. 2014. Multi-tenancy in cloud computing. In *Proceeding of the IEEE 8th International Symposium on Service Oriented System Engineering*. Oxford, United Kingdom, 344–351.
24. Chung, J. Park, S. Lee, and C. Kang. 2012. Digital forensic investigation of cloud storage services. *Digital Invest.* 9, 2 (2012), 81–95.
25. H. Mao, C. J. Wu, E. E. Papalexakis, C. Faloutsos, K. C. Lee, and T. C. Kao. 2014. MalSpot: Multimalicious network behavior patterns analysis. In *Advances in Knowledge Discovery and Data Mining*. Springer, Berlin, (2014), 1–14.
26. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan. The rise of "big data" on cloud computing: Review and open research issues. *Inform. Syst.* 47 (2015), 98–115.
27. M. Abbadi. 2014. *Cloud Management and Security*. John Wiley & Sons, New York, 238 pages.
28. Ray, K. Belyaev, M. Strizhov, D. Mulamba, and M. Rajaram. 2013. Secure logging as a service—delegating log management to the cloud. *IEEE Syst. J.* 7 (2013), 323–334.
29. Dykstra and A. T. Sherman. 2011. Understanding issues in cloud forensics: Two hypothetical case studies. *J. Network Forens.* 3, 1 (2011), 19–31.
30. Gerring. 2007. *Case Study Research. Principles and Practices*. Cambridge University Press, Cambridge, 278 pages. J. Hash, P. Bowen, A. Johnson, C. D. Smith, and D. I. Steinberg. 2008. An *Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*. Doctoral Dissertation, National Institute of Standards and Technology, 117 pages.
31. J. H. Beaver. 2015. Lessons on Efficient Log Analysis from Monex Insight. Case Study Report. Loggly Research. 3 pages. https://www.loggly.com/blog/lessons-efficient-log-analysis-monex-insight/.
32. Kent, S. Chevalier, T. Grance, and H. Dang. 2006. Guide to integrating forensic techniques into incident response. *NIST Spec. Publ.* (2006), 800–886.
33. K.Kent andM. Souppaya. 2014. Guide to computer security log management. *National Institute of Standards and Technology* (2014). 72 pages.
34. L. K. Ryan, P. Jagadpramana, and B. S. Lee. 2011a. Flogger: A file-centric logger for monitoring file access and transfers within cloud computing environments. In *Proceedings of the International Joint Conference of IEEE TrustCom-11/11/IEEE ICESS-11/FCST-11*. 765–771.
35. K. L. K. Ryan,M. Kirchberg, and B. S. Lee. 2011b. From system-centric to data-centric logging-accountability, trust & security in cloud computing. In *Proceedings of the IEEE Defense Science Research Conference and Expo (DSR)*. Singapore, 1–4.
36. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. 2010. A view of cloud computing. *Commun. ACM* 53, 4 (2010), 50–58.
37. Baum. 2014. Analyze & troubleshoot your cloud applications. *Technical Report. SplunkStorm.* https://
38. www.splunk.com/web_assets/pdfs/secure/Storm_Product_Fact_Sheet.pdf. M. Bradley and A. Dent. 2010. Payment Card Industry Data Security: What it is and its impact on retail merchants. *Technical Report. Royal Holloway Series.* http://cdn.ttgtmedia.com/searchsecurityuk/downloads/RHUL_Bradley_2010.pdf.
39. Prabha, C. Timotta, T. Rajan, and A. Jaleef PK. 2014. Encrypted query processing based log management in the cloud for improved potential for confidentiality. *Int. J. Comput. Appl. Technol. Res.* 3, 5. (2014), 309–311.
40. Santos, K. P. Gummadi, and R. Rodrigues. 2009. Towards trusted cloud computing. In *Proceedings of the 2009 Conference on Hot Topics in Cloud Computing.* 3–3.
41. Heath. 2014. Monitor your apps every single second. (2014). Retrieved November 16, 2015, from http://www.bmc.com/truesightpulse/customers/.

42. M. Trenwith and H. S. Venter. 2014. A digital forensic model for providing better data provenance in the cloud. In *Proceedings of the IEEE Information Security for South Africa (ISSA)*. 1–6.
43. Han, M. Shiraz, A. Gani, M. Whaiduzzaman, and S. Khan. 2014. Sierpinski triangle based data center architecture in cloud computing. *J. Supercomput.* 69, 2 (2014), 887–907.
44. A. Popa, J. R. Lorch, D. Molnar, H. J.Wang, and L. Zhuang. 2011. Enabling security in cloud storage SLAs with cloudproof. In *Usenix Annual Technical Conference*. 242 (2011).
45. R. Buyya, C. S. Yeo, and S. Venugopalirk. 2008. Market-Oriented cloud computing: Vision, hype, and reality for delivering IT services as computing utilities. In *Proceeding of the IEEE 10th International Conference on High Performance Computing and Communications*. 5–13.
46. R. Buyya, C. S. Yeo, S. Venugopalirk, J. Broberg, and I. Brandic. 2009. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Comput. Syst.* 25, 6 (2009), 599–616.
47. R. Dahl. 2014. Node.js on the Road. (2014). Retrieved November 16, 2015 from https://www.joyent.com/ noderoad.
48. R. Marty. 2011. Cloud application logging for forensics. In *Proceedings of the 2011 ACM Symposium on Applied Computing*. ACM, New York, NY, 178–184.
49. R. Vaarandi andM. Pihelgas. 2014. Using security logs for collecting and reporting technical security metrics. In *Proceedings of the IEEE Military Communications Conference (MILCOM)*. 294–299.
50. Ahmad, B. Ahmad, S. M. Saqib, and R. M. Khattak. 2012. Trust model: Cloud's provider and cloud's user. *Int. J. Adv. Sci. Technol.* 44, (2012), 69–80.
51. S. Butterfield, E. Costello, C. Henderson, and S. Mourachov. 2014. Slack so yeah, we tried slack. (2014). Retrieved November 16, 2015, from https://slack.com/.
52. S. Khan, A. Gani, A. W. A. Wahab, and M. A. Bagiwa. 2015. SIDNFF: Source identification network forensics framework for cloud computing. In *Proceeding of the IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW)*. 418–419.
53. Simon. 2014. KPI Dashboards that put your data to work. Retrieved November 16, 2015, from https://www.geckoboard.com/.U. Flegel. 2002. Pseudonymizing unix log files. In *Infrastructure Security*. Springer, Berlin, 162–179. V. Wesley, T. Harris, L. Long Jr., and R. Green. 2014. Hypervisor security in cloud computing systems. *ACM Comput. Surv.* (2014), 1–22.
54. X. Lin, P. Wang, and B. Wu. 2013. Log analysis in cloud computing environment with hadoop and spark. In *Proceedings of the IEEE 5th International Conference on Broadband Network & Multimedia Technology (IC-BNMT2013).* 273–276.
55. Z. Nik. 2011. Detection of network security breaches based on analysis of network record logs. *U.S. Patent No.* 7,904,479 (2011).