Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie
ISSN: (Online) 2222-4173, (Print) 0254-3486

Argitektuur vir die proaktiewe verkryging en analise van forensiese inligting in wolkstelsels

Authors:
D.J. Ras[1]
H.S. Venter[1]

Affiliations:
[1]Department of Computer Science, University of Pretoria, South Africa

Corresponding author:
D. Ras,
dras@cs.up.ac.za

How to cite this article:
Ras, D.J. & Venter, H.S., 2016, 'Argitektuur vir die proaktiewe verkryging en analise van forensiese inligting in wolkstelsels', *Suid-Afrikaanse Tydskrif vir Natuurwetenskap en Tegnologie* 35(1), a1418. http://dx.doi.org/10.4102/satnt.v35i1.1418

Architecture for the proactive acquisition and analysis of forensic information in cloud systems. Cloud systems have to deal with massive amounts of distributed, volatile data which makes forensic investigations difficult. Using the NIST reference architecture, a system is devised to proactively capture forensic data that can be used in an investigation. The system proposes using nested virtual machines with forensic capabilities.

Sedert die 1980s het die kapasiteit van rekenaarstelsels skerp toegeneem. Hiermee saam het die voorkoms van rekenaarmisdaad ook drasties gestyg. Digitale rekenaarforensika word ontwikkel om misdade te ondersoek en skuldige partye regtens te vervolg.

Met die koms van grootskaalse wolkrekenaarstelsels het die behoefte om forensiese ondersoeke op massiewe onbestendige stelsels uit te voer, toegeneem. Die data op hierdie stelsels kan boonop oor 'n groot hoeveelheid fisiese nodes versprei wees. Die standaardprosedures vir rekenaarforensika, soos vervat in die ISO 27043-standaard, is in hierdie omstandighede onvoldoende. Dit is byvoorbeeld nie wenslik om in 'n kommersiële omgewing 'n hele wolkstelsel af te skakel om 'n ondersoek te doen nie. Die koste van die ondersoek, wat betref ongebruikte mannekrag en verbeurde inkomste, maak 'n effektiewe ondersoek onmoontlik. 'n Forensiese ondersoek behels dat data gevind word, die herkoms daarvan nagespeur word, en die integriteit daarvan bepaal word. Weens die grootte, verspreidheid en onbestendigheid van die stelsel is al hierdie take kompleks en tydrowend. Dit is uit die aard van die saak noodsaaklik dat ondersoeke met minimale onderbreking uitgevoer word. Die bogenoemde probleme kan verminder of uitgeskakel word deur 'n metode te ontwikkel waarvolgens data proaktief in wolkstelsels versamel kan word.

Hierdie navorsing is daarop gemik om 'n metode te ontwikkel wat forensiese ondersoeke in die genoemde omstandighede sal vergemaklik. Dit gebruik die National Intitute of Standards and Technology (NIST) in Amerika se verwysingsargitektuur van wolkstelsels en pas die huidige ISO-standaard vir digitale en rekenaarforensika toe. Die voorstel behels dat virtuele rekenaars in die wolkstelsel genes word. In plaas daarvan dat 'n standaard- virtuele rekenaar direk op die wolkbedryfstelsel ontplooi word, word die virtuele rekenaar binne 'n forensiese virtuele rekenaar bedryf. Dit het tot gevolg dat die forensiese virtuele rekenaar alle kommunikasie van die standaard- virtuele rekenaar met enige ander stelsels kan monitor. Die kommunikasie wat die forensiese virtuele rekenaar onderskep, kan weggevoer word na 'n forensiese stelsel wat ook in die wolk bedryf word.

Die forensiese stelsel bestaan uit die berging van hutskodes en forensiese inligting, en 'n analisemasjien. Die stelsel stoor slegs die hutskodes van lêers in die verskeie virtuele rekenaars. Die forensiese inligtingberging stoor die inligting wat verkry is deur die spesifieke onderskepping deur die forensiese virtuele rekenaar. Laastens verwerk die analisemasjien die inligting in die bergingseenheid na 'n formaat wat aanvaarbaar is vir die ondersoekspan.

Dit is wel nie prakties om al die data van al die virtuele rekenaars in die wolkstelsel te onderskep nie. Dus word die virtuele forensiese rekenaars beheer deur 'n forensiese beheerder. Die beheerder is aan die sekerheidstelsel van die wolk gekoppel en bepaal die vlak van waaksaamheid van die forensiese stelsel. Sodra 'n aanval teen 'n spesifieke virtuele rekenaar vermoed word, kan die onderskepping van inligting vir die betrokke rekenaar opgeskerp word. Die daarstelling van al hierdie komponente vergemaklik die realisering van proaktiewe forensika in die wolk.

Note: A selection of conference proceedings: Student Symposium in Science, 29–30 October 2015, University of the Free State, South Africa. Organising committee: Mr Rudi Pretorius and Ms Andrea Lombard (Department of Geography, University of South Africa); Dr Hertzog Bisset (South African Nuclear Energy Corporation (NECSA); Dr Ernie Langner and Prof Jeanet Conradie (Department of Chemistry, University of the Free State).