Digital Forensics Challenges to Big Data in the Cloud

Xiaohua Feng
Department of Computer Science and Technology
University of Bedfordshire
Luton, UK
Xiaohua.feng@beds.ac.uk

Yuping Zhao
Microwave Wireless Telecommunications Research Lab
School of Electronics Engineering and Computer Science
Peking University, Beijing, China
yuping.zhao@pku.edu.cn

***Abstract* — As a new research area, Digital Forensics is a subject in a rapid development society. Cyber security for Big Data in the Cloud is getting attention more than ever. Computing breach requires digital forensics to seize the digital evidence to locate who done it and what has been done maliciously and possible risk/damage assessing what loss could leads to. In particular, for Big Data attack cases, Digital Forensics has been facing even more challenge than original digital breach investigations.**

Nowadays, Big Data due to its characteristics of three "V"s (Volume, Velocity, and Variety), they are either synchronized with Cloud (Such as smart phone) or stored on the Cloud, in order to sort out the storage capacity etc. problems, which made Digital Forensics investigation even more difficult. The Big Data-Digital Forensics issue for Cloud is difficult due to some issues. One of them is physically identify specific wanted device. Data are distributed in the cloud, customer or the digital forensics practitioner cannot have a fully access control like the traditional investigation does.

The Smart City technique is making use of ICT (information communications technology) to collecting, detecting, analysing and integrating the key information data of core systems in running the cities. Meantime, the control is making intelligent responses to different requirements that include daily livelihood, PII (Personally identifiable information) security, environmental protection, public safety, industrial and commercial activities and city services. The Smart City data are Big Data, collected and gathered by the IoT (Internet of Things).

This paper has summerised our review on the trends of Digital Forensics served for Big Data. The evidence acquisition challenge is discussed. A case study of a Smart City project with the IoT collected services Big data which are stored at the cloud computing environment is represented. The techniques can be generalised to other Big Data in the Cloud environment.

Keywords ***–Big data, Cloud Computing, Smart City system, IoTS, Cyber security and Personally identifiable information (PII) data protection, Personally Information against cyberstalking***

I. INTRODUCTION

Digital Forensics is important in cyber security. Evidence data is crucial for Digital Forensics. Big data evidence collecting is challenging in the cloud.

While Big Data is defined as a large collection of data sets which is too complex to be processed by people's hand. Instead, it needs database management tools to be handled. Big Data is a science/technology which analyses huge amount of data in order to find out the rules, collect valuable opinions and predict complex problems. It maybe involves capture, storage, search, sharing, transfer, analysis and visualization。

Big Data includes Volume, Velocity, and Variety (Veracity); especially in the Cloud environment these three "V"s determine their characteristics.

Volume is the amount of data, usually when data capacity reaches up to Terrabyte (1024 GB) and Pettabyte (1024 TB, 1,048,576 GB).

Velocity is the speed of collecting, processing and using data. Big Data Security often needs speedy processing or even real time processing data.

Velocity becomes a vital measure of big data usage, especially when real time data process is required. Variety is the type of big data involved. In current era, Big Data usages include text, audio, video and multimedia types of data format.

Currently, there is large volume of data available, which brings challenges for digital investigation. For example, challenges in data collection, data analysis, data recovery and many more (Harshish and Feng, 2011). The problem solving is complicated and is still in progress. (Alessandro, 2015)

At the Smart City project of the research, Big data are collected by the IoT automatically; which is a system combined information system communications technology which makes use of radio frequency identification and

electronic product code techniques to service global applications.

In our case study, the collected Smart City Big Data are stored at the intermediate nodes, (Liu, 2014) then the Computer Clouds. This is challenging to digital forensics whenever an investigation is needed. I will discuss the details next.

II. RECENT DEVELOPMENT

With technologies development, our society has changed enormously. These have a big impact on conventional digital forensics investigations. With the enhancement, Big Data could provide much more in terms of quality of service than before.

II.1 Big data development

The recent data science development such as health record, daily sports data, and national healthcare as well as smart city project demonstrated the future trends on Big Data applications. Big Data is ideal for Digital forensics security. Identifying cloud security threats is largely about looking for data patters that are out of the ordinary, whether it is an unauthorised user from an unknown IP address or a distributed denial of service (DDoS) attack. Understanding Big data techniques allows you to analyze cloud incoming and outgoing traffic to reveal anomalies that point to a data breach (Ernst & Young, 2015).

Its Volume, Velocity, and Variety characteristics has attracted majority of researchers pay more attention on social media and data science related subjects (Sremack, 2015).

II.2 Cloud computing development

There are three popular Cloud computing service models to be known:

SaaS (Software as a Service) the best known service model

PaaS (Platform as a Service) service model and

IaaS (Infrastructure as a Service) service model.

Their pros and cons are: at SaaS, the only thing users could be get involved is the access control (AC).

While at PaaS, apart from access control, users could also get involved with applications.

And at IaaS, users could be got involved with data load and operating system as well.

These characteristics heavily affected Digital Forensics investigations. Further more, PII (Personally identifiable information) is attracting more and more attention and related to majority people's everyday activities, such as Carphone warehouse and G20 cases (BBC, 2015a, b). That added a pressure on Digital Forensics to investigate PII breach in the Cloud.

III THE FORENSICS CHANLLENGES

Due to the cloud distribution feature, the conventional data acquisition regulation has not enough to meet the digital forensics evidence requirements. For instance, it is almost impossible to seize a physical hard drive to get all of the related forensics evidence for a case.

Many digital Forensics evidence acquisition issues are depending on the case are related to the CSP (Cloud Service Provider)'s support or co-operation. Zawoad (2013) has listed some updated cloud issues. The distributed data centre may cross several national borders in storage. That might make the Chain of Custody (CoC) as an important part of the document extremely difficult. When Big data in the cloud, the investigator officer has no physical control of device, the only possibility is rely on the CSP. If the related CSP is not technically competent or without to be trained sound forensically, there is no guarantee that the audit trail could be put into the Chain of Custody forms and could be completed appropriately for the future testimony.

Multi-state legal issue could be affected to obtain permissions for authentication of evidence search as well. For instance, if the case related data centre located at a country which does not have a Data Protection Act, trying to get the authorised data will be difficult.

A summary of Big Data digital forensics challenges in the cloud is reviewed and the consequence is as Table 1 shown; where the issues marked a yes (a "Y") shown problem outstanding; means further development work is still required currently; while the issues have a solution has been marked a no (i.e., a "N").

IV A CASE STUDY

Since 2014, a world-leading project in autonomous transportation systems and intelligent mobility (Sant, 2015) has started. The Milton Keynes Smart City project focuses on the application of the next-generation of information technology to all walks of life, thereby embedding sensors and equipment to vehicles on roads and railways, bridges and tunnels, mobile communications systems, and others in every corner of the place, thereby forming the internet of things through the internet. This will enable us integrate the Internet of things (IoTS) through powerful computer clusters and cloud computing. This will enable people to manage productivity and life more meticulously and in a more dynamic manner, leading to a state of global intelligence.

It is a typical Big Data collected by the IoTS and stored in the computer cloud. Here, we will discuss about Big Data in Smart City Project where IoTS and raspberry pies gathered information; *i.e*., Big Data in the cloud and their access security issues emerged, as well as the Digital Forensics cloud challenge solution with the impact on PII (ISO, 2014).

In this case study, the smartphone as an IoTS terminal device to collect customer's information data, the data volume of which is consistently increasing; *i.e*, Big Data formed. Then the substantial various data are transmitted to the cloud service provider to come up as Big Data in the cloud. The Smart City control centre according to these data to provide local information and suggest the best service, in order to make the customer has a very enjoyable stay at Milton Keynes. Therefore, Big information and interactive data generated. And in order to get cyber security, data acquisition, processing and storage become the consequence correspondingly.

In this case study, the smartphone as an IoT terminal device to collect customer's information data, the data volume of which is consistently increasing; *i.e*, Big Data formed. Then the substantial various data are transmitted to the cloud service provider to come up as Big Data in the cloud. The Smart City control centre according to these data to provide local information and suggest the best service, in order to make the customer has a very enjoyable stay at Milton Keynes.

However, if these Big data are breached, the provided information could be false, which maybe leads to serious crime. Then the digital forensics practitioner will walk in and acquire evidence to locate the suspect.

Nevertheless, in the cloud, Big Data of the Smart City are not the only data exist in that cloud. It might be distributed at several locations and at different sectors of the storage. If these data are hacked, the driverless vehicle is crashed. It would be extremely difficult to get a warrant, visit the crime scene, acquire the possible evidence, image the Big Data, filling-in the CoC (Chain of Custody) forms, preserve the acquired evidence (as Table 1 shown). Then examine recovered data and work out the analysis to report to the law enforcement.

The investigation officer needs to bear in mind; he does not own the cloud utility, no matter SaaS, PaaS or IaaS as the following table shown.

Many tasks need to be done by the CSP's help. Even under the CSP's support not all the investigation works could be complete as an individual digital/computer system experienced (Feng, 2015). The SaaS is the best developed service. However, apart from access control, authorized investigation officer cannot control the applications, data load, operating systems, servers and network system.

IaaS is the most closet to hardware scenario when a digital forensics cloud investigation is carried out. However, an IaaS user cannot get control of the servers and network system of the IaaS fully for the authorized investigation officer.

Digital forensics challenges to Big Data in the Cloud	Cloud services			Note
	SaaS	PaaS	IaaS	
Physical Access control/accessibility	Y	Y	Y	
CSP dependent	Y	Y	Y	Logs
Volatile data	Y	N	N	
Trustiness	Y	Y	Y	
Bandwidth	Y	N	N	
Multi-tenancy	Y	Y	N	
Distributed logs	Y	Y	Y	
Volatility of logs	Y	N	N	
Logs in multiple tiers and layers	Y	Y	Y	
Logs accessibility	Y	Y	Y	
Logs lack of critical information	Y	Y	Y	
Chain of Custody	Y	Y	Y	AC issues
Issues on existing forensic tools	Y	Y	Y	
Crime scene recognition	Y	Y	Y	
Crime scene reconstruction	Y	Y	N	
Multi-state laws	Y	Y	Y	
Report	Y	Y	Y	
Compliance	Y	Y	N	
Presentation	Y	Y	Y	
Combination issue	Y	Y	Y	
Integrity	Y	Y	Y	
Warrant	Y	Y	Y	
Localization	Y	Y	Y	locate

Table 1 Digital Forensics Challenges Big Data in the Cloud

V. DISCUSSIONS

Due to the volume issue, the investigation officer require an adequate bandwidth to image the virtual machine of the Big data in the cloud.

Ruan (2015) did a survey on cloud forensic capacity, the results shown, the majority lies on CSPs. With support from CSP, a read only API provided by the case relevant CSP for network, process and access logs to the representative of the customer to acquire some data by read only. Marty (2011) proposed an Ajax library for logging checking or imply log management in the cloud by the CSPs.

Hegarty et al (2011) suggested for each time uploading/downloading, checking data integrity as one of the problem solving solution; if anything suspicious going on, isolate the cloud immediately. Nevertheless it seems to complicate the cloud activities.

Another problem is potential multi location raised multi state-laws. In order to specify CSPs' responsibility in the cloud cyber security as well as their role in a digital forensic investigation, an updated Service Level Agreement (SLA) needs to be published and put into operation. Globally collaboration is required, all the states laws should apply.

VI. EVALUATION AND CONCLUSIONS

In this paper, we have explored the main Digital Forensics challenges about the Big Data with Cloud Computing PII in the cloud services. (Rezendes, 2015) (ISO, 2014). Updated impact has been discussed and problem solving solutions have been explored and critically analyzed. A serial of design and implementation have been carried out and there is still new development going on at the NCCR (National Centre of Cyberstalking Research) Institute, University of Bedfordshire, currently.

When the recent development finishes at the end of June, we can do a few decision making, according to further experiment results comparison and analysis (Feng, 2016), to recommend a more appropriate approach to sort out the Big data at Cloud Computing service environment issues for digital forensics investigations.

This digital forensics challenges with Big Data is crucial. Almost all the traditional way of investigation is not appropriate any longer, as cloud users lost control on many aspects. Here, a problem solving research with Big Data in the Cloud environment is significant for the upcoming cyber security applications in data science, such as the Smart City project. An impact on future cloud information governance, risk management, and compliance, trustworthiness (Liu, 2014) as well as human factor in Big Data cyber security would play an important role.

In particular, in Smart city projects, PII could be a cutting-edge element for citizen's trustiness (Petit, 2015) (Hoppe, 2008) and leads the consequence on the development and applications (Feng, 2015).

Since being created in 2004, European Network and Information Security Agency (ENISA) has done many works for the EU states. The Big Data and cloud development Big Data & Smart Sustainable Society Workshop -2016 pushes ENISA to produce more guideline and regulations to protect Big Data in the cloud. To date, we have investigated thoroughly about the outstanding issues, but there is still no perfect solution to sort all of these. There are more adventure work needed

VII. SUGGESTED FURTURE DEVELOPMENTS

Upon some of the Big Data digital forensics challenges we have summarized today, there are plenty of development need to be carried out to compromise the best trade-off between cloud application services and digital forensics in the Big Data cyber security; such as, analyze social media Big Data for cyber psychology issues; or analyze Big Data in the cloud for national citizen's health or sports activity record, data service for centralized national healthcare as well.

To date, there is still neither an appropriate professional digital forensic toolkit to carry out computing cloud investigations, nor for the Big Data cases. Guidance software and their peers need to speed up their developments.

Nowadays application research on cyber security field is getting more and more attention. Cyber psychology is one of the newly explorations. Cyber psychology is research on anything human psychology with Cyber technology related.

As a new cross-subject area, its aim and objectives are using the conventional psychology view to analyze the newly developed cyber techniques. Then provide user guide to make use of cyber resource and worked out efficient network management. Currently University of Bedfordshire NCCR is working on social media chat messages, which is another Big Data application. Its security is not only in technical side, but also in social psychology category.

So, using digital forensics technique to acquire social network messages and analyze the content becomes another Big Data challenge.

With Big Data and Cloud computing technology development, digital forensics will face more and more challenges in the near future. There are plenty of exploration for us to discover and work out the reasonable problem solving solutions.

REFERENCES

Alessandro Guarino (2015), "*Digital forensics as a Big Data challenge"*, eBook – 24 Aug 2015

Antoine Olivier, Mitchell Chris and Phillips John (2013), "*ISO/IEC 27018: The future standard for Personal Data protection in public cloud*", EBRC.

Zafarullah, Z.; Anwar, F. and Anwar Z. (2011), "*Digital forensics for eucalyptus*," in Frontiers of Information Technology (FIT). IEEE, 2011, pp. 110–116.

BBC (2015a): "*Carphone warehouse customer data breach investigated"*, BBC, UK, http://www.bbc.co.uk/news/uk-33840327, (Accessed: 08/08/2015).

BBC (2015b), "*G20 world leaders' data emailed to football organizers*.", http://www.bbc.co.uk/news/technology-32115443. (Accessed: 31/03/2015).

Bellare, M. and Rogaway, P. (2005): "*Introduction to modern Cryptography*". Verimag, France, pp.10. Available atwww-verimag.imag.fr/~plafourc/teaching. (Accessed: 04/10/2015).

Carrier, B. (2005): "*Filesystem forensic analysis*", Indiana: Addison Wesley Professional, 2005, ISBN: 9780321268174

Cohen, R. (2012) '*The past, the present, and the future of cloud computing*', Intel Technology Journal, 16 (4), pp.20-24.

Eric Cole (2015) "*Cyber Security Expert Professional*", Security Haven, www.securityhaven.com (Accessed: 22/2/2017)

Deekue S.; Feng X. and Liu, E (2013): "*A strategic framework for Nigeria e-government security*", ARSR2013 Workshop, University of Bedfordshire and Manchester, UK

Delport Waldo M. K. and Olivier Martin S. (2011), "*Isolating a cloud instance for a digital forensic investigation*", proceedings of the Information and Computer Security Architecture (ICSA).

Dykstra J. and Sherman A. (2011), "*Understanding issues in cloud forensics: Two hypothetical case studies,*" Journal of Network Forensics, vol.b, no. 3, pp. 19–31, 2011.

Ernst and Young (2013), "*Demystifying 'Big Data' analysis*". EY. 2013. http://www.isacantx.org/Presentations/2013-05Post-DemystifyingBigDataAnalytics,

(Accessed: 28/03/2016).

Fahad Abdullah Al (2015), "*Cloud computing security policy*", University of Bedfordshire, UK.

Farrell Paul (2015), "*Personal details of world leaders accidentally revealed by G20 organisers*", The Guardian, UK, March, 2015

http://www.theguardian.com/world/2015/mar/30/personal-details-of-world-leaders-accidentally-revealed-by-g20-organisers (Accessed: 31/3/2015)

Feng X. and Zhao Y. (2016): Cyber Security Data Mining with the Mobile Internet of Things (IoT) -- Personally Identifiable Information on Smart Technologies t, proceeding of the DaMIS 2016 -- International Workshop on Data Mining on Internet of Things Systems, U.K. 2016

Feng, X. and Zhang X. (2015) "*Personally identifiable information security in cloud computing*", International Conference on Computing and Technology Innovation (IEEE CTI-2015), May 2015, UK.

Feng X. and Louise, J. (2013), "*MITM attack detection on computing networks*", The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue: the Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13], San Francisco State University, CA, U.S.A., March 2013 Doi: 10.7321/jscse.v3.n3.78 e-ISSN: 2251-7545

Feng, X (2011) "*Computer Law in UK*", UCC Data Retriever, Digital Library Workshop, Ireland

Feng X. (2011) "*Incidence Response Strategies*", the 7th Annual Forensics Workshop, U.K.

Harshish M and Feng X. (2011) "*Challenges on Forensics, A Cloud investigations reference model*", STAN-2011, IEEE Symposium of Security, Technology and Networks.

Grispos, G. Storer, T. And Glisson, W. (2012), "*Calm before the storm: the challenges of cloud computing in digital forensics"*, International Journal of Digital Crime and Forensics (IJDCF), 2012.

Han, L. and Kendall G. (2003) "*An investigation of a tabu assisted hyper-heuristic genetic algorithm*", Evolutionary

Computation, 2003. CEC'03. The 2003 Congress on 3, 2230-2237

Hegarty R. Merabti M. Shi Q. and Askwith B. (2009), "*Forensic analysis of distributed data in a service oriented computing platform*", proceedings of the 10th Annual Postgraduate Symposium on The Convergence of Telecommunications, Networking & Broadcasting, PG Net.

Hoppe, T. Kiltz S., and Dittmann J., (2008). "*Security threats to automotive CAN networks-practical examples and selected short-term counter-measures*". Proceedings of Computer Safety, Reliability, and Security. 5 (2), pp. 235–248.

ICO (2014), "*Find out how to request your personal information*", http://ico.org.uk/for_the_public/personal_information. (Accessed: 7/5/2015).

ISO/IEC 27018: (2014), "*Information technology-- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, ISO 27018 standard*".

http://www.iso27001security.com/html/27018.html (Accessed: 24/3/2015)

Khoshgozaran A, Shirani-Mehr Houtan & Shahabi C. (2012), "*Blind evaluation of location based queries using space transformation to preserve location privacy*", Geoinformatica Journal, Volume 27, Issue 2, pp 413-427,

ISBN: 978-3-642-03510-4 Nov 2012.

Liu, E and Feng X. (2014): "*Trustworthiness in the Patient Centered Health Care System, Series: Communications in Computer and Information Science*", Volume, 426, Springer-Verlag, March, 2014

Ludwig Slusky M. D. and Parviz Partow-Navid, (2012) "*Cloud computing and computer forensics for business applications*," Journal of Technology Research, vol. 3.

Katz, J. and Lindell, Y. (2008), "*Introduction to modern cryptography*". Boca Raton: Chapman & Hall/CRC.

Marty R. (2011) "*Cloud application logging for forensics*," proceedings of ACM Symposium on Applied Computing, pp. 178–184.

Mollin, R.A. (2007), "*An introduction to cryptography*". 2nd Edition. Boca Raton, Flor. : Chapman & Hall/CRC.

Oltsik Jon, (2015): "*The Internet of Things: ACISO and network security perspective*", ESG (Enterprise strategy group) White Paper of Senior Principal Analyst.

http://www.cisco.com/web/strategy/docs/energy/network-security-perspective.pdf (Accessed: 08/08/2015).

Pollitt, M. (1995) "*Computer forensics: an approach to evidence in cyberspace*," National Information Systems Security Conference, vol. II, pp. 487-491, 1995.

Petit, J and Shladover S. (2015). "*Potential Cyberattacks on Automated Vehicles*". IEEE Transactions on Intelligent Transportation Systems. Vol. 16 (no. 2), pp.546-556

Reilly D. Wren C. and Berry T. (2011), "*Cloud Computing: pros and cons for computer forensic investigations*", International Journal Multimedia and Image Processing (IJMIP), vol. 1, no. 1, pp. 26–34, March 2011.

Rezendes Christopher J. and Stephenson W. David: (2013), "*Cyber security in the Internet of Things* " , https://hbr.org/2013/06/cyber-security-in-the-internet/ (Accessed: 08/08/2015).

Ruan K. Carthy J. Kechadi T. and Crosbie M. (2011), "*Cloud forensics: an overview*", in proceedings of the 7th IFIP International Conference on Digital Forensics, 2011.

Ruan K. Carthy J. Kechadi T. Crosbie M. & Bagglli I. (2013), "*Cloud* forensics definition and critical criteria for cloud *forensics capacity: an overview of survey results*", Digital Investigation Vol. 10, Elsevier, 2013.

Sant P. (2015), "*International PhD students learn about MK:Smart*", MK Smart and University of Bedfordshire, http://www.mksmart.org/enterprise/.

(Accessed: 08/08/2015).

Sremack Joe (2015) "*Big Data Forensics - Learning Hadoop Investigations*", Packt Publishing ISBN-10: 1785288105, ISBN-13: 978-1785288104 – 24 Aug 2015

Taylor M. Haggerty J. Gresty D. and Hegarty R.(2010), "*Digital evidence in cloud computing systems*," Computer Law and Security Review, vol. 26, no. 3, pp. 304–308,.

Uma Mohan and Saminu Salisu (2015) "*The use of big data in the field of digital forensics investigations*", International Journal of New Technologies in Science and Engineering, Vol. 2, Issue. 4, October 2015, ISSN 2349-0780 Available online http://www.ijntse.com 291

Zawoad Shams and Ragib H. (2013) "C*loud forensics: a meta-study of challenges, approaches, and open problems*", University of Alabama at Birmingham, USA.