Winter 12-13-2018

CHALLENGES AND BARRIERS TO DIGITAL FORENSICS IN THE CLOUD

Miloslava Plachkinova
University of Tampa, mplachkinova@ut.edu

CHALLENGES AND BARRIERS TO DIGITAL FORENSICS IN THE CLOUD

Miloslava Plachkinova, PhD
University of Tampa, FL
mplachkinova@ut.edu

ABSTRACT

Cloud computing provides individuals and organizations affordable access to various resources such as storage, servers, computing power, and software among others. The growing use of this decentralized approach presents many opportunities for cost and process optimization but at the same time it brings new challenges and barriers when it comes to solving crimes in the digital realm. For example, the cloud provides redundancy by making multiple copies of the data at various locations across the world. There are currently a lot of discussions regarding the ownership of the data on the cloud and jurisdiction issues because of the decentralized redundancy. So, when a crime occurs and data on the cloud is compromised, this brings up the problem of digital forensic investigations on third party networks and resources. While technology is progressing incredibly fast, policy makers tend to lag behind and not provide law enforcement with the necessary tools to solve some of these new 21st century crimes. The current paper provides an overview of some of the major challenges and barriers to digital forensic investigations involving the cloud. It offers recommendations for overcoming them and discusses directions for future research.

Keywords: Digital forensics, cloud computing, criminology, policy implications

CLOUD COMPUTING

One of the main advantages of cloud computing is that it eliminates the need to maintain complex, massive, and expensive hardware and software infrastructure. It requires no significant up-front investments and its scalability allows organizations and individuals to pay only for what

they use (Hashem et al., 2015). Armbrust et al. (2010) outline further obstacles and opportunities for cloud computing. More specifically, they discuss business continuity, data lock-in, data confidentiality and auditability of the cloud providers, software licensing, and performance unpredictability to name a few. While they touch upon a number of issues related to cloud utilization, they do it from a business information technology (IT) perspective. Current literature does not address in much detail the issues related to investigating crimes involving cloud solutions. Thus, the current study addresses this research gap and extends knowledge in the field.

Often times the consumers believe that the cloud is less secure than an in-house system (Kaufman 2010) because you cannot see where your data physically is and you have no control over its security and backup copies. To achieve maximum uptime, cloud providers make multiple copies of the data that could be stored anywhere in the world. While this practice provides excellent redundancy, it also raises numerous concerns as to the physical location of the data and the security profiles of the sites where it is located (Khan and Malluhi 2010). Such lack of transparency may be a significant issue for government agencies or healthcare facilities that may be required to host data on US soil only. Another issue related to the lack of trust in the cloud is the exploitation of various attacks, vulnerabilities, and threats. Modi et al. (2013) list several of those such as multi tenancy, vulnerabilities in the internet protocols being used, unauthorized access to management interfaces, browser vulnerabilities, malicious insiders, data loss/leakage, service hijacking, identity theft, and phishing to name a few.

REGULATIONS FOR DIGITAL FORENSICS

Digital forensics is a relatively new field and laws, regulations, and policies are yet to be fully developed. The Computer Crime and Intellectual Property Section (CCIPS) under the US Department of Justice is “responsible for implementing the Department's national strategies in

combating computer and intellectual property crimes worldwide"[1]. While the purpose of the attorneys who work at the agency is to improve the national legislature in the field of digital forensics, the US is still lagging in the development and implementation of legal frameworks for cybercrimes. For instance, some of the more pertinent laws would be: Wiretap Act, Pen Registers and Trap and Trace Devices Statute, and Stored Wired and Electronic Communication Act. It is interesting to notice that all of them were passed back in the 1980s. With the rapid speed that technology is changing, it is concerning that our legislature is so far behind. Furthermore, the CCIPS and the Department of Justice websites include mostly guidelines, manuals, reports, and white papers[2]. In addition, the National Institute of Justice has posted a document entitled "Electronic Crime Scene Investigation: A Guide for First Responders"[3]. While resources provide useful recommendations, they do not have the power of a law, they can only assist law enforcement officers in investigations involving digital assets. The US Computer Emergency Readiness Team (US-CERT) has also posted several resources on its website[4] but those are again directed towards prevention of cybercrimes and educating the public on the ramifications of these crimes. No specific information is offered on how to properly handle digital forensic investigations.

Although there is little legal direction on how digital forensic investigations should be conducted, there have been a couple of laws passed to protect the privacy of communications. More specifically, those are the Electronic Communications Privacy Act of 1986 and the Privacy Protection Act of 1980. Those were passed as a result of the "reasonable expectation of privacy" established in the Katz v US case from 1967 (Winn 2009). Overall, privacy seems to be defined

[1] https://www.justice.gov/criminal-ccips, accessed on 10/1/18
[2] https://www.justice.gov/criminal-ccips/ccips-documents-and-reports, accessed on 10/1/18
[3] https://www.ncjrs.gov/pdffiles1/nij/219941.pdf, accessed on 10/1/18
[4] https://www.us-cert.gov, accessed on 10/1/18

a lot better than the expectation for fair digital forensic investigations. A significant implication about this is the lack of consistency among the practices performed by investigators, which can potentially lead to inadmissible evidence in court.

Nance and Ryan (2011) identified two trends that can make digital forensics and criminal procedure even more complex. They saw the upcoming challenges of migrating to cloud platforms and predicted that it would lead to further blurring the boundaries between personal and corporate data and resources. Another issue the authors identified was the rapidly changing technologies that now have the ability to compromise our digital footprints and make criminal procedures even more complex. While these findings are completely valid and reasonable, it is concerning that the paper was published back in 2011 and not only that these issues have not been resolved but it seems like the problems are becoming even more serious with the growing amount of data we store on the cloud and the reliability on cloud services.

CLOUD COMPUTING CHALLENGES IN DIGITAL FORENSICS

Cloud forensics is the intersection between cloud computing and digital forensics and it is a subset of network forensics because essentially the cloud represents a network of virtual resources. Thus, similar practices should be employed when reviewing evidence on the cloud and on networks (Ruan et al. 2011). While this may seem like a simple extension of existing protocols for investigating computer networks, it actually poses a lot more issues for investigators due to the nature of the cloud. Its multi tenancy, multi jurisdictions, and dynamically changing data are just the tip of the iceberg.

Grispos et al. (2012) classified some of the most important challenges related to conducting digital forensic investigations on the cloud. The researchers utilize four principles of

digital forensic science as outlined by the Association of Chief Police Officers[5]. However, the authors focus more on the lack of tools and agreement on special procedures related to digital forensic investigations and processing evidence rather than on the lack of contemporary legislature in the field. Thus, clearly more research needs to be done to provide policy makers with more adequate resources to develop new regulations regarding digital forensics, especially in the cloud environment.

Most of prior research focuses on end user security and privacy concerns related to the cloud. Taking into consideration the amounts of data and services corporations and the government are storing on the cloud, it is imperative that best practices for forensic analysis are developed for potential investigations in the future. Grispos et al. (2013) demonstrate the importance of auditing policies, standards and guidelines applicable to cloud computing environments along with highlighting potential corporate concerns.

Daryabar et al. (2013) identified multiple themes in prior studies but some of the most highly investigated were cloud service provider (CSP), digital forensic concept, security/privacy risk, and cloud computing security. These findings raise some concerns that researchers are not paying enough attention to the field of forensic investigations on the cloud from a legal standpoint. While this need may not be fully realized yet, with the fast-changing technologies and advances in the field of cybercrime, we are going to see very soon a rapid demand in both practitioner and regulatory areas.

RECOMMENDATIONS FOR IMPROVEMENT

While there are many issues and concerns related to the digital forensics process on the cloud, there are certain steps that can be taken to improve it and to better preserve the integrity of the evidence. Even though technology may be available, there has to be appropriate legislature to

[5] http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf, accessed on 10/1/18

provide better guidance to investigators when they deal with the complex issues of this new and emerging field. For instance, when Mark Zuckerberg, the CEO of Facebook, testified in front of Congress earlier this year[6], it was evident that the policy makers were not ready or able to make any significant legislative changes to how technology is regulated[7]. There are many possible reasons for this, including lack of agreement among the Democrats and the Republicans. However, it is also interesting to note that the average age of a Representative is 57 and the average age of a Senator is 61, which is almost 20 years older than the average American[8]. Such a significant age gap can potentially hurt the people as policy makers belong to a different generation and they may not have a good understanding of how technology works and may potentially miss to address important points. There is a concerning trend that members are older and older with each Congress and while this may be an advantage in many aspects, from a technological standpoint it is often a drawback as younger generations are practically raised with technology these days and it is much more intuitive for them (Helsper and Eynon 2010; Zickuhr 2011).

While it may not be easy or feasible to simply replace Congress members with a younger generation, a possible improvement could be to have their staff members more involved in the policy development process and to make sure that these individuals are more tech savvy and understand the complications of the digital forensics process, especially when it is involving data and systems hosted on the cloud. Also, experts can be hired to provide input and advise Congress members on such important issues.

[6] https://qz.com/1251646/what-we-learned-from-mark-zuckerbergs-congressional-testimony/, accessed on 10/1/18
[7] https://qz.com/1089907/why-washington-dc-is-incapable-of-regulating-the-worlds-tech-giants/, accessed on 10/1/18
[8] https://www.quorum.us/data-driven-insights/the-115th-congress-is-among-the-oldest-in-history/175/, accessed on 10/1/18

If there is more publicity about the technical and policy issues regarding digital forensics on the cloud, this can lead to a more public debates and can draw the attention to the severity of the problem. Currently, because of its complex nature and insufficient visibility in the media, the lack of regulations seems to be severely underestimated. Digital forensics alone are challenging enough because of the ever-changing technologies involved. Adding to that the multi tenancy, multi jurisdictions, and dynamically changing data and systems makes this even more complicated. However, if more light is shed on the problem, this can put pressure on policy makers to develop new regulations that reflect the current state of technology integration in our lives.

Best practices on how to conduct digital forensic investigations already exist and they have been created by law enforcement agencies all over the world. A good first step in the right direction could be to modify those and make them relevant to the use of CSPs. In addition, terms of use and contracts corporations and end-users sign should be revised to reflect the potential need to audit CSPs and their mechanisms for provisioning data on the cloud.

RESEARCH QUESTION

The current paper aims to answer the research question: "What are the challenges and barriers to digital forensics in the cloud?" by first investigating the cloud computing phenomenon and its implications for practice. Second, it looks at the digital forensics process to provide a better understanding of how evidence gathering, and analysis can occur in a digitized world. Third, the study will examine the obstacles associated with forensic investigations on the cloud. And finally, some recommendations will be provided as to how these challenges and barriers can be overcome and what directions can future researchers take to aid policy makers in keeping up with the advancements in technology.

CONCLUSION

The cloud provides many benefits that were for individuals and businesses that were not even imaginable twenty years ago. The lower costs, high resiliency, and ease of use make it a desirable tool and an integral part of our lives these days. However, with the rapid change of technology also come the challenges that we couldn't even imagine before. Some of those include conducting forensic investigations involving data and systems stored on the cloud. Policy makers need to provide a more adequate reaction to the changing reality of technology in the 21st century and support the efforts of law enforcement officers who are dealing with these complex issues daily. As a society, we can and should do more to request policy makers to take this problem seriously and to provide better protection for all of us using cloud services. Cybercrimes are the new way for criminals to terrorize our society and we need to do more to overcome the technological and legal issues associated with digital forensic investigations on the cloud.

REFERENCES

Daryabar, F., Dehghantanha, A., and Udzir, N. I. 2013. "A Review on Impacts of Cloud Computing on Digital Forensics," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)* (2:2), pp. 77-94.

Grispos, G., Glisson, W. B., and Storer, T. 2013. "Cloud Security Challenges: Investigating Policies, Standards, and Guidelines in a Fortune 500 Organization," in: *21st European Conference on Information Systems*. Utrecht, The Netherlands.

Grispos, G., Storer, T., and Glisson, W. B. 2012. "Calm before the Storm: The Challenges of Cloud Computing in Digital Forensics," *International Journal of Digital Crime and Forensics (IJDCF)* (4:2), pp. 28-48.

Helsper, E. J., and Eynon, R. 2010. "Digital Natives: Where Is the Evidence?," *British educational research journal* (36:3), pp. 503-520.

Kaufman, L. M. 2010. "Can a Trusted Environment Provide Security?," *IEEE Security & Privacy* (8:1).

Khan, K. M., and Malluhi, Q. 2010. "Establishing Trust in Cloud Computing," *IT professional* (12:5), pp. 20-27.

Modi, C., Patel, D., Borisaniya, B., Patel, A., and Rajarajan, M. 2013. "A Survey on Security Issues and Solutions at Different Layers of Cloud Computing," *The journal of supercomputing* (63:2), pp. 561-592.

Nance, K., and Ryan, D. J. 2011. "Legal Aspects of Digital Forensics: A Research Agenda," *System Sciences (HICSS), 2011 44th Hawaii International Conference on*: IEEE, pp. 1-6.

Ruan, K., Carthy, J., Kechadi, T., and Crosbie, M. 2011. "Cloud Forensics," in *Advances in Digital Forensics Vii*. Springer, pp. 35-46.

Winn, P. 2009. "Katz and the Origins of the Reasonable Expectation of Privacy Test," *McGeorge L. Rev.* (40), p. 1.

Zickuhr, K. 2011. "Generations and Their Gadgets," *Pew Internet & American Life Project* (20).