Chapter 26
Designing a Forensic-Enabling Cloud Ecosystem

Keyun Ruan
University College Dublin, Ireland

ABSTRACT

Cloud computing is a major transition, and it comes at a unique historical and strategic time for applying foundational design thinking to secure the next-generation computing infrastructure and enable waves of business and technological innovation. In this chapter, the researcher summarizes six key research and development areas for designing a forensic-enabling cloud ecosystem, including architecture and matrix, standardization and strategy, evidence segregation, security and forensic integration, legal framework, and privacy.

INTRODUCTION

Cloud computing is like a supercomputer split among cloud actors connected and delivered via networks. The split of technical infrastructure as an evolutionary computing service delivery model provides massive cost reduction and increases resource utilization. The split among cloud actors, on the other hand, requires new interfaces, trust and transparency, as well as legal framework to ensure smooth and secure service delivery with clearly defined segregation of duties for all cloud actors to implement relevant technical, organizational, and legal controls and mechanisms. Foundational thinking for designing standards, system architecture, and research roadmaps are needed at the current stage of cloud development. In this chapter, the researcher discusses the importance and strategies for designing a forensic-enabling cloud ecosystem.

With the ever-rising cyber crime and the rapid emergence of cloud computing, digital investigations are faced with significant challenges. While data are being migrated to cloud computing environments, so does digital evidence. In 2011, hackers rented Amazon servers and triggered the second-largest online data breach in U.S. history (Galante, et al., 2011). Cases as such cannot be handled by traditional digital forensic tools and procedures due to cloud forensic challenges outlined by pioneering researchers in Spyridopoulos and Katos (2011), Birk and Wegener (2011), Biggs and Vidalis (2009), Ruan et al. (2011a). At the meantime, global cybercrime is growing

DOI: 10.4018/978-1-4666-6539-2.ch026

at an astonishing rate causing devastating financial losses. Annual loss caused by cyber crime in Europe alone is estimated to be 750 billion Euros (Cheslow, 2012). Designing a forensic-enabling cloud ecosystem is thus of high importance in order to prevent explosive growth of cybercrime in cloud environments due to lack of forensic considerations during cloud adoption.

The Information Society Alliance published a report (ISA, 2010), and it argues that the solution to current cyber security challenge is a fundamental change in market behavior so that the complex IT systems, on which society increasingly depends, have security embedded from the start rather than added as an afterthought. This did not happen in the history of the computer era. Even though John von Neumann designed the first theoretical computer virus (Neumann, 1949), he did not include security design in his own computer architecture known as the von Neumann Architecture (Neumann, 1945). Gartner (2012) estimates that personal cloud will replace personal computer by 2014, however, study shows security still is an afterthought during cloud adoption (Ernst & Young, 2011). Compare to security, forensic implementations have been an "after-after-thought." Anderson et al. (2012) carried out a research aimed to scientifically estimate the cost of cyber crime, and it concludes that "we should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response, i.e., the prosaic business of hunting down cyber criminals and throwing them in jail." The good news is that cloud computing is still at early stage of development and it is expected to reach maturity in another 10 years (Thomason, 2010, CSA & ISACA, 2012). According to CIO and CAOC (2012), cloud computing represents a paradigm shift that is larger than IT. This new paradigm requires agencies to re-think not only the way they acquire IT services in the context of deployment, but also how the IT services they consume provide mission and support functions on a shared basis. Researcher believes that now is a historically unique timing for including security and forensic implementations by design into cloud architecture iterations, and it might not be too late to change the game.

The cost of litigation and investigation in a cloud ecosystem without forensics by design can be very high. For example, the court in *In Re Fannie Mae Securities*, held an agency in contempt for failing to meet discovery deadlines even though the agency had already spent 6 million USD (9% of its total budget) on discovery. Using e-discovery tools to streamline search, collection, and processing could help Federal agencies avoid great cost in litigations, congressional requests, investigation, and other types of data requites. Federal agencies should inquire if there is an option or offering for e-discovery capabilities as part of the cloud service provided. If the right e-discovery functionality and tools are incorporated into an agency's CSP environment, there may be a potential for additional and significant cost avoidance and IT efficiencies (CIO & CAOC, 2012).

In this chapter, six strategic areas and directions for designing a forensic-enabling cloud ecosystem are discussed as follows:

1. **Architecture/matrix:** The need for cloud forensic reference architecture and control matrix
2. **Standardization/strategy:** The need for considering forensic aspects in cloud standardization efforts as well as national cloud strategies
3. **Evidence segregation:** The need for designing a data segregation strategy for multi-tenant cloud ecosystem enabled by virtualization technologies
4. **Security and forensics integration:** The need for further integrating forensic design into security architectures
5. **Legal framework:** The need for designing a legal framework to secure cross-border data transfer and facilitate international collaboration on digital investigations

Evolution of Fog Computing Applications, Opportunities, and Challenges: A Systematic Review
Hewan Shrestha, Puviyarai T., Sana Sodanapalliand Chandramohan Dhasarathan (2021). *International Journal of Fog Computing (pp. 1-17).*
www.irma-international.org/article/evolution-of-fog-computing-applications-opportunities-and-challenges/284861