Cloud computing and digital forensics

Concerns about evidence in cloud environments have expanded over the years as this technology has become more widely used.

Criminals use cloud computing in various ways, including to store incriminating evidence, launch attacks, and crack encryption keys. To cover their tracks, criminals can de-provision their cloud-based haven and let it dissolve into the ether.

Organizations are becoming more reliant on cloud computing to process and store data, including credit card transactions and other sensitive information. When cyber criminals target these potentially valuable online resources, digital investigators are faced with the challenge of acquiring associated evidence in the cloud.

However, it is important to realize that many aspects of digital investigation remain unchanged in a cloud environment, despite the new terminology and technology. In addition, cloud computing creates significant opportunities to support digital forensics, providing useful evidence in digital investigations and enhancing our forensic processing capabilities.

1. Cloudy evidence

Concerns regarding evidence in cloud environments include potential lack of information, inaccessibility of data, and uncertain provenance of evidence. Cloud systems are rarely designed with digital forensics or evidence integrity in mind. As a result, digital evidence may not be available on these systems or it may not be possible to verify the integrity of available evidence on these systems.

These concerns are not new. These same concerns have existed since the earliest digital investigations. In fact, the same concerns exist in other forensic disciplines. Crime scenes are not designed to make forensic analysis easy. Many things can occur to change, relocate, obscure, or obliterate evidence, including emergency response efforts and the weather. The term “evidence dynamics” is used to describe many of these issues.

As a point of reference, since the 1990’s, network intrusion and data breach investigations have dealt with many of the issues that are cause for concern in cloud environments. From the outset of a network intrusion investigation, the full extent of the damage is unknown, making it necessary to perform a scope assessment that is similar to the iterative aspect of the framework for cloud computing proposed by Martini et al. in this issue of the Journal (see “An integrated conceptual digital forensic framework for cloud computing”). The main purpose of the scope assessment cycle is to guide the digital investigator through the collection and analysis of data, and then push the results into the search for additional affected devices. This scope assessment cycle is repeated until no new evidence related to the intrusion is discovered.

Furthermore, when investigating a network intrusion, it is common for the victim organization to be unprepared, and it is rarely feasible to shut down the entire network in order to preserve the digital crime scene. As a result, useful evidence may no longer be available, may be difficult to collect, may be entirely out of reach, or may not have been preserved in a forensically sound manner. For example, various types of logs can be invaluable in a network intrusion investigation, but many organizations do not collect such logs or do not retain logs for more than a few days, or do not store logs in a way that ensures their integrity. As another example, during network intrusion investigations, it is not uncommon to encounter compromised systems running in virtualized environments and utilizing network-based storage, making it necessary for digital investigators to apply forensic principles in a new context in order to preserve evidence.

Digital investigators cannot expect digital crime scenes to be designed in their favor. Even in the ideal situation where an organization has prepared their systems from a forensic perspective, novel situations will arise and evidence dynamics will still exist. Ultimately, digital investigators have to be resourceful in order to obtain and make use of whatever information is available. A solid understanding of forensic principles and how they can be applied in new contexts is one of the most important capabilities that a digital investigator can possess.

2. Enhancing capabilities

Over the years, forensic methods and tools have been developed to support the investigation of network intrusions and other offenses involving distributed systems. These capabilities include remote forensic techniques, network forensic tools, memory forensic methods, and database forensic approaches. New research and
development in all of these areas, including the papers in this issue and upcoming issues of the Journal, improve our ability to handle digital evidence in cloud environments.

Forensic analysis of traces left by cloud storage services on computers and smartphones are detailed by Chung et al. (see “Digital forensic investigation of cloud storage services”), providing a wealth of information and practical methods to support digital investigations.

Smartphones make extensive use of cloud services, and recovery of data from these devices is an important digital forensic capability as detailed by Park et al. (see “Forensic analysis techniques for fragmented flash memory pages in smartphones”).

Deeper insight into memory forensics is provided by Vömel & Freiling (see “Correctness, atomicity, and integrity: Defining criteria for forensically-sound memory acquisition”) and by Saleh & Al-Sharif (see “Utilizing data lifetime of TCP buffers in digital forensics”). Such enhancements in memory forensics can benefit a wide range of digital investigations, including those involving virtualized systems in a cloud environment.

A reliable approach to reconstructing digital evidence stored in databases is presented by Fasan and Olivier (see “Correctness proof for database reconstruction algorithm”). This is an important topic since more evidence is stored in databases, including in cloud environments.

Improved methods for detecting tampering or hidden information in digital evidence are becoming more important for digital forensics, particularly when limited information about provenance is available as is sometimes the case in cloud environments. A novel approach to detecting tampering in digital video is described by Dong et al. (see “A MCEA based passive forensics scheme for detecting frame-based video tampering”). A new method for detecting hidden data is proposed by Quach (see “Locating payload embedded by group-parity steganography”).

These papers raise the bar in digital forensics, and demonstrate the value of research and development in a wide range of domains to support digital investigations.

3. Silver lining

As the saying goes, every cloud has a silver lining. For digital forensics the positive aspect of cloud computing is the potential to scale our automated forensic processes to handle larger datasets.

As our shared understanding of evidence sources grows, the complexity and costs associated with performing digital forensic examination in a consistent manner is increasing. These challenges are exacerbated by mounting caseloads and larger quantities of data.

Some digital forensic laboratories are developing comprehensive automation systems to extract information from many common sources of evidence on various digital devices, and provide digital investigators with deeper insight into available evidence in a shorter time. For example, the XIRAF system described by Bhoedjang et al. (see “Engineering an online computer forensic service”) in this issue of the Journal has matured into a powerful forensic platform and is currently being redesigned to take advantage of cloud computing.

This use of cloud computing can increase the efficiency and consistency of automated forensic processes, providing digital investigators with a more comprehensive view of available information in a case. As a result, digital investigators can concentrate their efforts and expertise on utilizing the evidence to address the primary questions in a case.

4. Conclusion

Although cloud computing presents technical, logistical and legal challenges for digital investigators, we have overcome similar challenges in the past. Research and development is necessary to address emerging challenges in digital forensics, and we must redouble our efforts and investment in this area to keep pace with new technology. By taking advantage of the opportunities that cloud computing creates, digital investigators can make this technology the foundation of success in digital forensics, both as a major source of evidence and as a powerful platform to support forensic processes.

Eoghan Casey
Johns Hopkins University Information Security Institute,
216 Maryland Hall, Baltimore, MD 21218, United States
E-mail address: eoghan@jhu.edu