Forensics investigation challenges in cloud computing environments

ABSTRACT

Cloud computing discusses about sharing any imaginable entity such as process units, storage devices or software. The provided service is utterly economical and expandable. Cloud computing attractive benefits entice huge interest of both business owners and cyber thefts. Consequently, the ñcomputer forensic investigationò step into the play to find evidences against criminals. As a result of the new technology and methods used in cloud computing, the forensic investigation techniques face different types of issues while inspecting the case. The most profound challenges are difficulties to deal with different rulings obliged on variety of data saved in different locations, limited access to obtain evidences from cloud and even the issue of seizing the physical evidence for the sake of integrity validation or evidence presentation. This paper suggests a simple yet very useful solution to conquer the aforementioned issues in forensic investigation of cloud systems. Utilizing TPM in hypervisor, implementing multi-factor authentication and updating the cloud service provider policy to provide persistent storage devices are some of the recommended solutions. Utilizing the proposed solutions, the cloud service will be compatible to the current digital forensic investigation practices; alongside it brings the great advantage of being investigable and consequently the trust of the client.

Keyword: Cloud computing; Forensics investigation; Security; Virtualization; Forensic challenges