Cloud computing and conflicts with digital forensic investigation

ABSTRACT

Unfortunately, the nature of the cloud is in conflict with the characteristic of digital forensic investigation approach since many of the common forensic steps are not possible to follow during the inspection of the case. The distribution of cloud resource location in different countries, utilization of numerous storage devices and very limited physical access to the low-level storage devices and physical memories are just some of the reasons caused this conflict. This paper proposes some basic, yet useful, solutions to conquer the described issues. Implementing multi-factor authentication, utilizing Trusted Platform Module (TPM) in Hypervisor and applying specific changes in the Cloud Service Provider (CSP) contract to provide persistent storage to the customer are parts of suggested approaches, capable of making the current digital forensic investigation practices applicable to the cloud computing environments. This is an absolutely essential requirement for CSP's mainly due to the significance of the clients' trust which demands the ability for being investigated.

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