Cloud Forensics : Isolating Cloud Instance

Mariam J. AlKandari, Huda F. AlRasheedi
& Ayed A. Salman
Computer Engineering Department
Kuwait University
Kuwait City, Kuwait
mariamalkandari@gmail.com, eng.hudaalrasheedi@gmail.com,
ayed.salman@ku.edu.kw

***Abstract*—Cloud computing has been the trending model for storing, accessing and modifying the data over the Internet in the recent years. Rising use of the cloud has generated a new concept related to the cloud which is cloud forensics. Cloud forensics can be defined as investigating for evidence over the cloud, so it can be viewed as a combination of both cloud computing and digital forensics. Many issues of applying forensics in the cloud have been addressed. Isolating the location of the incident has become an essential part of forensic process. This is done to ensure that evidence will not be modified or changed. Isolating an instant in the cloud computing has become even more challenging, due to the nature of the cloud environment. In the cloud, the same storage or virtual machine have been used by many users. Hence, the evidence is most likely will be overwritten and lost. The proposed solution in this paper is to isolate a cloud instance. This can be achieved by marking the instant that reside in the servers as "Under Investigation". To do so, cloud file system must be studied. One of the well-known file systems used in the cloud is Apache Hadoop Distributed File System (HDFS). Thus, in this paper the methodology used for isolating a cloud instance would be based on the HDFS architecture.**

***Keywords:* cloud computing; digital forensics; cloud forensics**

IRJECE