Abstract

The decline in traditional forensics and the emergence of cloud forensics has made it hard for digital forensic investigators to conduct digital investigations due to inadaptability of the cloud to digital forensic processes. Additionally, data that resides in the cloud is normally scattered across constantly changing data centers, hosts and virtual instances are easily destroyed as they are created. On the same note it is not easy to seize physical devices where a particular crime has occurred and locating the origin of an object in the cloud can be a challenge when we do not know where the actual data resides. Data provenance provides a solution whereby one can trace data based on the tag as it keeps changing directions in the cloud. However, if the distance between two particular tagged data is taken into account then the source and destination of an object can be located easily which can then enable digital forensic investigators to locate the physical devices. The problem that this paper is addressing is that, there is no easy way of locating data provenance in the cloud environment without estimating the distance between tagged data that moves in the cloud. Based on this, the authors have proposed a mechanism for locating the provenance of an object using successive bisection method.
method. Similar tests have been carried using different intervals in an experiment and the results are very promising.

References

An Approach for Estimating Forensic Data Provenance of an Object in the Cloud Environment using One Dimensional Successive Bisection Method using Artificial Immune System in the cloud. In Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2014 Third International Conference on (pp. 52-57). IEEE.


Index Terms
Computer Science Information Sciences

Keywords
Forensic, data, provenance, object, cloud, bisection method