Cloud Computing, a relatively new concept and all its associated methodologies offer uncountable advantages now-a-days. These advantages range from integrating different systems, offering guarantee over searching mean distribution and to software tools integration, used by various cloud service providers and consumers. So all these provisions are not only making our lives easier but attract lots of intruders and malicious actors to perform various cloud crimes. This paper aims to contribute towards the design of an ontology based cloud forensic framework with a view to identify the malicious actors. The proposed framework consists of mainly two components - Ontology-Enabled Forensic Blackboard (OFB) and Ontology-Enabled Forensic Controller and Processor (OFCP). The main function of OFB is to communicate with the investigators after receiving the classified crime incident scene collected from VM snapshots where ontology base is used spontaneously to distribute the investigators' request for proper information relevant to the investigation. Whereas, the function of the OFCP is to interact with different Cloud Malicious Actor Identifier (CMAI) so that accurate information can be gathered based on the distributed request with the help of a meta-ontology framework that acquire and
restructure data using different AI reasoning tools and finally the mapping with its corresponding requests is done.

References


Index Terms

Computer Science  Distributed Systems

Keywords

Digital forensics; cloud computing; cloud forensics; SaaS; PaaS; IaaS; virtualization; Ontology; OWL; Protégé;