Abstract

The study proposes a cloud security framework for Cloud Service Providers (CSPs) in Ghana. It adopted a number of strategies, such as experimental research achieved through integrated simulation and mixed mode research method approach, using SPSS for data analysis to execute the study expectations of proposing a new cloud security framework. It also carried out an investigation into cloud security deployment technologies, and then undertook a comparative study of these technologies.

In addition, it also investigated whether or not CSPs in Ghana follow any cloud security policy guidelines to deliver cloud services in Ghana. An experimental research approach adopted an Open AM server for the purpose of achieving integrity and secure authorization in the proposed framework which employed XACML Version 3.0 to define and enforce policies. Tools such as, Cygwin, curl/libcurl, Scala and IntelliJ IDEA IDE were used together to enhance simulation in the study. The results from analysis revealed that, HSM, OTFE and other cloud based security
systems are the major security technologies deployed by service providers for integrity and authorization. Two curl HTTP/1.1 GET request were made at the service application endpoint where the access controller is wrapped over. Based on the rule set, two basic users were allowed and disallowed when accessing a cloud resource. A basic resource of an application with HTTP gave a status and a security token. To maintain the integrity of cloud data, the study recommends a root hardware TPM Chip be adopted to ensure maximum application security and systems performance. The proposed security framework assures cloud data integrity and also ensures authorization. The study therefore also recommends XACML V3.0 to be adopted as a language for cloud systems for policy definition and enforcement.

References


Index Terms

Computer Science  Security

Keywords