Open Science Index, Computer and Information Engineering Vol:8, No:05, 2014 publications.waset.org/abstracts/8920.pdf

Data Confidentiality in Public Cloud: A Method for Inclusion of ID-PKC Schemes in OpenStack Cloud

Authors : N. Nalini, Bhanu Prakash Gopularam

Abstract : The term data security refers to the degree of resistance or protection given to information from unintended or unauthorized access. The core principles of information security are the confidentiality, integrity and availability, also referred as CIA triad. Cloud computing services are classified as SaaS, IaaS and PaaS services. With cloud adoption the confidential enterprise data are moved from organization premises to untrusted public network and due to this the attack surface has increased manifold. Several cloud computing platforms like OpenStack, Eucalyptus, Amazon EC2 offer users to build and configure public, hybrid and private clouds. While the traditional encryption based on PKI infrastructure still works in cloud scenario, the management of public-private keys and trust certificates is difficult. The Identity based Public Key Cryptography (also referred as ID-PKC) overcomes this problem by using publicly identifiable information for generating the keys and works well with decentralized systems. The users can exchange information securely without having to manage any trust information. Another advantage is that access control (role based access control policy) information can be embedded into data unlike in PKI where it is handled by separate component or system. In OpenStack cloud platform the keystone service acts as identity service for authentication and authorization and has support for public key infrastructure for auto services. In this paper, we explain OpenStack security architecture and evaluate the PKI infrastructure piece for data confidentiality. We provide method to integrate ID-PKC schemes for securing data while in transit and stored and explain the key measures for safe guarding data against security attacks. The proposed approach uses JPBC crypto library for key-pair generation based on IEEE P1636.3 standard and secure communication to other cloud services.

Keywords : data confidentiality, identity based cryptography, secure communication, open stack key stone, token scoping
Conference Title : ICEIT 2014 : International Conference on Education and Information Technology
Conference Location : Montreal, Canada
Conference Dates : May 12-13, 2014