Abstract

Cloud computing provides way to share information. This information is secured at cloud ends only. Any third party intruder may hack confidential information. While outsourcing its business-critical data and computations to the cloud, an enterprise loses control over them. How should the organization decide what security measures to apply to protect its data and computations that have different security requirements from a Cloud Service Provider (CSP) with an unknown level of corruption? The answer relies on the organization's perception about the CSP's trustworthiness and the security requirements of its data. This paper proposes a decentralized, dynamic and evolving policy-based security framework that helps an
organization to derive such perceptions from knowledgeable and trusted employee roles and based on that, choose the most relevant security policy specifying the security measures necessary for outsourcing data and computations to the cloud.

References


Index Terms

Computer Science

Distributed System

Keywords
<table>
<thead>
<tr>
<th>Service Provider</th>
<th>Csp Credentials</th>
<th>Encryption</th>
<th>Decryption</th>
</tr>
</thead>
</table>