Abstract

Although the security Outsourcing companies can provide several security services to its customer organizations, but the customer organizations should avoid Outsourcing security risks which emerge from providing security services to the customers through open environments or malicious behaviors which the security providers at Outsourcing companies may carry out. For this problem we propose a new methodology represented in a security design model which combine Cryptography and Access Control techniques to prevent the external security providers of an Outsourcing company to access the sensitive data assets of the customer organizations. We could achieve the realism of this methodology through a proposed algorithm in MATLAP Language. Using our new access control model, the customer organizations can control and manage the external access rights of security providers of specific Outsourcing Company which the customer organization communicated with it.
Index Terms
Keywords

Outsourcing  Security Providers  Encryption /Decryption  access control  Two layer encryption model
access policy changes
AES algorithm
MATLAP Language