Secure and Privacy Enhanced Authentication & Authorization in Cloud

By

Umer Khalid

2011-NUST-MS-CCS-35

Thesis Supervisor

Dr. Abdul Ghafoor

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree
Of Masters of Science in Computer and Communication Security (MS CCS)

In

Department of Computing (DoC)
School of Electrical Engineering & Computer Science (SEECS)
National University of Sciences & Technology (NUST),
Islamabad, Pakistan

(2014)

Abstract.

Cloud computing is a general purpose technology that greatly impacts business owners and organizations in terms of energy, cost and efficiency. However, organizations are reluctant about shifting sensitive information such as identity credentials over the cloud environment. Up till now, legacy security standards have been used by organizations for the protection of resources which pose unique threats like identity theft and privacy leaks due to the use of Personally Identifiable Information (PII) during the exchange of authentication and authorization messages.

This research provides the design and implementation of an anonymous authentication and authorization protocol as a solution to these problems. The solution consists of carefully selected components such as, FIPS 196 for a proven and robust authentication mechanism, whereas, XACML based Policy Enforcement Point (PEP) for authorization. An identity management system (IDMS) is chosen in order to maintain a record of the registered users. For anonymity, the designed protocol uses traceable anonymous certificates (TAC's) instead of simple public key certificates generated using anonymous identities (AID). A client side application passes these certificates as initial parameters for authentication to a strong authentication server (SA server). Certificates are modified further such that they do not leak any Personal Identifiable Information (PII) about the users. Authorization is provided using standard XACML based access control policies which are binded to the anonymous identities of the registered users instead of real identities. Hence using this protocol, threats such as identity theft and leakage can be mitigated with minimal changes to existing setups. In order to validate the designed protocol, Scyther is used. After validation, it is verified that our security protocol resists against man-in-the-middle, replay and attacks on confidentiality of user's credentials.