Summer 8-1-2020

DEVELOPMENT OF SECURE CLOUD SERVICES FOR STORING AND ACCESSING DATA IN ROLE BASED ACCESS CONTROL APPLICATIONS

K. RAJESH RAO

Abstract

Security risks are relatively high in the public cloud because users have less control over the deployed sensitive data. Hence, cloud providers offer various security services with the help of mechanisms such as data encryption, identity and access management. Secure cloud services for data storage is not concerned much with data residency protection, data storing, and data accessing in access control applications. So, this thesis investigates cloud security related problems in storing and accessing data in role based access control applications. It is intended to provide security mechanisms that can be hosted by the service provider to protect the data.

The first proposed framework known as *Data Resident Storage* considers data security together with compliance. It addresses data residency issues related to data location, extraterritorial access, multi-jurisdiction laws, and data access. The second mechanism is based on a string search in an encrypted domain, where an arbitrary group of users can search and access encrypted files depending upon roles known as *R-PEKS* scheme, i.e., Role enabled Public-Key Encryption with Keyword Search. Unlike previous constructions, this scheme is free from bi-linear mapping and is relevant for commercial applications involving a large group of users with role based access structure. Further, the scheme is proven to be secure under the definition of adaptive security and performs better in a timely manner during encryption and search. The third approach optimizes user-role assignments in access management applications with the introduction of a role recommendation model for role based access control system known as *Role Recommender-RBAC*. This system optimizes user-role assignments at the user-level to satisfy the least privilege principle, unlike the existing models which optimize user-role assignments at the system level. Further, the system proves to be secure while accessing data and performs better during optimization.

Finally, security services are developed based on the above mechanisms to protect the data in cloud applications. The Data Resident Storage mechanism helps cloud vendors to provide security service as "Data-Residency-as-a-Service", which preserves data privacy and confidentiality in the cloud environment. The R-PEKS scheme helps the cloud vendors to provide security service as "Searchable-Encryption-as-a-Service" in role based access control applications, which preserves data privacy and confidentiality. Finally, the Role Recommender-RBAC system helps cloud vendors to provide security service as "Role-Assignment-as-a-Service" in role based access control applications, which preserves data confidentiality during access.

Keywords- Cloud security service, Data confidentiality, Data privacy, Public key Encryption with Keyword Search, Role Based Access Control.