SecRBAC: Secure data in the Clouds

Aim:

The aim of this project is to protect user data from the Cloud service provider that holds it.

Objective:

- To protect the data from CSP.
- To implement authorization rules under the control of data owners.

Abstract:

This paper presents a data-centric access control solution with enriched role-based expressiveness in which security is focused on protecting user data regardless the Cloud service provider that holds it. Novel identity-based and proxy re-encryption techniques are used to protect the authorization model. Data is encrypted and authorization rules are cryptographically protected to preserve user data against the service provider access or misbehavior. The authorization model provides high expressiveness with role hierarchy and resource hierarchy support. The solution takes advantage of the logic formalism provided by Semantic Web technologies, which enables advanced rule management like semantic conflict detection. A proof of concept implementation has been developed and a working prototypical deployment of the proposal has been integrated within Google services.

Introduction:

Security is one of the main user concerns for the adoption of Cloud computing. Moving data to the Cloud usually implies relying on the Cloud Service Provider (CSP) for data protection. Although this is usually managed based on legal or Service Level Agreements (SLA), the CSP could potentially access the data or even provide it to third parties. Moreover, one should trust the CSP to legitimately apply the access control rules defined by the data owner for other users.. Users may loss control on their data. This situation leads to rethink about data security approaches and to

move to a data-centric approach where data are self-protected whenever they reside. Encryption is the most widely used method to protect data in the Cloud. There is no data-centric approach providing a Role-based Access Control (RBAC) model for access control in which data is encrypted and self-protected. The proposal in this paper supposes a first solution for a data centric RBAC approach, offering an alternative to the ABAC model. An RBAC approach would be closer to current access control methods, resulting more natural to apply for access control enforcement than ABE-based mechanisms. In terms of expressiveness, it is said that ABAC supersedes RBAC since roles can be represented as attributes. However, when it comes to data-centric approaches in which data is encrypted, ABAC solutions are constrained by the expressiveness of ABE schemes. The cryptographic operations used in ABE usually restrict the level of expressiveness for access control rules.

A data-centric approach is used for data self-protection, where novel cryptographic techniques such as Proxy Re-Encryption Encryption (PRE), Identity-Based Encryption (IBE) and Identity-Based Proxy Re-Encryption (IBPRE) are used. They allow to re-encrypt data from one key to another without getting access and to use identities in cryptographic operations. These techniques are used to protect both the data and the authorization model. Each piece of data is ciphered with its own encryption key linked to the authorization model and rules are cryptographically protected to preserve data against the service provider access or misbehavior when evaluating the rules. It also combines a user-centric approach for authorization rules, where the data owner can define a unified access control policy for his data. The solution enables a rule-based approach for authorization in Cloud systems where rules are under control of the data owner and access control computation is delegated to the CSP, but making it unable to grant access to unauthorize parties.