Effective C-RBAC Framework Based on Role Provisioning for Data Protection in Business Application Systems

M. Auxilia[1], K. Raja[2] and K. Kannan[3]

[1] *Department of CSE, Sathyabama Institute of Science and Technology, Chennai, India*
[2]*Department of CSE, Dhaanish Ahmed College of Engineering, Chennai, India*
[3]*Department of IT, Adhiparasakthi College of Engineering, Kalavai, India*

Security plays a key role in any business organization for the purpose of information sharing and privacy. However, there is a lack of privacy and safety among the information. Business data and organizational data are considered to be the highly sensitive data because of the impact that may result in the business process. The employees of any organization are the real assets for their concern and it's the responsibility of the organization should have a clear vision about the activity of all the employees under legal business development. In this article, new RBAC (Role Based Access Control) framework is developed to navigate the process for a particular employee and their services in any business organization. RBAC framework is especially developed to provide security based on role provisioning during information sharing. AgZKPk (Aggregate Zero Knowledge Proof knowledge) and OCBE (Oblivious Commitment Based Envelope) Protocols are used for role enrollment for RBAC concept (condition policies). In this paper, C-RBAC (Cloud– Role Based Access Control) framework is proposed which can fit in any business organization application. In this C-RBAC, PEP (Policy Enforcement Point) is used to avoid unwanted information sharing with the neighbouring employee or peers. The analysis is done based on the security level for several security algorithms in C-RBAC framework. C-RBAC framework with RSA provide well security based on number of employee with the data handled by the particular employee than the existing RBAC framework with AES (Asymmetric Encryption Standard) and RSA (Rivest–Shamir–Adleman) in terms of number of information they can handle per user. Our analysis revels few threats that arise due to sharing of data and violation in agreements. Also, it is inferred that by adopting our proposed framework, we can avoid data leaks and can protect the data even within the organization.

Keywords: Aggregate zero-knowledge proof knowledge, Oblivious commitment based Envelope, Policy enforcement point, Role based access control