Abstract No: SC-28 **Smart Computing**

Improved hierarchical role based access control model for cloud computing

***N. N. Thilakarathne and Dilani Wickramaaarachchi**

Department of Industrial Management,
Faculty of Science, University of Kelaniya, Sri Lanka
**Neranjanthi@gmail.com*

Abstract

Cloud computing is considered as the one of the most dominant paradigms in the field of information technology which offers on demand cost effective services such as Software as a Service (SAAS), Infrastructure as a Service (IAAS) and Platform as a Service (PAAS). Promising all these services as it is, this cloud computing paradigm still associates number of challenges such as data security, abuse of cloud services, malicious insider and cyber-attacks. Among all these security requirements of cloud computing access control is the one of the fundamental requirement in order to avoid unauthorized access to a system and organizational assets. Main purpose of this research is to review the existing methods of cloud access control models and their variants pros and cons and to identify further related research directions for developing an improved access control model for public cloud data storage. The paper presents detailed access control requirement analysis for cloud computing and have identified important gaps, which are not fulfilled by conventional access control models. As the outcome of the study an improved access control model with hybrid cryptographic schema and hybrid cloud architecture and practical implementation is proposed. The study tested the model for security implications, performance, functionality and data integrity to prove the validity. It used AES and RSA cryptographic algorithms to implement the cryptographic schema and used public and private cloud to enforce our access control security and reliability. By validating and testing we have proved that the model can withstand against most of the cyber-attacks in real cloud environment. Hence, it has improved capabilities compared with other previous access control models that we have reviewed through literature.

Keywords: Hybrid cloud, Hybrid cryptographic schema, Public cloud data storage,

Introduction

Cloud is one of the major and dominate technologies, which paved the way for digital transformation across the globe. It is a model for providing convenient on demand network access for computing resources such as applications, services, servers and storages that can be rapidly provisioned and released with minimal management effort or service provider interaction (Bibin, 2013). Cloud has lot of advantages mainly in ubiquitous services where everybody can access computer services through internet. This cloud model composed of three service delivery models mainly SAAS, PAAS, and IAAS. Depending on the type of data that you are working with, cloud computing come in three forms. Public cloud, Private cloud and the Hybrid cloud. Along with the rapid steady development of the cloud applications cloud computing cyberattacks are also increased and cloud itself create a good attacking surface for hackers. (Faisal at el., 2015)Denial of Service attacks (DOS attacks), Authentication attacks, Side channel attacks, Cryptographic attacks, and Inside Job attacks are best attack vectors for those hackers and due to these generalized attacks we need a better security reinforcement for cloud computing as it can lead to a major cyber-attack. Due to this reason, there are a number of security challenges associated with utilizing