Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/jisa

An access control model for cloud computing

Younis A. Younis*, Kashif Kifayat, Madjid Merabti

School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool L3 3AF, UK

Keywords:
Cloud computing
Cloud computing security
Access control models
Task-Role Based Access Control
Cloud based access control model

ABSTRACT

Cloud computing is considered one of the most dominant paradigms in the Information Technology (IT) industry these days. It offers new cost effective services on-demand such as Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). However, with all of these services promising facilities and benefits, there are still a number of challenges associated with utilizing cloud computing such as data security, abuse of cloud services, malicious insider and cyber-attacks. Among all security requirements of cloud computing, access control is one of the fundamental requirements in order to avoid unauthorized access to systems and protect organizations assets. Although, various access control models and policies have been developed such as Mandatory Access Control (MAC) and Role Based Access Control (RBAC) for different environments, these models may not fulfil cloud's access control requirements. This is because cloud computing has a diverse set of users with different sets of security requirements. It also has unique security challenges such as multi-tenant hosting and heterogeneity of security policies, rules and domains. This paper presents a detailed access control requirement analysis for cloud computing and identifies important gaps, which are not fulfilled by conventional access control models. This paper also proposes an access control model to meet the identified cloud access control requirements. We believe that the proposed model can not only ensure the secure sharing of resources among potential untrusted tenants, but also has the capacity to support different access permission to the same cloud user and gives him/her the ability to use multiple services securely.

1. Introduction

Cloud computing is an open standard model, which can enable ubiquitous computing and offer on-demand network access to a shared pool of configurable computing resources. It is Internet-centric and provides all of its resources as services such as storage, computation and communication. Cloud computing is a unique combination of capabilities and innovation technologies. It needs minimal management effort from service providers (Mell and Grance, 2011) and delivers scalable and dynamic infrastructure, global/remote access and usage control and pricing. Almost three-fourths of 572 surveyed business leaders, indicate that their companies have piloted, adopted or considerably implemented cloud computing in their organizations and 90% expect to have done so in next three years. Moreover, those companies who have substantially implemented cloud computing are expected to grow from 13% to 41% within the next three years (Berman and Kesterson-Townes, 2012).

Security is one of the primary concerns and a major barrier to adopt cloud computing. Cloud computing may suffer from conventional distributed systems' security attacks such as

* *Corresponding author.*
E-mail addresses: Y.A.-Younis@2012.ljmu.ac.uk, younis_amy@yahoo.com (Y. A. Younis).

http://dx.doi.org/10.1016/j.jisa.2014.04.003

malicious code (Viruses, Trojan Horses), back door, Man-in-the Middle attack, Distributed Denial-Of-Service (DOS) attack (Wang, 2011), insecure application programming interface, abuse and nefarious use of cloud computing and malicious insiders (Dan Hubbard and Michael Sutton, 2010). Cloud services could be inaccessible due to these attacks and generate negative impact. It is an important and primary requirement for cloud service providers to ensure its services are fully usable and available at all time (Wang et al., 2009). Moreover, cloud computing has brought new concerns such as moving resources and storing data in the cloud with probability to reside in another country, which has different regulations. Furthermore, cloud computing is a shared environment, which uses sharing infrastructure. Hence, data may face issues like privacy and unauthorized access. These issues can get more complicated when different service providers use various types of technologies and cause potential heterogeneity issues (Subashini and Kavitha, 2011). Furthermore, virtualization brings its own issues such as data leakage (Lombardi and Di Pietro, 2011).

Information in cloud computing is likely to be shared among different entities, which could have various degrees of sensitivity. Therefore, it would require robust isolation and controlling access mechanisms. In order to draw the whole picture, we have done an in-depth investigation on cloud security and identified different security requirements for different cloud users (e.g. critical infrastructure service providers and small businesses). We have found access control is one of the common and fundamental requirements for all types of cloud users. However, conventional access control models cannot be applied in the cloud environment due to the following reasons:

- Cloud computing can be very complex and sophisticated due to the dynamic nature of the cloud's resources (Masood and Shibli, 2012).
- Entities which are cloud based are likely to reside in varied trusted domains and may be located in different countries that have various regulations. Thus, they may not trust each other (Wan et al., 2012).
- Conventional access control models in cloud computing would suffer from the lack of flexibility in attribute management and scalability.
- Heterogeneity and variety of services (Takabi et al., 2010).
- Diversity of access control policies and various access control interfaces can cause improper interoperability (Tianyi et al., 2011).
- Dealing with a large number of users, different classification, high dynamic performance, mobility features and changes in high frequency (Wang et al., 2011).
- Different access permissions to a same cloud user, and giving him/her ability to use multiple services with regard to authentication and login time (Wang et al., 2011) (Almutairi et al., 2012).
- Sharing of resources among potential untrusted tenants, multi-tenancy and virtualization, mechanisms to support transfer customers' credentials across layers to access services and resources are crucial aspects in any access control model going to be deployed in cloud computing (Almutairi et al., 2012).

There may be possibilities to extend existing access control models and use them in the cloud environment. However, this could be a potential risk and may not solve the problem as conventional access models may focus on a specific problem in a specific platform or environment and miss the remaining interconnected issues. This could happen due to inexistence of a complete list of access control requirements for cloud computing. In other words, the success on any access control solution for cloud computing will depend on analyzing and accurately identifying a complete list of requirements.

In this paper, we have performed an in-depth investigation and identified access control requirements for cloud computing. To the best of author knowledge, fundamental requirements of cloud based access control models have not yet been adequately investigated. This paper also proposes a novel Access Control model for Cloud Computing (AC3). We believe the proposed model can fulfil access control requirements for diverse cloud based users who are sharing resources among potential untrusted tenants.

The AC3 has three different levels of security, which can be used according to the level of trust. It supports various sensitive levels of information in order to restrict who can read and modify information in the cloud. The proposed model has the flexibility to cope with different access permissions to the same cloud user and give him/her the ability to use multiple services with regard to time of authentication and login.

The layout of this paper is as follows: Section 2 provides a critical analysis to traditional access control models and proposed access control approaches utilized in the cloud so far. It also illustrates an in-depth analysis of the fundamental requirements of cloud based access control models. Section 3 sets out the proposed model. A comprehensive security analysis and discussion are presented in Section 4. This is followed by our conclusion in Section 5.

2. Access control in cloud computing

An access control system is a collection of components and methods that determine the correct admission to activities by legitimate users based upon preconfigured access permissions and privileges outlined in the access security policy (Anderson, 2010). The fundamental goal of any access control system is restricting a user to exactly what s/he should be able to do and protect information from unauthorized access. There is a wide variety of methods, models, technologies and administrative capabilities used to propose and design access control systems. Thus, each access control system has its own attributes, methods and functions, which derive from either a policy or a set of policies.

Cloud computing is a shared open environment, which has its own characteristics and features such as on-demand services and mobility. Thus, cloud service providers need a strengthened access control system for controlling admission to their resources with the ability to monitor precisely who accesses them. They should have the ability to deal with dynamic and random behaviours of cloud consumers, heterogeneity and diversity of services. In this section, a background about conventional access control models and why cannot be deployed in the cloud are presented. It also illustrates