UNIVERSITY OF SCIENCE AND TECHNOLOGY

COLLEGE OF GRADUATE STUDIES AND ACADEMIC ADVANCEMENT

Access Control Methods in Cloud Systems

A Thesis

Submitted to the College of Graduate Studies and Academic Advancements

in Partial Fulfillment of the Requirement for the Degree of Master of Science in Information Technology

Prepared By:

Maha Elfadil Mohamed Ahmed

Supervisor By:

Prof. Noureldien Abdelrhman Noureldien

Jan 2017

Abstract

Cloud computing is considered as a large scale distributed computing paradigm which provides a flexible, cost-effective and proven delivery platform for business and consumer services over the Internet.

Clouds provide simultaneous, secure hosting of services for various customers utilizing the same cloud infrastructure resources, but one customer can gain unauthorized access to the information of other customers. In this context, it is important to control the user's access to the network entities and information. Access control is generally defined as a policy or procedure that allows, denies or restricts access to a system. Many access control techniques were originally designed for enterprise environments that do not consider the characteristics of cloud computing and multi-tenancy environments. These techniques are definitely effective but we need complimentary techniques that fit cloud computing and prevent unauthorized access to the resources in the distributed system.

In this thesis we study and analyze some of the existing methods of controlling access in cloud environments, and then we provide a systematic, organized, and classified literature survey for these methods.

المستخلص

تعتبر الحوسبة السحابية نموذج حوسبي موزع واسع النطاق يوفر المرونة، الفعالية من حيث التكلفة، و يمثل منصة للخدمات التجاريةللمستهلكين عبر الانترنت. الحوسبة السحابية تمكن عملائها المختلفين الاستفادة من خدماتها المقدمة و مواردها في آن واحد ، و لكن قد ينتج من ذلك ان يتمكن احد العملاء من الوصول غير المصرح به لمعلومات عملاء آخرين في نفس السحابة.

في هذا السياق لابد من السيطرة على وصول هؤلاء العملاء الى شبكة المعلومات بإتباع تقنية التحكم في الوصول (Access Control)، و التي تعرف بأنها سياسة او اجراء من شانه ان يسمح ، يمنع، او يقيد وصول المستخدم او العميل الى النظام.

هنالك عدة تقنييات تم تصميمها للتحكم في الوصول، تناسب البيئة المؤسسية و لكننا بحاجة لتقنيات تتناسب مع خصائص الحوسبة السحابية و البيئات المتعددة الايجار لمنع المستخدمين و المستأجرين من الوصول غير المصرح به للموارد.

فيهذا البحث قمنا بدراسة بعض الطرق المقترحة بواسطة الباحثين للتحكم في الوصول في بيئات الحوسبة السحابية، و من ثم تنظيمها ، تصنيفها و ترتيبها.

UNIVERSITY OF SCIENCE & TECHNOLOGY

1.1 Introduction

In the early years between 1960 and 1961 John McCarthy, an American computer scientist and cognitive scientist, came up with the idea of computer or information utility. In 1961 at MIT Centennial John McCarthy pointed out “If computers of the kind I have advocated become the computers of the future, then computing may someday be organized as a public utility just as the telephone system is a public utility. The computer utility could become the basis of a new and important industry”.

Cloud Computing (CC) has developed from McCarthy’s idea of utility computing which begins the commoditization process to a new service that is widely available and has become undistinguishable from others like it, which consumers make the decision to purchase it based on price [1].

Cloud Computing technology has become a popular alternative to traditional computing technologies. This technology provides a new concept of a pay-per-use utility model of computing resources based mainly on virtualization technology. Numerous benefits result from these features, such as cost-effectiveness, time saving, scalability, and green information technology environment.

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. Access control is one of the common and fundamental requirements for all types of cloud users.

1.2 Problem Statement

Cloud computing faces many challenges associated with utilizing it such as data security, abuse of cloud services, malicious insider and cyber-attacks. It also has unique security challenges such as multi-tenant hosting and heterogeneity of security policies, rules and domains. Among all these 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.

There are 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 fulfill cloud’s access control requirements because they don’t have the ability to deal with dynamic and random behaviors of cloud consumers, heterogeneity and diversity of services.

In a cloud, users are normally identified by their attributes or characteristics and not by predefined identities. Thus, one needs dynamic access control to achieve cross-domain authentication

Many research papers have been published on the topic of cloud control access methods and techniques. Some of these papers proposes a new methods, others are an enhancement for an existing ones and a few papers try to survey theses proposed methods.

The existing of an up-to-date survey that provides the state of the art of cloud access control techniques is of great importance to cloud community.

1.3 Research Objectives and Research Questions

The objective of this research is to provide insight on the problem of restricting a user to exactly what s/he should be able to dote avoid the data in the clouds being illegally accessed, distorted and used. Our aim is to identify and analyze the problem and to investigate the controlling access in cloud computing through studying various methods that have been proposed, in order to provide an organized, systematic, and classified up-to-date survey.

The questions of this research are:

1- How user’s access is controlled in cloud computing environment?

2- What methods have been proposed for access control?

3- How access control methods are classified?

1.4 Motivations

Almost all enterprises today share their data among their internal users and customers. In their local networks, enterprises have full potential on user's access control. Moving towards cloud computing, enterprises must be confident on security and access control mechanism provided by Cloud Service Providers (CSP).

As far as the confidentiality and privacy in cloud computing is concerned, the area of an access control has been attractive for the researchers. Some of the works carried out by them to develop an efficient access control models, our thesis gives an up-to-date review on some of the existing methods.

1.5 Research Methodology

The information for this thesis was collected from research papers published in journals, conference and digital libraries. A literature review methodology is applied which contains seven steps: searching, obtaining, assessing, reading, critical evaluation, recording, and writing. This methodology is explained in details in chapter 3.

1.6 Research Scope

This thesis will not discuss any technical description or mathematics behind the proposed access control methods.

1.7 Thesis Contribution

The contribution of this is:

i. Clarifying the concept of cloud access control.
ii. Identifying the currently proposed cloud access control methods.
iii. Classifying the proposed cloud access control methods.

1.8 Thesis Structure

The remaining contents of the thesis are organized as following:

Chapter 2 contains important aspects of cloud computing, including its definition, essential characteristics, models of cloud services, pros and cons of using cloud computing. The chapter also briefly stated the challenges and security issues that faces cloud computing.

Chapter 3 presents the research methodologies being used to conduct this research. Chapter 4 gives the technical background needed to understand some of the proposed access control model, such as Role-Based Access Control (RBAC), Attribute-Based Encryption Access Control(ABEAC), and Multi-Tenancy Access Control (MTAC). Finally chapter 5 includes the conclusion and future direction of research in an access control methods.

UNIVERSITY OF SCIENCE & TECHNOLOGY