Profile-Based Access Control in Cloud Computing Environments with applications in Health Care Systems

By

Umair Mukhtar Ahmed Naushahi

A thesis submitted to the
Department of Computer Science
In conformity with the requirements for
The degree of Master of Science

Bishop's University
Sherbrooke, Quebec, Canada
February 2016

Abstract

Recently cloud computing has gained tremendous attention among researchers from both academia and industry. It has emerged as a promising technology for delivering on demand information technology services over the Internet while providing great flexibility in enhancing the hardware, software and network infrastructure of organizations. Consequently many institutions, organizations and individual users are migrating from a traditional computing environment to a cloud computing environment. Cloud computing has also been used in providing health care services such as information sharing, accessing various health care services, and utilizing resources across the board. While cloud computing offers numerous benefits, it also introduces some new and recurring challenges such as data computation & communication integrity, security and privacy. Due to its potential data security and privacy concerns, adopting a cloud based infrastructure for health care domain while meeting the privacy and security regulations recommended by HIPAA, PIPEDA and PHIPA is a big challenge. We study and analyze the security and privacy requirements of health care systems in a cloud computing environment and present a profile based access control system to improve the security and privacy of health care data while providing seamless service provisioning. We extend the concept of access control list by incorporating the *Profile* attribute and define rules for each profile to grant access to the system and its resources. In addition, when user authentication is done, profiles are mapped to the applications running on the cloud and eliminate the need of repetitive authentication requests for accessing each application. We also decompose the access control list in different parts. Such a decomposition helps reduce the management and administration cost, and allows

updating or adding new rules without maintaining complex rule matrices. The profile authentication process can be offered as a service to support authentication and system availability across different cloud deployments. Simulation results show that our solution offers reduced data access time and improves service provisioning while reducing authentication requests. Considering the hierarchical organizational structure of health care systems, the profile based access control approach best fits its requirements.

Acknowledgements

Firstly, I would like to express my sincere gratitude to my advisor Prof. Stefan Bruda for the continuous support towards my degree and related research, for his patience, motivation, timely assistance during meetings constant evaluation of various drafts of my work, immense technical knowledge and technical support. His guidance helped me in all the time of research and writing of this thesis. I would also like to thank Prof. Nelly Khouzam for her support throughout my studies.

Last but not the least, I would like to thank my family my parents and sisters for supporting me spiritually and praying for me throughout writing this thesis.

Table of Contents

List of Figures

List of Abbreviations

ABE	Attribute Based Encryption
ACL	Access Control List
CURD	Create, Update, Retrieve, Delete
HIPPA	Health Insurance Portability and Accountability Act
IAAS	Infrastructure-as-a-Service
IBE	Identity Based Encryption
IBHMCC	Identity-Based Hierarchical Model for Cloud Computing
IBS	Identity Based Signature
ICT	Information and Communication Technology
NIST	National Institute of Standards and Technology
PAAS	Platform-as-a-Service
PEHR	Personal Electronic Health Record
PHR	Personal Health Record
PIPEDA	Personal Information Protection and Electronic Document act
SAAS	Software-as-a- Service
SAP	SSL Authentication Protocol
SLAs	Service Level Agreements
XACML	eXtensible Access Control Markup Language

1 Introduction

The emergence in information and communication technologies (ICT) has changed the way organizations and individuals used to perform their daily workflow and business operations. Recently cloud computing has gained tremendous attention among researchers from both academia and industry. It has emerged as one of the promising technologies that is shifting the computing paradigm from traditional computing into the new era of cloud computing. The pervasive access to dynamic unbounded computing resources, network and software infrastructure with increased elasticity and flexibility has provided computing and communication to users ubiquitously and at an affordable cost. Consequently many institutions, organizations and individual users are migrating from traditional computing environments to a cloud computing environment. Cloud computing has also been introduced to provide health care services such as information sharing, accessing various health care services, utilizing resources across the board and improving and enhancing overall information and communication infrastructure among its major stakeholders such as patients, doctors, and pharmacists.

While cloud computing offers numerous benefits like dynamic scalability, anytime anywhere computing and communication, reduced infrastructure cost, etc, it also introduces some new and recurring challenges in data computation & communication integrity, security and privacy etc. These challenges have become a major concern in adopting cloud computing for health care industry, as data security and privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA) [7] , and the Personal Information Protection and Electronic Document Act (PIPEDA) [5] require health care services providers to ensure security and privacy of patients health related data (Personal Electronic Health Record or PEHR for short), continuous access to data, data protection, and prevention from unauthorized access. In this thesis, we study the security and privacy requirements of health care data and present a security architecture for protecting health care data in cloud computing environments. In this chapter, we present the introduction to cloud computing technology, design and security issues in cloud computing, problem statement addressed in this thesis followed by our research objective.

1.1 Cloud Computing

Cloud computing technologies are a new paradigm shift in computing platforms [10]. Cloud computing is becoming popular nowadays. Companies like, Microsoft, Amazon, Google, IBM and others are adopting cloud systems and migrating their services to cloud to reduce the cost and attract more customers [2]. Generally speaking cloud computing is not a new technology, it mainly inherits its technical and operational concepts from existing technologies like grid computing, virtualization, utility computing and autonomic computing. The research and advancement in these technologies helped coin the concept of cloud computing. With all the commonalties with above mentioned technologies the main difference of cloud computing compared with the traditional computing model is a new operation and delivery model that leverages the Internet and other communication channels to provide computing and other services to its user while reducing the cost. The most commonly cited and comprehensive definition for cloud computing is presented below:

"Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [33]".

From the definition above, Peter et al [33] presented some basic characteristics of cloud computing which make it stand apart from traditional computing models, as follows:

- **On-Demand Self-Service:**

The on demand characteristic of cloud computing allows cloud users to utilize services and resources automatically and on demand. While accessing on demand services, users can customize their services without requiring any human interaction. The services that are required by the users can be provided to them when needed which saves time and reduce the overall cost.

- **Broad Network Access**:

The broad network access characteristic of cloud computing allows cloud providers to offer services that can be accessed by their users from heterogeneous communication channels. This gives users the opportunity to access cloud service and resource ubiquitously and stay connected to the services they are subscribed to. This also promotes the interoperability of services across the cloud networks.

- **Resource Pooling:**

The resource pooling characteristic of cloud computing allows multiple users to utilize services using a multi agent model. The services and resources are dynamically assigned to users based on their demand. As the services are offered in a cloud environment, users are not aware of the exact location of the services and resources they are using. For instance a user saving data on Dropbox[1] is not aware of the location of the storage server.

- **Rapid Elasticity:**

The rapid elasticity characteristic of the cloud makes the cloud computing architecture more flexible and scalable. This elasticity allows organizations to scale their services rapidly based on their needs.

- **Measured Service:**

Unlike the traditional computing model, cloud computing offers a control to measure the use of infrastructure (e.g. storage, processing, bandwidth and active user accounts) that are available to its users. The cloud provider can control and monitor the use of the services and resources by leveraging metering capabilities. This allows users to utilize the services when needed while reducing the cost of the service or resource.

1.1.1 The Cloud Service Delivery Models

The service model is controlled and monitored with the help of the cloud management. There are a number of cloud service providers utilizing different cloud management techniques to control, manage and monitor all the activities executed on the cloud.

[1] https://www.dropbox.com/about

Service models are the core components of cloud computing [40]. The three most commonly used service models are briefly described as follows:

- **Software-as-a-Service**

Software as a Service (SAAS) provides on demand software access to the cloud users. The customized software applications are simulated on the cloud. The main goal of this layer is to reduce the cost of the infrastructure and hardware. The layer is usually maintained by the cloud service provider [36].

- **Platform-as-a-Service**

Platform-as-a-Service (PAAS) provides services for application development, design and implementation. These services are also provided on demand according to the user specification. The main purpose is to reduce the cost of buying and managing a large amount of hardware. Users can also avoid the cost of creating a testing environment. The user can set the application development environment parameter according to its specification and needs [40].

- **Infrastructure-as-a-Service**

Infrastructure-as-a-Service (IAAS) is a model that provides the basic computing infrastructure including storage, network, software and server. These services are provided on demand according to the companies or users requirements for example local computing infrastructure can be replaced by cloud infrastructure, local telecommunications infrastructure can be replaced with Voice over IP and other off-site Internet services [11].

1.1.2 Cloud Deployment Models

Like traditional computing environments, cloud computing has its own deployment models to implement the service models described above. There are three commonly used deployment models to implement the cloud service architecture.

- **Public Cloud Model**

The public cloud model is the most commonly used deployment model for the cloud computing service. In this type of model services are offered using public or shared networks such as the Internet. The services offered using this model are generally shared among all user groups and therefore all the resources and services are available and visible to everyone using the cloud. The best example of this kind of deployment model is the cloud-based web hosting services such as Amazon Elastic Compute Cloud (EC2), Google Apps, etc. where resource and service offered by the provider are shared among all their hosting clients.

- **Private Cloud Model**

The private cloud model is mostly used by individual organizations where the resources and services are only offered to their own employees or customers. In this model the access to services is offered using private leased lines or other secure communication channels, so that services and resources are not visible to unauthorized users and are only accessible to specified users. This model provides greater privacy and control compared to the other variants. The best example of this kind of deployment model is private data centers or virtual private cloud services.

- **Hybrid Cloud Model**

The hybrid cloud model is the combination of the private and public cloud models. The functioning of this type of model is similar to private and public cloud models as discussed above. The advantage of this model allows organizations to distribute part of their services on public and the other part on private cloud infrastructure.

1.2 Design and Security Challenges

Security and privacy are important requirements when designing the cloud based infrastructure for health care systems. We outline some common design and security challenges for designing security architecture for health care computing in a cloud computing environment.

- **Availability**

Availability refers to all-time availability of data or service when they are needed. In the health care domain patient data is of great importance, any loss or unavailability of data or service may cause serious consequences and threat to patient's life. Therefore a cloud solution for health care applications must ensure all-time availability of data and services, proper load balancing, secure access control and other security requirements to garantee proper delivery of services for its users.

- **Confidentiality**

Confidentiality means ensuring data privacy, i.e. the data and services should not be accessible to unauthorized users. The system must implement access control policies and police the user personal information so that it is not transferred or used in any unauthorized manner. Thus cloud computing solutions designed for health care systems must ensure data privacy and protection.

- **Authorization**

Authorization is a secure access control mechanism in place to access the data and services offered on the cloud. In health care applications patient data are accessed and shared among multiple stakeholders, hence systems implementing health care solutions should implement secure and scalable authentication mechanisms.

- **Integrity**

Integrity is ensuring the data security in terms of its contents. For instance systems should ensure data validity by not allowing unauthorized users to modify or alter the data. As stated above patient data is of great importance, any unauthorized modifications or alteration in data will impact the diagnosis and treatment decisions of a patient. Therefore systems implementing cloud solutions for health care applications should ensure data integrity so that the data is never compromised.

1.3 Problem Statement

The information and communication systems have been integrated into a number of real time and critical applications such as weather monitoring, flood detection, emergency response, etc. [14]. In recent years, health care computing systems have gained tremendous attention and more and more institutions are implementing health care solutions to enhance and improve their services while minimizing the overall cost [26]. The objective of health care computing systems is to provide their users with easy and anywhere anytime access to health care data and services. Hence to achieve this objective, cloud computing and its business model can play a vital role by providing these services at larger scale and at affordable cost. However, it has been reported that most of the health care institutions are hesitant in adopting cloud computing based solutions due to their potential data security and privacy concerns [21] [41].

In a cloud computing environment, health care systems and services are offered through public or private cloud and so they are vulnerable to many security threats. There is a high probability that unauthorized users may attempt to gain access to personal health data which can lead to serious data security and privacy concerns [13]. In this thesis, we study the security and privacy challenges of health care data in cloud computing environments and present a solution to prevent the unauthorized access to data by proposing a new access control mechanism that can act as security layer on the top of all cloud service models.

1.4 Research Objective

Our objective is to design a security architecture that will provide a solution of the common software application security issue that exists in the cloud computing service model. The proposed architecture will be analyzed in the context of the public or private cloud computing environment. The design of the proposed solution will be based on open source technologies.

1.5 Thesis Organization

The rest of this dissertation is organized as follows; Chapter 2 presents the literature review that highlights the existing security and privacy solutions for cloud computing environments followed by the analysis of existing solutions and their shortcomings. Chapter 3 presents our security solution along with a discussion on the system components. Chapter 4 presents the simulation results. We conclude our work in Chapter 5 along with some open questions and future research directions.

2 Related Work

This chapter presents the detailed discussion on the security mechanisms which can be utilized for securing information in a cloud computing environment. The three main areas which will be discussed in this chapter include cloud computing security solutions, firewall acting as a virtualization security solutions and access control based solutions. An analysis of the existing solutions will also be presented to identify their limitations and drawbacks.

2.1 Security in Cloud Computing

Security, privacy and trust issues have existed since the inception of the Internet. The reason they are widely discussed these days is because of the cloud computing scenario [37]. Security is considered as one of the main concerns in the adoption of the cloud computing model. Security issues in such an environment include service management (service provisioning and service execution), user access control (while using role based model or working in a hierarchical infrastructure), multiple access to services or resources, denial of service, memory and resource management. However data security and privacy are considered as one of the critical challenges in every information system and it is one of the major concerns in cloud computing research as well [27].

For instance if patient medical data is infected, misused, stolen, lost or is not available when required this will result in serious consequences for that patient and also for the organization managing patients data. Therefore issues related to data security such as access, privacy, availability or integrity are the main research challenges for health care system in a cloud computing environment.

Numerous solutions to secure data in a cloud computing environment are reported in the literature. However, challenges and opportunities still exist while replacing legacy system and adopting and implementing cloud computing based solutions for health care domain. Health care information systems contain high level of records of patients, appointment scheduling, work schedule management, medical journals and other related information that must be secured and kept confidential [44].

There are number of research studies conducted for securing data and addressing privacy issues in the cloud. These studies identified possible attacks and security threats and presented solutions to secure the cloud environment. Researchers suggested using access control as one of the effective mechanism while dealing with service or data access security scenarios. The access control mechanism provides access and privileges to authenticated users to access resources and data. The cloud computing environment offers a dynamic relationship between users and the resource they use. Designing a dynamic, secure, flexible and scalable access control system is a great challenge. The reminder of this chapter presents a discussion on related solutions and their limitations for data security and privacy for health care application data.

Khan [20] suggested to use the attribute based access control mechanism for cloud environments and presented an attribute based access control mechanism. In his solution, access to data, resources and services are granted on the bases of the attributes of the requestor. If the requestor fails to provide the correct attributes for the service requested, then the system does not grant access to the service or resource that is been requested. Although attribute based access control could be a good solution when it is applied within the same security domain, there is no evidence on how the system will perform when dealing with multiple security domains. Indeed, in the dynamic and competitive business model of cloud computing users and service providers are not in same security domain.

Raykova et al, presented a two-level access control method that combines coarse-grained access control at the cloud end to provide security against partial view of user access, with fine-grained cryptographic access control at the user end to provide the desired expressiveness of user access and control policies. The two main operations (i.e. read and write) were tested to validate the system [35]. The limitation of this solution is at the cloud end where one has to continuously upgrade the cryptographic algorithms to avoid unauthorized access to the resource and keep the security system updated against new security threats.

In another effort Li et al [24] presented an access control method for health care applications where multiple users can access their data in the cloud environment. The authors presented a scalable novel access control framework based on the attribute based encryption (ABE) techniques that encrypt each patient's Personal Health Record (PHR) data. Their system is divided into multiple security domains, where each domain manages only a subset of the users. This system division helps reduce the key distribution complexity which is an important component in such multi-owner settings. However, encryption key distribution among users remains an open question when dealing with multiple deployment models and accessing service across the cloud environments.

In another effort, Li et al [23] presented an identity based access control method to secure the access to the cloud services. The authors presented an identity-based hierarchical model for cloud computing (IBHMCC) and its corresponding encryption (i.e. identity based encryption (IBE)) and signature (i.e. identity based signature (IBS)) schemes and compared their results with the traditional SSL Authentication Protocol (SAP). The author argued that their solution is lightweight and more efficient than SAP. The solution is best suited for private clouds. No evidence about the performance of this system in the public cloud and with different security models is provided.

In another work, Almutairi et al. presented the Distributed Access Control Architecture for Cloud Computing based on principles drawn from security management to meet the user's access control requirements and principles drawn from software engineering to generate security requirement specifications. Their solution can be implemented using an XML-based formalism which makes it easier to implement in the current service model of cloud computing [3]

Similar to this work several other authors presented their solution to ensure the cloud security. For instance Nurmi et al. presented a solution to ensure secure access to control and execute services in virtual environments [32]. In another work Berger et al presented a role-based access control mechanism with security labels to secure the data and resources in the cloud environment. Their system allows the users to access services and resources based on the access roles and rules defined by the administrator [6].

Another paper argued the need of a more dynamic, flexible and scalable access control mechanism that can support the large number of users and service offered in a heterogeneous environment. The author proposed dynamic risk-based access control architecture by adding three new components namely the risk engine, the risk quantification web services, and the risk policies using the eXtensible Access Control

Markup Language (XACML) standard. The model grants access to resources based on a combination of XACML decision and risk analysis. However to make the best use of this system, the system has to be manually trained and extensive risk assessment has to be performed [12].

In another work, the authors presented the access control mechanism based on the concept of trusted computing [38]. Their system audits and examines each user that accesses the cloud data and resources. The system imposes high security and privacy, but the process of auditing and examining each user becomes increasingly complex when the network traffic increases.

Meghanathan presented a review of existing access control models for cloud computing and divided the existing access control models into three different categories: (1) role-based models, (2) attribute-based encryption models, and (3) multi-tenancy models. The author presents the pros and cons of each model. To get more insight on each category the reader is invited to browse this review [29]; a similar review is also available [34].

In another solution Iqbal et al [18] proposed an Intelligent Security Framework for Cloud Computing Environment. The framework implements a secure access control method that can be deployed on top of any service model based on the NIST architecture [30]. In their solution, the authors proposed a role based access control mechanism based on the key exchange methodology. The access control has two main parts: the first is a role & rule book and the second is the concept of security tags. The former is more like the active directory mechanism where the cloud provider can assign and grant access to its users, whereas the latter is used to create security and data tags for the applications offered on the cloud. Although the authors argued that their solution can be deployed in any cloud deployment model and improve the security of application access and provisioning, a tradeoff between performance and security takes place. In addition, we cannot eliminate the limitations of software ID tags and hash keys which can cause high resource utilization, costly software audits and the possibility of hackers developing fake software ID tags.

The system security architecture is always considered the center piece of attention as every organization is concerned about their data security and privacy [4]. In addition to the access control solutions summarized above, researchers presented other security frameworks that can be used to improve the overall security of the cloud computing architecture. Efforts have been put into securing cloud computing by virtualization based security solutions [28] [19]. In these types of solutions the hypervisor concept is used to secure cloud access. Here the hypervisor acts as a security rule component or a security layer which safeguards the access to the cloud services based on the defined access rules. Another paper [22] presented an architecture for addressing the data security issue that can be deployed as a third party solution (logical access layer on the cloud delivery model) on any delivery model of the cloud computing architecture. In another work, Mishra et al presented a security framework based on the user authentication mechanism [31]. The framework has three main components (Lightweight Directory Access Protocol, SAML and Kerberos server authentication) which can be applied at any layer of the cloud environment or can be offered as security as a service. Another paper [9] presented the solution based on database security principles to address the issue of data migration that may appear during the transfer from a traditional solution to a cloud application. Other researchers [40] highlight the security and privacy issues that can occur during the data migration from traditional computing systems to the cloud computing environment and presented possible solutions to secure the migration process.

2.2 Analysis

In this section, we present our analysis of the literature review presented above. It has been reported that data security is one of the main concerns in adopting cloud computing technologies especially for the health care domain. Numerous studies advocate the need of improving the traditional security solutions to meet the security requirements of cloud computing technologies. To the best of our knowledge most of the solutions are at the access control layer level and researchers have presented solutions that are best suited to the particular scenarios described in their solutions. However, when we analyze these solutions in the health care domain, we see a need for more secure and generic solutions that can satisfy the data security and privacy need of health care applications. For instance solutions like packet sniffing [30] keys hashing and X.10 security based solutions [15] [1], IP spoofing [16], are customarily used to secure the access to the cloud services. All these solutions have disadvantages including high computation requirements, security key generation and management algorithms, multi user support to function in multi user organizational hierarchy environment where every user has different roles and access right for the data and service they access, and various degrees of support to function in different cloud deployment and service models.

We have also surveyed in the previous section advanced security solutions that can function well with service oriented models of cloud computing. Our survey shows that there is work to be done when addressing issues like multi-access in heterogeneous environments, lack of support for Service Level Agreements (SLAs), lack of multi-tenancy supports etc.

A number of concerns arise during the adoption of cloud computing, such as data security, data availability, integrity, data privacy and control, etc. These issues are important in other domains but they become even more important when dealing with health care data [8] [4]. The data in health care computing systems needs to be more secure, as any denial of service or loss of data may result in serious implications. Securing such an environment is a big concern when migrating health care services from traditional to cloud computing environments.

3 Profile Based Access Control

In this chapter, we present our proposed solution to secure the health care data in a cloud computing environment. In our effort we tried to address the data security, data availability, data integrity, and data privacy issues by presenting an access control mechanism at the security layer of the cloud computing architecture. Our solution is based on the concept of traditional access control lists [39], which allows filtering the incoming traffic based on some predefined criteria and so selectively grants access to services and resources. In the remainder of this chapter we will present the detailed description of, and also a discussion on the proposed solution.

3.1 Preliminaries

Before we begin our description, we would like to discuss some related concepts that will help readers understand the proposed solution. First, we include a brief discussion on the cloud computing reference architecture and its components proposed by NIST [25]. In addition, we provide an analysis of the security solution proposed by Iqbal et al [18], followed by a discussion on access control list [39].

3.1.1 NIST Cloud Computing Architecture

In our discussion above (Chapter 1), we presented the definition of cloud computing, defined by Peter, et al. [33]. This definition is widely accepted among researchers from academia and industry. Based on the definition, researchers at NIST formulated the conceptual architecture for the cloud computing model. The architecture presents a high level conceptual view of the cloud computing model and identifies the major actors along with their activities and functions. It serves as a reference model for researchers to study the cloud computing model and its various components to design and simulate the cloud based services. The reference architecture is presented in Figure 3-1. It incorporates five important entities that play an important role in the development of cloud computing models.

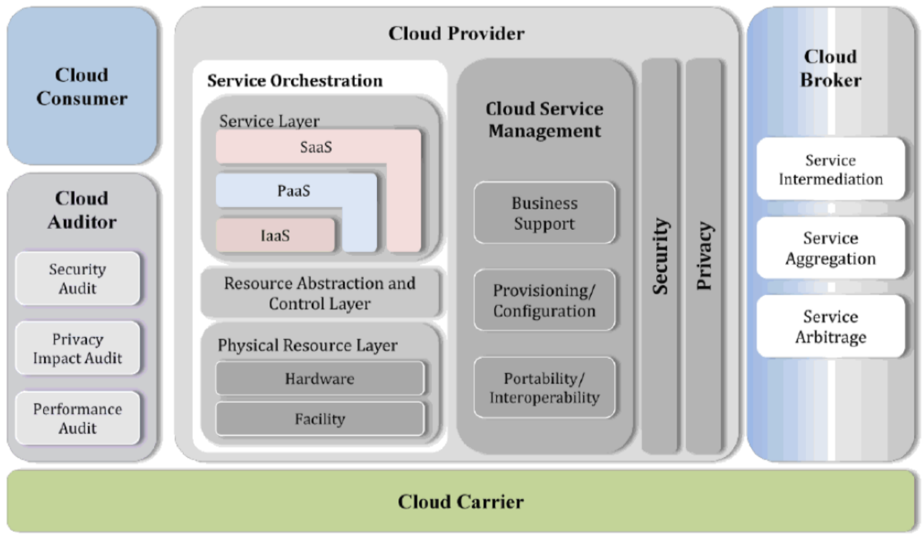


Figure 3-1 NIST Cloud Computing Reference Architecture [33]

1. **Cloud Consumer**: The cloud consumer is a person or organization that maintains a business relationship with a cloud provider, and uses its services offered on a cloud. Examples include hospitals, schools etc.
2. **Cloud Provider:** The cloud provider is a person, organization, or entity responsible for making a cloud service available to interested parties. Examples include Google, Microsoft, Amazon Web service etc.
3. **Cloud Carrier:** The cloud carrier is a party that can conduct an independent assessment of cloud services, information system operations, performance and security of the cloud implementation.

4. **Cloud Auditor:** The cloud auditor is an entity that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers.
5. **Cloud Broker:** The cloud broker is an intermediary that provides connectivity and transport of the cloud services from cloud providers to cloud consumers.

Numerous researchers have adopted this architecture to design and simulate the cloud computing models. Major research has been invested to improve the components presented at the cloud provider end. Our effort is no exception, as we present an access control-based security solution to improve the security and privacy of a cloud computing environment.

3.1.2 Intelligent Cloud Computing Security Framework for Private and Public Clouds

To improve the security of cloud computing environment, Iqbal et al [18] presented a role based access control mechanism. The major contribution of their work is improving the access control mechanism at the security layer of a cloud computing model. The system exchanges secret keys for users to grant access to services and resources based on their roles and defined rules. In addition to user authentication and service provisioning, the authors presented the concept of Software ID tags to improve the application security. Software ID tags provide application access based on keys, but it does not specify the access rights for the applications. The core system access depends on the keys exchanged, which requires regular updates to the encryption algorithms and higher computational cost.

3.1.3 Access Control List

The access control method has been widely used as one of the promising security solutions when it comes to data/resource security and provisioning. It mostly functions based on the access policies defined by system administrators. The access control policies can be defined on any layer or component of the system. For example, access to files can be defined on file servers, access to web services on web servers, etc. [42].

These security policies are defined in many ways and at different levels. The access control list (ACL for short) is one of the mechanisms which helps the system administrator define the security and access policies for their system. The ACL is a sequential list with allow/deny entries defined for the services and resources that are available for legitimate users at any given time. ACLs ensure that only legitimate users get access to the authorized services by Providing traffic filtering, security policy execution, user provisioning etc.

3.2 Profile Based Access Control System

To secure the data and resources in a cloud computing environment, we propose a profile-based access control mechanism based on the concept of access control list. Traditionally ACLs were used to filter the incoming traffic based on IPv4 addresses and some predefined rules in an access matrix. In our solution, we incorporated the Profile attributes and rule identifiers instead of IPv4 addresses. A rule identifier points to the dictionary where all the CURD (Create, Update, Retrieve, and Delete) operations are defined for each profile and services in the system. Once a user is validated, the system generates a service access token for that user, and shares it with the user as well as the resource provisioning service. This mechanism helps minimize the authentication requests and seamlessly maps users to the services and the resources available on the cloud.

ACLs are used to define and execute the access rules for each profile. The structure of our proposed ACL is Profile (i, j), where Profile is an entity (for instance the user profile can be Patient, Doctor, Nurse, etc.), i is the service or resource (such as patient monitoring service, personal health record system (PHR) etc.) and j is the rule dictionary (which contains the data model, rule sets and pointers to other rules dictionaries) associated with service i. For instance in the construct *Patient* (*PHR*, R^{th}) Patient is the profile, *PHR* is the service that patient can and has access to, and its access rules are defined in R^{th} rule dictionary. The rule dictionary is separately stored to avoid any alteration and manipulation, and all future changes and modifications can be made without doing major alteration. The system creates access rules for all services and resources and maps them to the profiles. When a user accesses the cloud services, the profile is verified and the user is granted access to all the services that are available for that profile as defined in the rule dictionary. This mechanism helps reduce repetitive user authentication and service provisioning delays.

The distributed nature of the cloud architecture allows the cloud architect to deploy applications in different deployment models. However, supporting and maintaining the security of different services is a complex task. In our solution, access to services and resources is based on user profiles, and the system administrator can easily define access rules for each profile and deployment model. These access rights (such as CURD) can be defined while designing the application as well as while creating or modifying the rule dictionary of the application. In addition, access can also be defined for applications for different deployment models. This allows users to access services and resources across different deployment models.

Compared to the traditional access control system, our proposed system offers more flexibility and scalability to define security and privacy of data and services offered on a cloud. For instance, in role based approach defining access rules for roles at different deployment models (public, private, hybrid) is a complex task and it increases the administration and management cost for the cloud operators. In addition, compared to software ID tags proposed in [18] implementation of the rule dictionary extends the security and accessibility of applications across different deployment models. We now present the components of our system.

3.2.1 System Components

The presentation of our solution is based on the layered NIST architecture [33] as described earlier. The solution is presented at the security layer which is the gateway to access the cloud services. For the proof of concept we simulated our approach only for “SAAS” delivery model, but the solution can be extended to incorporate other delivery models. The major contribution of our solution is an improved access controller. There are three main components in the proposed access control system.

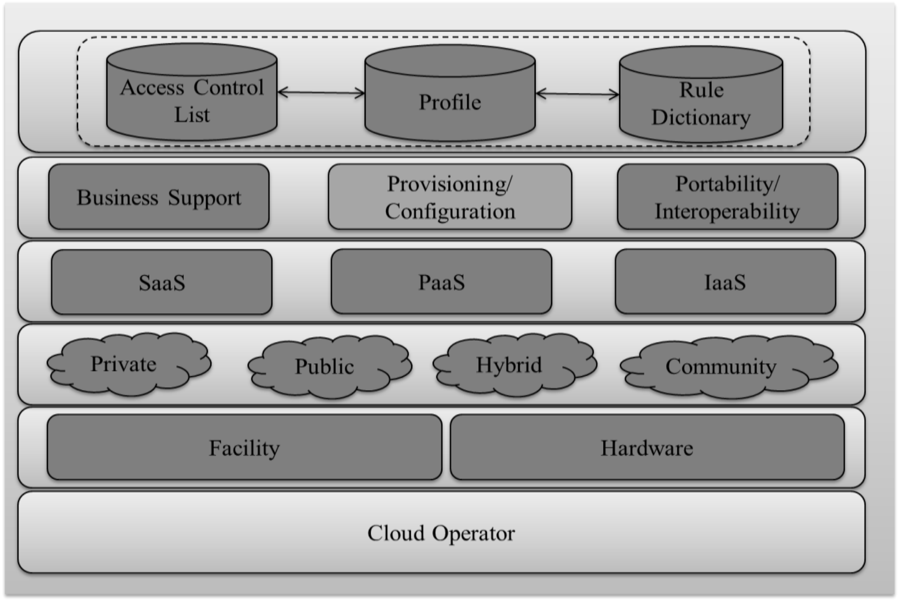


Figure 3-2 Proposed Cloud Computing Security Architecture

A. Profiles

Profile or user personalization is not a new concept in computing world. Nowadays personalization has widely been used to personalize content and services according to the user's interests and preferences. The personalization attributes are used to present users with content or services that match their profiles. In the cloud computing environment, it is highly desirable to have some kind of automatic mechanism in place that can verify the security and access policies of services and resources for the cloud users.

In our solution, we used a profile-based access control system that can be used to define security and access policies for the services and resources offered on the cloud. The profile in our case is an entity that has some pre-defined privileges to access cloud services. When a user accesses the cloud and provides the credentials, the authentication system in place validates the user credentials and verifies the user profile. Once the user profile is validated the access token is granted to the user for all the services that are available to the user of that particular profile. This prevents user to perform repetitive authorizations for each service. Also, it improves the overall security of the cloud as only services which are available for that particular profile are exposed to the user. The high level process flow of our system is presented in Figure 3-3. As a first step in the process, the user sends his/her credentials to the cloud gateway, where the authentication service will validate the user. Once the user is validated, the profile provisioning service validates the profile, and generates a user's service access token. Later, this token is shared with the resource provisioning service and is also passed to the user in an authentication access message. The benefit of sharing the access token is that we thus eliminate the process of user authentication for every service they want to access. The access token expires once the user signs out from the cloud or when the access session expires.

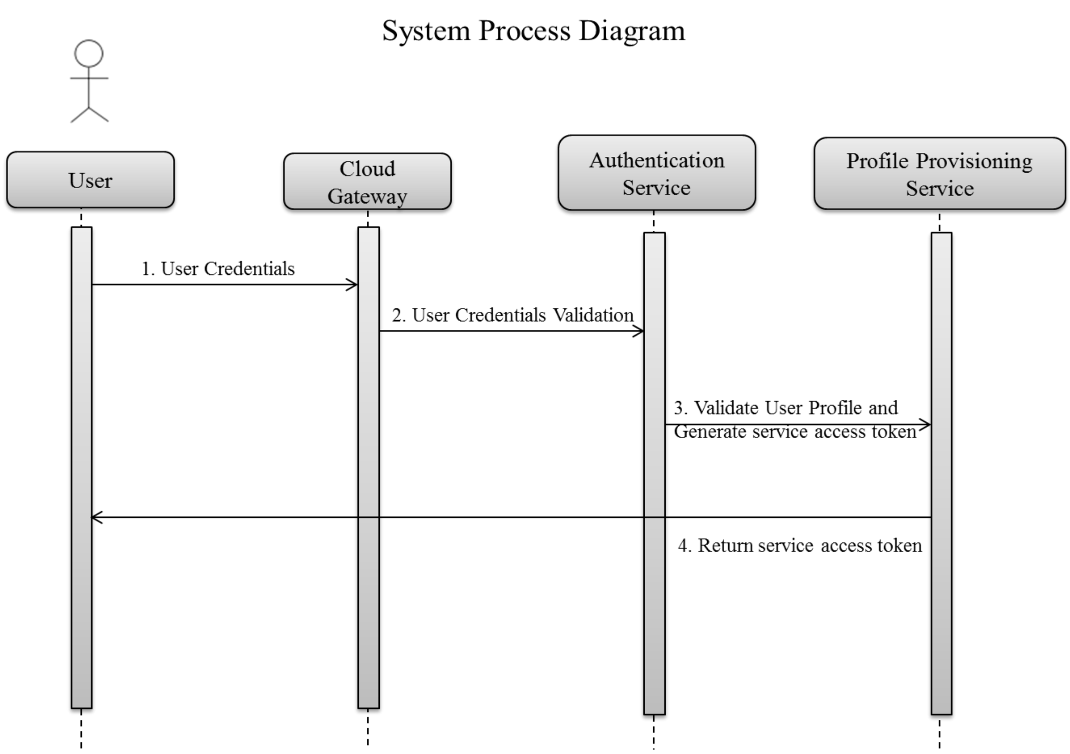


Figure 3-3 System Process Diagram

B. Rule Dictionary

The rule dictionary is proposed to define the security policy of the system. It defines the access privileges for all the resources offered by the cloud. These privileges are defined in the rule dictionary for each service the profile can access. Traditionally rules were separately defined for every CURD operation, thus increasing the number of entries in the rule book and so its management cost. In our solution, a rule identifier is defined and stored against each service and profile. The access policy (i.e. CURD operations) of these identifiers is stored in the rule dictionary. The identifier reads the rule dictionary and executes the security policy defined for each service and profile. The benefit of this approach is that it allows system administrators to update the rule dictionary for each rule identifier without affecting the access control list. This also reduces the management and implementation cost of ACL. In addition to CURD operations, the rule dictionary can also define access rules for different deployment models. This helps improve the service interoperability and access rights across cloud networks. For simplicity, we have only incorporated two deployment models (public, private). However, this can all be extended based on cloud operator requirements.

C. Access Control List

The services that are accessible to a particular profile and the access rules associated with it are defined in the access control list with the following data structure: Profile (i, j) where i represent a service or resource, and j represents the rule identifier. An example of such an ACL entry is Patient (PHR, Rule R^{th}), A more complete example of access control list is shown in Figure 3-4a.

Profile	Services Resources (*i*)	Rule Dictionary (*j*)
Doctor	Service A	Rule A
Patient	Resource A	Rule B
Nurse	Service A	Rule A
Guest	Resource A	Rule C

(a) Profile based cloud access control list.

Service ID	Services Resources Description
Service A	Patient Monitoring System
Resource A	Data storage

(b) Service and resource list

Profile	Services Resources (*i*)	Rule Dictionary (*j*)
Doctor	*Service A*	Rule A
Patient	*Service A*	Rule B
Nurse	*Service A*	Rule A
Guest	*Service A*	Rule C

(c) Access Control List for Service *A*

Profile	Privileges				Deployment Model	
	C	U	R	D	Public	Private
Doctor	Y	Y	Y	Y	Allow	Allow
Patient	Y	Y	Y	N	Deny	Allow
Nurse	N	Y	Y	N	Allow	Allow
Guest	N	N	Y	N	Allow	Deny

(d) Rule A^{th} Dictionary

Figure 3-4 presenting the rofile-based Access Control List

The entries for services and resources are shown in Figure 3-4b. All new services and resources offered in the cloud will be added to this list. Figure 3-4c shows the entries for access rights defined for each profile along with the respective rules for Service A. Finally the rules and access privileges for each service are defined in the rule dictionary. Figure 3-4d shows the access and privilege entries for *Rule* A^{th}. Traditionally, the access list is maintained as one big list, which increases the complexity of maintaining it. In the proposed solution, we have decomposed the list in different parts. The benefits of such a decomposition is a reduction in management and administration cost. This decomposed version is also easier to implement in a cloud computing environment where rules can be offered as a service.

In summary we presented a new profile based access control system. The solution is proposed at the security layer of the cloud computing architecture. The management of

ACL requires less administrative effort as compared to traditional solutions. The profile management and rule assignment is less complex when compared with Iqbal at el. [18]. In addition, our solution offers reduced data access time and cost as service provisioning is done only when the user is authenticated at the gateway router. In addition, considering the hierarchical organizational structure of the health care system, the profile based access control approach best fits its requirements. In the next chapter, we present simulation results to support these claims.

4 Evaluation Results and Discussion

In this chapter, we present simulation results of our solution. The system performance has been tested in a simulation environment and the results are compared with the architecture introduced by Iqbal et al [18]. The results show that proposed solution fulfills its intended use and project objectives.

4.1 Simulation Environment

To validate the performance of our solution, we have used an agent-based modeling approach to model the system components and verify the performance parameters. There are no standard or common simulators available to simulate the cloud computing environment. To validate, we have simulated our solution in the NetLogo simulator [43]. NetLogo is an integrated multi agent finite modeling environment simulator. It offers modeling and simulation of various dynamic models in the multi agent technology, which allows simulating various aspects of system dynamics. The NetLogo agents operate independently of each other in the environment called the "world". Each agent maintains a state (i.e. state variables and their values) which is initialized when the model is simulated. The agents that have a common set of state variables form a set called breed. There are four important types of agents:

1. *Turtles*: Turtles are the agents that move over the grid defined in the model.
2. *Patches*: Patches are stationary agents and are arranged in a grid form in the "*world*". Patches are used to define the operating region (two dimensional square patch) within which agents can operate and interact with each other.

3. *Links*: Links are basically used to connect two turtles. NetLogo provides directed and undirected links between agents.
4. *Observer*: the observer is a special kind of agent, which oversees the whole operation performed by turtles, patches and links. In addition, it can perform additional operations that other agents cannot perform.

As described above, agents in NetLogo can operate independently, thus their behavior is based on the activities and rules defined for them. To model our system, we define agents randomly for each profile (i.e., patient, doctor and nurse) as breeds of "turtles" along with their access attributes models. Turtle's access rights are derived from rules dictionary enforced by a cloud operator (in our case an observer agent). The agents are defined in breeds as each breed shares the same attributes and follow the same set of rules. Services and resources are also modeled as turtles (agents), and their access rights are defined as agent attributes. All agents, i.e. profile, services and resources are controlled by the observer agent. Links are used to establish the communication among agents, i.e. links are automatically established between the nodes which are allowed to communicate with each other. In a real world scenario, when users are authenticated, they will be authenticated for all the services that are made available under their profile.

The access to services and resources is based on access rules defined by the administrator for each profile. In our simulation access rules are enforced by the observer agent who verifies the attribute of profiles (agents) and allows the establishment of links between service and resource agents.

To verify the behavior of the agents, we have adopted the behavior model. The behavior model is a software tool integrated with NetLogo that enables experiments with models to identify the possible model behaviors and determine which combinations of settings cause the behaviors of interest.

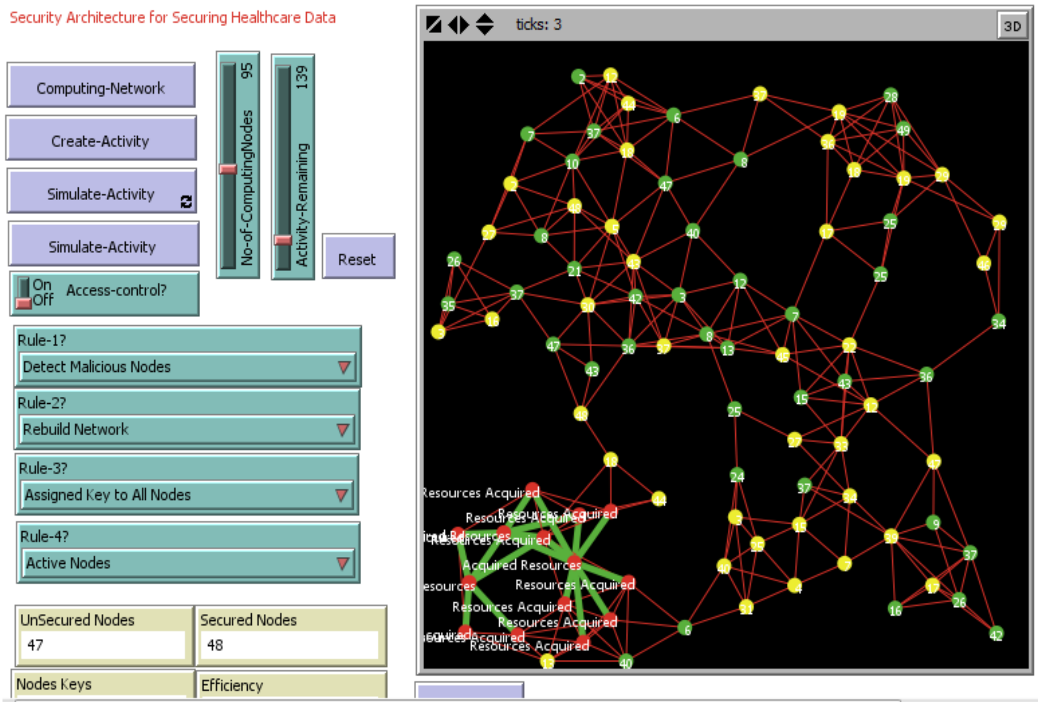
4.2 Simulation Results and Discussion

To the best of our knowledge, there are no common performance parameters defined to evaluate an access control system for cloud environments. NIST provides guidelines for qualitative and quantitative assessment of access control system designed for complex systems. To validate the performance of our solution, we analyzed and compared our solution with the existing solution presented in Iqbal et al. [18] and have evaluated our solution based on the quantitative performance parameters defined by NIST in [17].

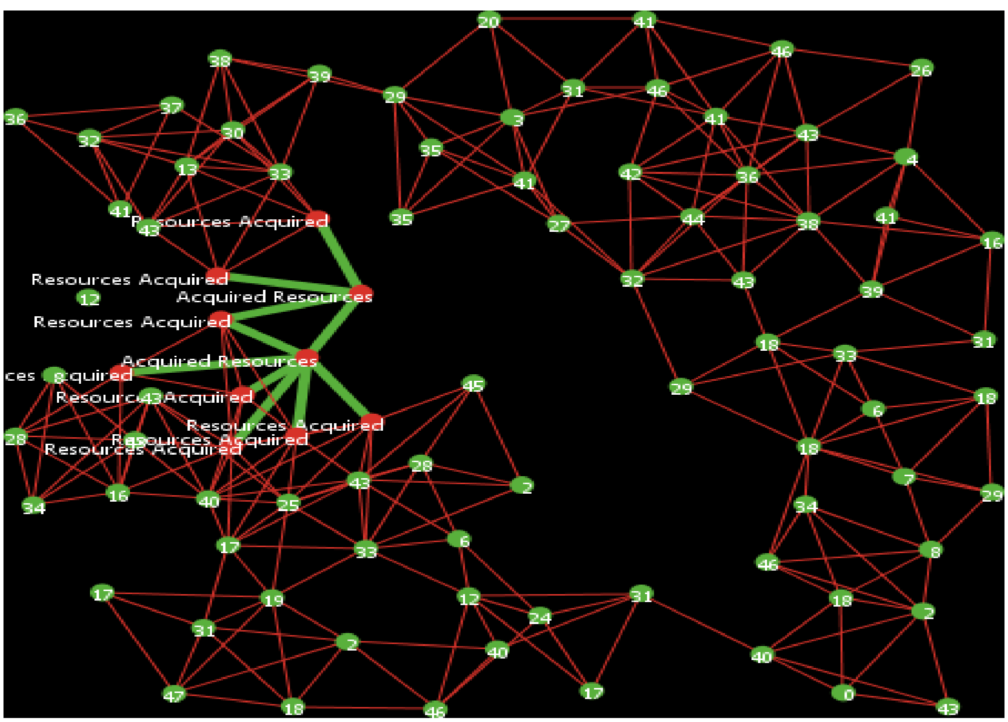
Simulation Parameters		
Number of Nodes.	180	
Observer Node, act as cloud operator that control the network	1	
Simulation Model:	Behavior Model	
Simulation Region i.e. size of World	Random i.e. pixel per *x* and *y* coordinates respectively (random-pxcor random-pycor) pxcor and pycor).	
Simulation Device	Intel i5 Core	2.50GHz
	Process cores	2 x 2.50GHz
	RAM	6 GB
	OS	Windows 7 64 bits

Table 4-1 Simulation Parameter set in NetLogo

Simulation parameters are presented in Table 4-1. Figure 4-1a shows the simulation "Dashboard" while the "World" view of the cloud computing environment is shown in Figure 4-1b. Next, we present the evaluation results for profile-based access control system along with its comparison with intelligent access control system [18]. To compare both the systems, we simulated our experiment with the same experiment parameters and simulation settings (data set provided by the authors) as of Iqbal et al. [18].



(a).Simulation Dashboard



(b) World view of the cloud computing environment

Figure 4-1 Simulation Dashboard and World View of Cloud Environment

4.2.1 System Response Time

Response time is one of the important performance parameters defined by NIST. In this experiment, we tried to simulate our system to find out what would be the response of granting access to the user, and how the system performs when the number of transactions (requests from the users) increases over time. All the nodes (turtles) communicate with the observer node to get access to services and resources (other turtles in the network). The observer validates the access request and the node which initiated the request can now establish the link with the allowed nodes. In the real world environment, this will be performed when the cloud operator will receive an access request from its users and after the profile is authenticated; the server will grant access for the user to all services and resources that the profile has access to. The access policy is defined by the administrator of the cloud service provider as discussed in Chapter 3.

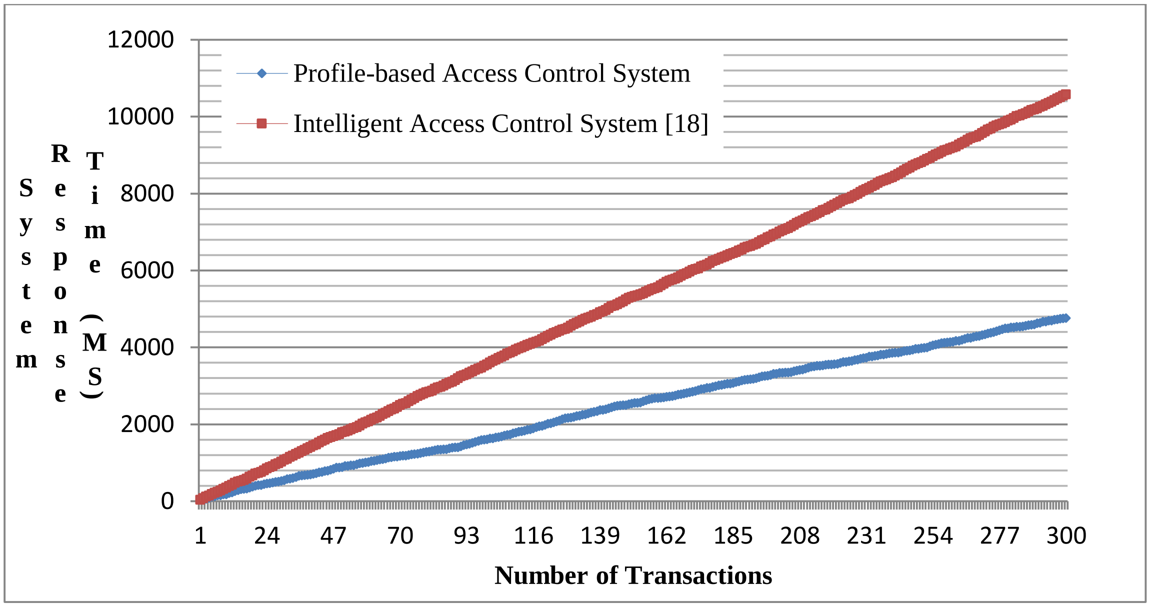


Figure 4-2 Comparison of system response time per transaction

To evaluate the response time of our system, we simulated the system for 300 transactions. The results of the simulation are presented in Figure 4-2. From the results, we can see the response time of our solution is better as compared to Iqbal et al. [18]. This is due to the use of profile based authentication, and avoiding repetitive authentication requests for granting access to users for all the services. Our system verifies the profile credentials and passes the user's service access token to the profile provisioning service. However, in Iqbal et al. [18], the system verifies the user's credentials and then looks for the user's role in the system. Later based on the roles, the system looks for the access rules that apply to that particular user. The process repeats for all the available services in the cloud environment. In addition, their use of Software ID Tags along with access keys adds an extra task in the authorization and service provisioning process. Hence, in case of authentication and service provisioning response time, our solution is efficient when compared with Iqbal et al. [18].

4.2.2 Service Request and Provisioning Time Delay

The service request & provisioning time delay is identified as one of the important factors to validate the performance of access control system in the NIST guidelines [17]. The evaluation of this performance parameter depends on how efficiently the access control process user requests and grants access to the required services, and how fast users access the services available to them. In our previous experiment, we have computed the response time of the profile authentication process. In this experiment, we extended our analysis to find how efficient service provisioning process is once the profile authentication is done. This will ultimately affect the overall performance of the system, i.e. if the delay in service provisioning is higher, then it is likely that the system will process fewer user requests. The comparison results of this test are presented in Figure 4-3. It can be seen from the results, that the proposed system has less time delay as compared to Iqbal et al. [18]. The performance of our system is better because users don't have to repeat the authentication process for every service they want to access. Hence service provisioning is much faster than the existing solution.

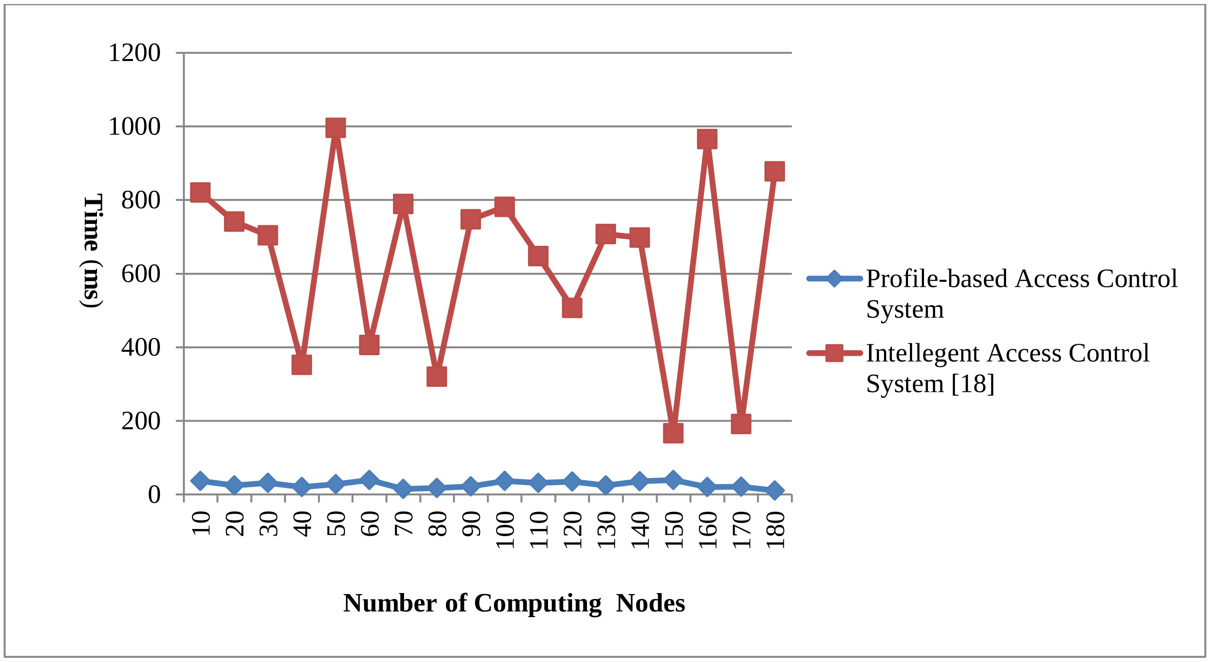


Figure 4-3 Comparison of system access time delay

4.2.3 Communication Overhead

Communication overhead is one of the important performance metrics when analyzing the performance of Internet based systems. In this experiment, we analyze the overall communication overhead for the cloud system. To validate, we have investigated and compared the data packet overhead between the existing and our solution. In our simulation implementation, nodes (turtles) send the message to other nodes in the network (observer and other serving nodes). These messages correspond to real world data packets exchanged between user and application servers, as well as the communication that takes place for user authentication and service provisioning. The results of this test are presented in Figure 4-4. The comparison shows that proposed system has less communication overhead as compared to the system proposed in Iqbal et al. [18].

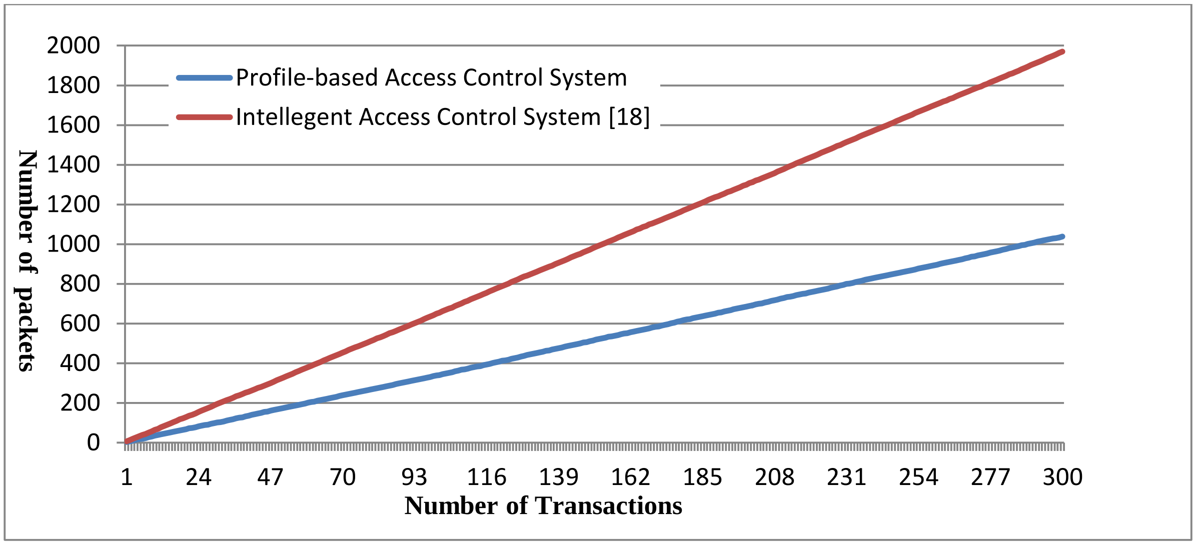


Figure 4-4 Comparison of Data Packet overhead

It can be concluded from the quantitative results presented above that the proposed access control mechanism performs better as compared to its competitor. It is also the case that our system has less overhead when it comes to system policy management and auditing, delegation of administrative capabilities. In the proposed system cloud operators only need to set and modify rules for each profile as compared to traditional system where access rules are defined for each user which increases management and computational overhead. In addition, the system is also scalable as profile authentication can also be offered as a service which will increase the system availability across multiple domains.

5 Conclusion and Future Work

This thesis describes the security challenges in adopting a cloud computing environment for the health care domain. Numerous studies have been reported that advocate the need of improving the traditional security solutions to meet the security requirements of cloud computing technologies. In an effort to improve the security and privacy of Health care system, a profile based access control system is proposed. The proposed system addresses the data security, data availability, integrity, and data privacy issues by presenting an access control mechanism at the security layer of a cloud computing architecture. The proposed system incorporates the concept of profiles to define the access control policy of the user and applications running in the cloud environment. Compared to traditional IPv4 based addresses, in the proposed solution ACL have been extended by incorporating the Profile attribute along with rules for each profile to grant access to services and resources. The structure of the ACL is: Profile (i, j) where Profile is the entity, i is the service or resources and j is the rule dictionary. This approach helps to map the profiles to the applications running on the cloud based on access rules while reducing the number of authentication steps towards accessing and provisioning each service and resource. The most important component of the system is the rules dictionary which is separately stored to avoid any manipulation. This dictionary can also be shared across the network to provide access to users and can be updated when necessary. In addition, the cloud operator can easily implement access rules for each deployment and service model which can improve the security and accessibility of the system across the network and reduce the authentication requests made by a single user.

The proposed solution provides the finer grained access control mechanism to implement security and privacy policies across the cloud network. With a relatively less complex implementation and thus reduced resource requirements our solution can scale well to accommodate multiple service and deployment models. The solution is light weight when compared to its competitors. The management of ACL requires less administrative effort. Simulation results show reduced data access time and efficient service provisioning.

The cloud computing environment offers a dynamic relationship between users and the resource they use. Therefore, designing a dynamic, secure, flexible and scalable access control system is a great challenge, Although our solution does address the security and privacy concerns in the cloud environment, there are still open questions, including but not limited to modeling the profile and individual user, defining different access role for the same profile and user, and interoperability issues while migrating users from one cloud operator to another. We believe that these are all important issues that need to be addressed to improve the overall performance of the system.

Reference

1. Agrawal, R., Abhinav, G., Debjani, S., & Arya, K. B. (2014). Parallelization of industrial process control program based on the technique of differential evolution using multi-threading. Industrial Engineering and Engineering Management (IEEM), 546-550.

2. Ahmed, M., & Hasibuan, Z. A. (2012). E-Government based on cloud environment in indonesia. Seminar Nasional Aplikasi Teknologi informasi . yagyakarta.

3. Almutairi, Abdulrahman A., et al. "A distributed access control architecture for cloud computing." IEEE software 2 (2011): 36-44.

4. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., et al. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

5. Bennett, C. J. Statutory review of the Personal Information Protection and Electronic Document Act (PIPEDA).

6. Berger, S., Cáceres, R., Goldman, K., Pendarakis, D., Perez, R., Rao, J. R., & Valdez, E. (2009). Security for the cloud infrastructure: Trusted virtual data center implementation. IBM Journal of Research and Development, 53(4), 6-1.
7. Borkin, S. (2003). The HIPAA final security standards and ISO/IEC 17799. Collect. Information Security Reading Room.

8. Catteddu, D. (2010). Cloud Computing: benefits, risks and recommendations for information security. Springer.

9. Chen, D., & Zhao, H. (2012). Data security and privacy protection issues in cloud computing. Computer Science and Electronics Engineering (ICCSEE), 1, pp. 647-651.

10. Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., et al. (2009). Controlling data in the cloud: outsourcing computation without outsourcing control. Proceedings of the 2009 ACM workshop on Cloud computing security, (pp. 85-90).

11. Cusumano, M. (2010). Cloud computing and SaaS as new computing platforms. Communications of the ACM, 53(4), 27-29.

12. dos Santos, D. R., Merkle Westphall, C., & Becker Westphall, C. (2014, May). A dynamic risk-based access control architecture for cloud computing. In Network Operations and Management Symposium (NOMS), 2014 IEEE (pp. 1-9). IEEE.
13. Gajanayake, R., Iannella, R., & Sahama, T. (2011). Sharing with care: An information accountability perspective. Internet Computing, IEEE, 15(4), 31-38.

14. Galegher, J., Robert, E. K., & Carmen, E. (2014). Intellectual teamwork: Social and technological foundations of cooperative work. . Psychology Press.
15. Hayes, B. (2008). Cloud computing. Communation ACM, 9–11.
16. Heiser, J. (2009). What you need to know about cloud computing security and compliance, . Gartner, Research, ID Number: G00168345.
17. Hu, Vincent C., and Karen Ann Kent. Guidelines for access control system evaluation metrics. US Department of Commerce, National Institute of Standards and Technology, 2012.
18. Iqbal, M. J., & Muhammad, U. G. (2015, March). Intelligent Cloud Computing Security Framework for Private and Public Clouds. MAGNT Research Report, 3(3), 885-891.
19. Kanoongo, B., Jagani, P., Mehta, P., & Kurup, L. (2014). Exposition of Solutions to Hypervisor Vulnerabilities.
20. Khan, A. R. (2012). Access control in cloud computing environment. ARPN Journal of Engineering and Applied Science, 7(5), 613-615.
21. Kuo, Alex Mu-Hsing. "Opportunities and challenges of cloud computing to improve health care services." Journal of medical Internet research 13.3 (2011).
22. Kuyoro, S., & Ibikunle, F. (2011). Cloud computing security issues and challenges. International Journal of Computer Networks.
23. Li, H., Dai, Y., Tian, L., & Yang, H. (2009). Identity-based authentication for cloud computing. In Cloud computing (pp. 157-166). Springer Berlin Heidelberg.
24. Li, M., Yu, S., Ren, K., & Lou, W. (2010). Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings. In Security and Privacy in Communication Networks (pp. 89-106). Springer Berlin Heidelberg.
25. Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST cloud computing reference architecture. NIST special publication, 500, 292.
26. Lohr, H., Sadeghi, A.-R., & Winandy, M. (2010). Securing the e-health cloud. Proceedings of the 1st ACM International Health Informatics Symposium, (pp. 220-229).
27. Luo, W., Xu, L., Zhan, Z., Zheng, Q., & Xu, S. (2014). Federated Cloud Security Architecture for Secure and Agile Clouds. In High Performance Cloud Auditing and Applications (pp. 169-188). Springer.
28. Luo, X., Yang, L., Hao, D., Liu, F., & Wang, D. (2014). On Data and Virtualization Security Risks and Solutions of Cloud Computing. Journal of Networks, 9(3), 571-581.

29. Maghanathan, N. (2013). Review of access control models for cloud computing. Computer Science & Information Science, 3(1), 77-85.
30. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (draft). NIST special publication, 800(145), 7.
31. Mishra, K. K., Vimal, C., & Michael, G. (2013). Prevention Of Online Password Hacking Process With Secured Multi Authentication Scheme.
32. Nurmi, D., Wolski, R., Grzegorczyk, C., Obertelli, G., Soman, S., Youseff, L., & Zagorodnov, D. (2009, May). The eucalyptus open-source cloud-computing system. In Cluster Computing and the Grid, 2009. CCGRID'09. 9th IEEE/ACM International Symposium on (pp. 124-131). IEEE.
33. Peter, M. & Tim, G. (10 July 2009). The NIST definition of Cloud Computing, Version 15. Information Technology Laboratory. Retrieved from http://www.hexistor.com/blog/bid/36511/The-NIST-Definition-of-Cloud-Computing
34. Punithasurya, K., & Jeba Priya, S. (2012). Analysis of Different Access Control Mechanism in Cloud. International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS, 4(2).
35. Raykova, M., Zhao, H., & Bellovin, S. M. (2012). Privacy enhanced access control for outsourced data sharing. In Financial cryptography and data security (pp. 223-238). Springer Berlin Heidelberg.
36. Robert , P. M. (2009). Software as a Service Market Will Expand Rather than Contract Despite the Economic Crisis. IDC Finds.
37. Schrödl, H., & Turowski, K. (2011). SCOR in the Cloud Potential of Cloud Computing for the Optimization of Supply Chain Management Systems. European, Mediterranean & Middle Eastern Conference on Information Systems. Athens, Greece.
38. Shaikh, F. B., & Haider, S. (2011). Security threats in cloud computing. Internet technology and secured transactions (ICITST), 2011 international conference for, (pp. 214-219).
39. Shirey, R. "RFC 4949–Internet Security Glossary." (2007)
40. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.
41. Sultan, Nabil. "Making use of cloud computing for healthcare provision: Opportunities and challenges." International Journal of Information Management 34.2 (2014): 177-184.
42. Tsai, W., Jin, Z., & Bai, X. (2009). Internetware computing: issues and perspective. In: Proceedings of the first Asia-Pacific symposium on Internetware., 1–10.

43. Wilensky, U. (1999). http://ccl.northwestern.edu/netlogo/. Retrieved 05 28, 2014, from http://ccl.northwestern.edu/netlogo/: http://ccl.northwestern.edu/netlogo/

44. Wilkowska, W., & Ziefle, M. (2011). Perception of privacy and security for acceptance of E-health technologies: Exploratory analysis for diverse user groups. Pervasive Computing Technologies for Healthcare (PervasiveHealth), 2011 5th International Conference on, (pp. 593-600).