Cloud MA-MOrBAC: A Cloud Distributed Access Control Model Based on Mobile Agents

Zeineb Ben Yahya, Farah Barika Ktata, Khaled Ghedira
National School of Computer Science of Tunisia (ENSI)
University of Manouba
Tunisia
{zeineb.benyahya@ensi-uma.tn} {farah.ktata@gmail.com} {khaled.ghedira@isg.rnu.tn}

ABSTRACT: *Cloud services are designed to provide scalable access to applications, resources and services, and are fully managed by cloud service providers. On-demand cost-effective services are offered such as software as a service, infrastructure as a service and platform as a service. Despite the promising facilities and benefits of these services, most organizations and companies are worried about accepting to use them due to security issues and challenges within the cloud like data security, abuse of cloud services, malicious insiders and cyber-attacks. In order to fulfill organization data security requirements, protect organization assets and win the trust of cloud service consumers, models should be designed to solve organizational and distributed aspects of information usage stored in a cloud and to protect them against unauthorized access and modification. However, various access control models have been developed such as: role-based models, attribute-based encryption models and multi-tenancy models. In spite of such model diversity, cloud dynamic and distributed access control requirements may not be fulfilled, for several reasons: (i) the user-resource relationship is dynamic in the cloud. (ii) Service providers and users are typically not in the same security domain. (iii) The multi-tenant hosting and heterogeneity of security policies. In this paper, a novel access control model using the technology of mobile agents for cloud computing is presented to meet the distributed access control requirements. It aims to protect the sensitive data of cloud service consumers, to guarantee the availability of cloud service providers' as well as the confidentiality and integrity of costumers' data and to secure sharing resources.*

Keywords: Cloud Computing Security, Cloud Service Provider, Distributed Access Control Models, Mobile Agents

Received: 14 June 2019, Revised 7 November 2019, Accepted 25 November 2019

DOI: 10.6025/ijwa/2020/12/1/1-15

1. Introduction

A cloud service provider is a company that offers an increasing variety of services of cloud computing, typically infrastructure as a service, software as a service and platform as a service, to other businesses or individuals. Some cloud service providers have differentiated themselves by tailoring their offerings to vertical market requirements. Their cloud-based services might seek to

deliver industry-specific functionalities or help users meet certain regulatory requirements. For instance, several healthcare companies have been maintained to consider migrating healthcare data from their own storage to the cloud, where healthcare providers store, maintain and back up personal health information. The cloud service market presents a range of providers, but three public cloud companies have established themselves as dominant forces: Amazon Web Services, Microsoft and Google.

There is a number of things to think about when Cloud Service Customers (CSCs) evaluate Cloud Service Providers (CSPs). Security in this context is an important consideration. Organizations like the Cloud Security Alliance (CSA) offer certification to cloud providers that meet their criteria. The CSA's Trusted Cloud Initiative program was created to help CSPs develop industry-recommended, secure and interoperable identity, access and compliance management configurations and practices (CSA, 2011).

However, CSCs (individuals or organizations) are worried about cloud storage security. Reasons for these doubts include reports of security breaches among even popular CSPs. Equally, they do not completely guarantee the availability, confidentiality and integrity of customers' data.

Due to cloud environment deployment characteristics, such as multi-tenancy nature and sensitive data outsourcing, critical applications and infrastructure in the cloud are bothersome. Organizations and individuals are very anxious about how security can be guaranteed in a cloud environment. Moreover, companies and individuals have strong constraints on hosting their sensitive data and critical applications on clouds. Thus, the biggest challenge in cloud computing is to successfully address the security issues associated with their deployment (Safiriyu E, 2011)(Xuan Zhang, 2010), and to provide evidence to their customers that their data are safe.

With the increasing number of distributed applications and users, cloud computing attacks are also increased. The most predominant attacks on the cloud are (Y.G.Min, 2012):

- Distributed Denial of Service (DDoS) or DoS attacks
- Side channel attacks
- Man-in-the cloud attacks
- Man-in- the middle cryptographic attacks
- Authentication attacks

To avoid this kind of attacks', a better security policy in cloud computing is needed. In this context, access control is generally a policy or procedure that allows, denies or restricts access to a system (A.R.Khan, 2012). It may, as well, monitor and record all attempts made to access a system. Access control may also identify users attempting to access an unauthorized system. It is a mechanism which is very important for protection in computer security.

The fundamental goal of any access control system is restricting a user to exactly what they 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 are derived from either a policy or a set of policies.

In this context, CSPs need a strengthened access control system for controlling admission to their resources with the ability to precisely monitor who accesses them. They should have the ability to deal with dynamic and random behaviors of cloud consumers, as well heterogeneity and diversity of services. Therefore, CSPs should provide the following basic functionalities from the perspective of access control:

- Control access to the service features of the cloud based on the specified policies and the level of service purchased by the customer.
- Control access to consumer's data from other consumers in multi-tenant environments.
- Control access to both regular user functions and privileged administrative functions.
- Maintaining accurate access control policy and updating user profile information.

Subsequently, in order to prevent critical access control issues and to alleviate security fears, many techniques for access

control in cloud computing have been suggested. The literature in this area shows a variety of these approaches There are three broad categories of access control models for cloud computing: (1) role-based models; (2) attribute-based encryption models and (3) multi-tenancy models.

Despite the richness, range and diversity of access control models proposed, as well as the efforts of researchers in this area all over the last few years, the problems of access control in cloud computing are becoming more complex, due to the diverse set of users with different sets of security requirements and cloud environment deployment characteristics. Future research directions in this area should turn towards developing effective access control models for cloud computing environments, able to secure data access and to solve problems related to access control in this kind of environments, such as the automatic evaluation and interrogation of distributed policies, and the modeling and cooperation of policies organized according to different models.

For this, we propose in this paper a new solution based on a mobile agent paradigm and on an MA-MOrBAC (Z.BenYahya, 2017) model to offer secure and performant distributed access control. It is worth mentioning that the mobile agent (J.Ferber, 1999) paradigm has an ever-growing impact on information sharing between systems. They have proved to be very useful in the heterogeneous and interoperable context for helping to solve collaborating issues that can arise when we try to connect different organizations or collaborative sessions and workflow interactions in the cloud.

Knowing that, applying well managed access control, a CSP can ease sensitive data sharing and reduce the number of incidents of data breaches, which can result from unauthorized access. For this, our model takes benefit from the mobility aspect of agents as a communication entity between CSPs and costumers, which is beneficial for reducing the traffic on the network and the amount of the information exchanged, in order to improve classical access control models. Additionally, using a mobile agent paradigm able to reinforce the trust between CSPs and costumers makes also use of cryptographic mechanisms, such as encryption and digital signatures to ensure authentication, identification, confidentiality and integrity.

For this, the remainder of the paper is organized as follows. Section 2 provides a survey of cloud access control threats and challenges. It also illustrates an in-depth analysis of the fundamental access control requirements around cloud computing. In section 3, we present a review about conventional access control models and why they cannot be deployed in the cloud. It provides as well a critical analysis of various access control approaches utilized in the cloud so far. Through section 4, we present an overview of our suggested approach, their components and operations. Moreover, a detailed example that aims to clarify the contributions and the functioning of our proposed model is presented in this section, with a further discussion on benefits and shortcomings of our approach detailed in section 5. Finally, we present ideas for future work based on our experience, with a conclusion of the paper, in Section 6.

2. Access Control Challenges around Cloud Computing

2.1 Distributed Access Control in Cloud Computing

In cloud computing, access control (Zhuo Tang, 2010) is a necessary condition for a variety of services to work together and implement a distributed environment. It is a mechanism that limits the actions or operation that a legitimate user of a computer system can perform. In open service-oriented systems, users access to various resources and services after the verification of their identity. The access context is to determine what a user can do directly around an object. It can be considered as the major center of computer security gravity. Compared to traditional systems, the cloud computing is much more dynamic and distributed, and security for such an environment poses many challenges. Therefore, access control in distributed environments is required to cross the borders of security domains, to be implemented between heterogeneous systems.

Hence, the main goal of any access control system is to control which entities (persons, processes, machines ...) have access to which resources in the system, which files they can read, which programs they can execute, and how they share data with otherentities (R. S. Sandhu,1994). Cloud computing is a shared open environment, which has its own characteristics and features such as on-demand services and mobility. Thus, considering the importance of security and privacy of cloud costumers' resources, CSPs need 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 behaviors of cloud consumers, heterogeneity and diversity of services. In this section, we present a detailed access control requirements analysis for cloud computing, which identifies important gaps not fulfilled by conventional access control models.

2.2 Needs of Highlevel Access Control for Cloud Computing

Security issues in cloud computing are difficult to address, given the diverseness of users, data, and servers. Furthermore, with the dynamic technological change, protecting data is very challenging that an organization or group of organizations are often called to collaborate with other organizations in order to benefit or provide services, to communicate, to access and to deliver information. With respect to the new vision of computing, new technologies in heterogeneous systems as cloud computing are often used for collaborative services, where a lot of customers work together to accomplish a task. An access control model in cloud computing is a necessary condition for a variety of services to work together and implement cooperative environments. It must provide a secure shared-task structure for users who share permissions for collaborative needs.

In this context, cloud computing may suffer from security attacks conventional distributed systems such as malicious codes (Viruses, Trojan Horses), Man-in-the-middle attacks, DDOS attack (Wang Z, 2011), abuse and nefarious use of cloud computing, and malicious insiders (Dan Hubbard and Michael(Dan Hubbard W, 2012). Consequently, cloud services could be inaccessible due to these attacks and generate a negative impact. As a result, it is an important and primary requirement for CSPs to ensure that its services are fully usable and available at all times (Wang C, 2009). Moreover, cloud computing has brought new concerns such as moving resources and storing data in the cloud with the probability to reside in another country, which has different regulations. Furthermore, cloud computing is a shared environment, which uses shared 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 S, 2010). Furthermore, virtualization brings its own issues such as data leakage (Lombardi F, 2010). In general, 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 have a more precise idea in this context, we do an in-depth analysis on cloud security and identifying different security requirements for multiple CSCs. Access control is one of the common and fundamental requirements for all types of cloud users, so it is necessary to ameliorate access control models.

The underlying desire to improve the access control in all information systems is to propose the right structure to translate to a better security policy. These policies are expressed in natural language at the beginning of the development cycle of an access control model. The rules of these policies must then be expressed through access control models that are (R. S. Sandhu, 1994):

- Sufficiently expressive, to allow the expression of security complex rules and faithfully represent the structure and operation of a system
- Decidable, able to evaluate permissions from security rules.
- Easily administrated, to provide a set of primitive features and simplify the activities of administrators.

The concepts of constraints and security properties have been studied to add meaning to access control policies. The purpose is to enable organizations to express the specificities of their services through rules and restrictions which access control policies must meet. The current needs of administrators are to verify access control policies so as to ensure that one policy is secure, equivalent to another, that it instantiates a model, or that it meets security properties. In this context, tools that automate the analysis and verification of security policies are needed and research should make it possible to provide elements of answer to the most current issues on access control: automatic policy repair, interrogation of distributed policies, modeling of administrators' rights, or cooperation of policies organized according to different models.

In the next section, we will focus on the following two broad categories of access control models for cloud computing: (1) distributed access control models, and (2) distributed access control models based on a mobile agent paradigm. We will review the existing literature on each of the above access control models and their variants (technical approaches, characteristics, applicability, pros and cons).

3. Review of Access Control Models for Cloud Computing

In order to provide an ideal and secure environment to facilitate sharing data and services, and to improve collaborative work quality, several access control models have been proposed. In this section a presentation of the two main categories of these models is illustrated: distributed access control models and distributed access control models based on mobile agents for cloud computing.

3.1. Distributed Access Control Models for Cloud Computing

According to the literature, distributed access control is the access control applied in the field of distributed, cooperative and collaborative environments, such as cloud computing, where various users access to data and services with different access rights. Due to the increasing number distributed applications, the need for a high level of distributed access control has become vital for academic and industrial environments. Researchers in this area should be able to solve problems related to access control in each kind of environments.

During this part, we present some research activities in this area, by analyzing the work carried out by researchers;

RBAC(Role Based Access Control) (Kuhn, D, 1992)

David Ferrailo and Richard Kuln put forward an RBAC model in 1992, they considered the it as an alternative approach to DAC and MAC models, which reduces the access control management complexity. It is suitable for a fixed and fairly hierarchical structure of organizations. It has a lot of advantages compared to, DAC and MAC models. Yet it has its own difficulties and problems when it is deployed in the real-world (Suhendra V, 2011). Roles in the RBAC model classify subjects in a number of categories, so each subject has to have a role in order to access the system. Nevertheless, it does not support the delegation principle, which is needed in organizations for dealing with absences of their staff. Furthermore, it does not consider the time and location constraints, which are utilized for restricting access to system files and decreasing the probability of information leakage. It also fails to cope with dynamic and random behaviors of users. Before utilizing the RBAC in cloud computing, it has to ensure access decisions in a reasonable time and according to system requirements. For example, the response time is crucial in many applications such as the health care system. A consultant away from a hospital needs to access the system in a timely manner, disregarding a number of access requests to the RBAC model. In addition, any critical infrastructure service provider who aims to migrate to the cloud, with thousands of users, hundreds of roles and millions of permissions, faces a tremendous task that cannot realistically be centralized by a small team of security administrators (Munawer Q, 2000).

3.2. Distributed Access Control Models based on Mobile Agents for Cloud Computing

A suitable distribution of an application requires prior knowledge on its evolution, allowing the fairly fine modeling of the application. In most cases, this knowledge is very expensive or impossible. For this, the question of the code mobility has been studied to deal with these problems. This has been done in order to improve the efficiency of the system by providing loading capabilities, and also to permit dynamic reconfiguration of the system. The multiplicity and complexity of physically distributed problems and the important need to resolve them in a timely manner and an efficient way, place the mobile agent paradigm among the most insightful solutions.

Over the last decade a number of researchers have used agents in their work, which in theory could provide some basic levels of computer and network defense that could be applied to the cloud computing security. In this context, researchers in field of access control have been interested using the mobile agent technology to improve the existing distributed access control models. Some of research work in this area is described below.

In (Shantanu Pal, 2012), Shantanu & al. put forward a cloud security two-tier framework based on a collaborative agent and a trust model to protect cloud resources by monitoring the unauthorized access. They propounded a novel trust model to assure the trustworthiness of the system by calculating a current or updated trust degree for each user service request and the domain from where the request was coming. In their model, a proxy server was used as a communication channel between two domains, to authenticate each service request and to deliver the response to the service user. In the two levels, cloud users and providers, two agents were utilized to calculate and update the user and domain trust degree via the trust function (Florina Almenarez,2004). They also maintained their databases and user activities. As a consequence, only the users who have a trust degree greater than a threshold trust could access and get the information from CSPs. On the other hand, a malicious user could not have any access and they would be removed from its domain. This model had a major advantage that the domain would remain unaffected by non-trusted users. However, this model suffered from some weaknesses, because it increased some workload of domains and it failed to prevent malicious activity without the CSP information about user activities. Besides, the proxy server presented a weak point. If it crashed, the users could not communicate with the CSPs.

In (Priyank.s, 2011)Priyank& a. suggested a trust model agent based technique for cloud architecture. Mobile agents were used as security agents to collect information from the virtual machines in order to help the user and the service provider keep track of the privacy of their data and virtual machines. These agents monitored virtual machines integrity and authenticity. Security agents could circulate and migrate in the network, and replicate and perform the assigned tasks for monitoring of virtual machines.

Mobile agents are introduced at multiple levels in the cloud infrastructure in order to monitor the resources utilization and minimize security threats. They also used security agents to build a strong trust between cloud users and cloud providers. However, they ignored the user identification, the identity management, and the security of the agents themselves.

In (Alwesabi, A.,2014), the authors propounded a multi agent system framework. It was presented as a two-layer framework: a virtual server composed by a set of agents to intercept the users request, and a cloud layer also containing a set of agents to perform the requested service in the cloud, each agent had a specific task to do. They used a mobile agent as a communication entity between the two layers, which was beneficial for reducing the traffic on the network and the amount of the information exchanged. They presented their methods as a multi agent system cooperating to achieve a global goal, which was the satisfaction of a user's service request, but they did not clarify how the security of the system was maintained.

In (Alwesabi Ali,2013), the implementation of the cloud computing approach based on mobile agents was proposed as a new approach that used mobile agents in cloud computing. Its architecture was based on mobile agents that kept the goal of secure communication in cloud computing. Different layer were utilized. At each layer, different agents were used for processing the services. The mediation layer had two agents: mediator and analyzer. The role of mediator agents was to act as a mediator between the interface layer and the mediation one. This would generate mobile agents to process the service requested from the user. The analyzer agents would communicate with the mediator agent and analyze the request of the user. At the interface layer, the interface agent is responsible only for sending information from the user to the appropriate agents and stores this data in the database.

At the mobile agent layer, transfer agents are mobile and they are generated at the mediation layer. They sent data to the mediator and analyzer agents. Finally, at the cloud layer, the role of security agents was to maintain the security at the cloud. Added to that, the executor agents executed the service requested from user. They were local agents at the cloud, it is responsible for responding to requests from mobile agents arriving at their cloud computing.

3.3. Analysis and Discussion

Recently several authors have dedicated their research for an ideal access control model proposal and development. Consequently, several efficient models have been suggested to provide and improve security and access control in collaborative and cooperative systems. Despite the diversity and wealth of those models, almost all of them have tried to achieve the highest security level. However, with distributed computing and efficient storage and collaboration technologies that make sharing and diffusion of system resources easier, security problems are much more complex in this kind of systems compared with the traditional environment. Some of these include communication, authentication, authorization, data integrity, data privacy and sharing, heterogeneous environments, distributed management, consistency of time, reliability, availability, parallel execution, and graceful degradation.

A key limitation of these researches is that they do not address the problem of meeting the exigencies of communication and collaboration security difficulties encountered between or within organizations having distributed computing infrastructures where a large number of computers are connected together by a network. Furthermore, most of the proposed security solutions do not offer a mechanism to detect the security policy violation and do not suggest any decision to be taken in such a case. Moreover, they do not put forward any technique to secure interactions in a collaborative session between all stakeholders of heterogeneous environments. Besides, the consistency of the security policy is not checked. Additionally, in a cloud environment, where CSPs are just partially trusted, we need to satisfy the following requirements:

- Data privacy. The privacy of Cloud service customers (CSCs) must be protected when uploaded to CSP. Suitable encryption schemes are desired.

- Fine-grained access control. A CSCs owner should be able to enforce access policies so that different users will have various access privileges to shared resources.

- Efficient access control management. The access control scheme should also be efficient in terms of computational and distribution overhead.

- Prevention of improper resources access by users with multiple roles. The problem of improper resources access must be taken care of.

For this, we believe that a proper solution for the access control issue in distributed environments needs extensive research, especially in the organizational conflict management of access control policies. In a heterogeneous cloud computing environment, it is very important to ensure the two cloud issues: the first issue is, the security of data communication, because data and software are stored, accessed and run on machines that are not owned or directly managed by their owners. The second issue, is the trust between CSPs and CSCs. The agent's technology offers various solutions to cloud vulnerabilities, such as: control access and authentication, distributed trust management, audit and intrusion detection, attack vector pursuit, and diagnostic and system restoration. Autonomous agents can make clouds smarter in the interaction with users and more efficient in allocating processing, resources and storage to applications and users. In clouds, there is a veritable need to design and implement techniques that can monitor the dynamic behaviors and change the configurations and heterogeneity of cloud computing environments. Autonomic techniques as multi agent systems seem to be suitable for providing a promising approach to addressing this requirement. For these reasons, a new access control model based on mobile agents is proposed in this paper. In the following, we will describe this suggested approach.

4. Proposed Model

In this section we will first present the objectives of the proposed system and its overall architecture. Then we will highlight its two main layers and overall functioning.

4.1. Objectives of Proposed Model

Owing to the cloud computing properties and agent based system benefits and characteristics, as well as the advantages of an agent based approach, we consider that it will be an efficient and secure approach to exploit the paradigms of mobile agents, so that the access requests of cloud customers can be mediated through the agents.

Based on our previous MA-MOrBAC (Z. Ben Yahya, 2017) access control model suggested for multi-organization systems and environments, we propose "Cloud MA-MOrBAC» which is an MA-MOrBAC enhancement that involves a multi-level access control mechanism having a lot of entities and using multi-agents architecture able to manage various security policies, It also provides an overall level of homogeneous and sufficient security and guarantees the coherence between access control policies associated with several cloud computing actors.

In this context, in our proposed model, the collaboration and interaction between CSCs and CSPs are made by the mobile agent technology, which provides platform-independent protocols and standards for exchanging heterogeneous interoperable data services. Software applications written in various programming languages and running on many platforms can use mobile agents to exchange data over computer networks in a manner similar to inter-process communication on a single computer. In the suggested model, we integrate the mobile agent technology to achieve these objectives:

- Ensuring the consistency of different access control policies
- Handling multiple security policies and improving the detection of violation of security policies.
- Providing the authentication, integrity and confidentiality of data exchanged in a cloud environment
- Providing secure interactions with a high level of confidence
- Protecting the user's sensitive information from other internal or external users and hackers
- Detecting policy breaches, where the users are notified in order to take necessary actions when malicious access or a malicious activity occurs
- Securing data storage in the cloud to provide better protection of shared data.

4.2. Our Proposed Framework Architecture

Our suggested model has a hierarchical structure that is composed of two layers; CSPs and CSCs as shown in the figure 1.

The proposed model relies on a set of agents ensuring secure data sharing and interactions in a collaborative session between different cloud computing stakeholders, which are done by agent's mobility. A set of agents is used in the suggested architecture and is described in the following with their functions:

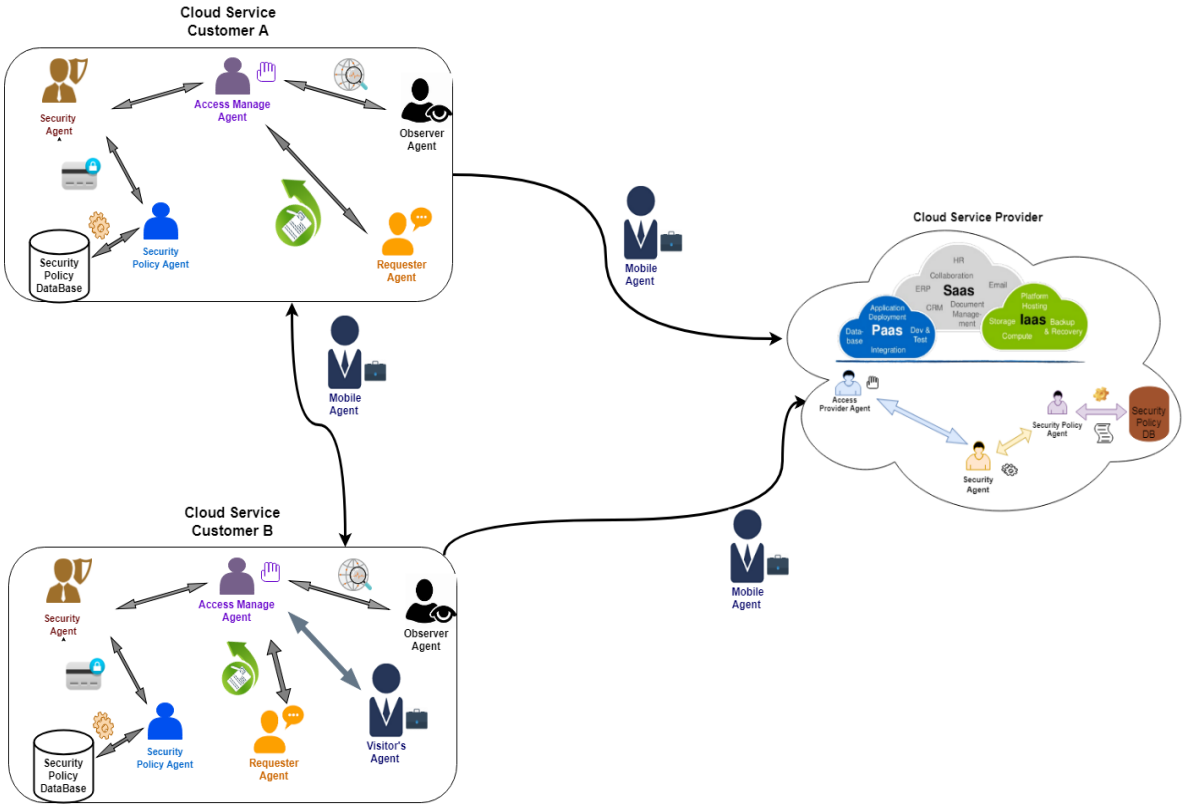

Figure 1. Cloud MA-MOrBAC model

4.2.1. Access Manager Agent: It is the responsible agent and the access manager. This agent is responsible equally for managing agents of the CSCs' platform: It is responsible for creating, activating and sending agents.

4.2.2. Security Policy Agent: It is the agent responsible of policies and security rules management and updating, in CSCs and CSPs platforms'. It provides control according to a security rule database. Knowing that a rule can be a permission, prohibition, recommendation or obligation, the security policy agent is the one who will grant or reject an access request by checking the security policy contained in different formats (database, XML file) and generates an evidence of authorization (table 1), in order to guarantee its identification at the external place.

It also ensures security policies consistency (e.g., political security rules are contradictory: One action is both permitted by one rule and prohibited by another and security policies fusion problem management (the definition of compatible organizational roles and structures, the detection of conflicts in the policy obtained by fusion, and the proposal of a method for solving these conflicts).

4.2.3. Requester Agent/Mobile Agent: It is the agent that gives a graphical interface and helps users to interact with the CSPs system. It is also responsible for receiving and interpreting access users' queries and preparing and submitting responses to the requester (user, organization). It treats the queries of requesters, shows it the information about the treatment of the request, follows the execution process of the request and visualizes responses in the format required by the requester. Equally, it is used as a communication channel between domains and a manager for sending and receiving a consumer's request to and from CSP.

4.2.4. Security Agent: It performs the verification and authentication of the agent requester to ensure its integrity. In fact, a process of a sharing key is running between the two "Security Agents" of both cloud services frameworks. This allows it to obtain a common shared key. It is a key of 256 bits introduced in an encryption process between both sides, using the crypto-graphic algorithm, AES (NIS T, 2001). It is responsible for checking the authentication of each user and their credentials.

Parameters	Description
Subject login	Identifies the subjects that are sending the access requests (organization or simple CSC).
Access Rights Ticket	Contain details of access rights affected to the mobile agent “Requester Agent” (permissions, obligation, recommendation and prohibition) to do a local or remote mission.
Task	Contains the description of the different tasks to be performed by “Requester Agent” in different CSPs.
Agent ID	Used to identify the visitor agent “Requester Agent” in several CSPs they can visit during their mission.
Access Request level	Represents the emergency level of the access request (non-emergency =0 ; emergency= 1)
Action Deadline	Represents task execution duration. Once this duration expires the mobile agent “Requester Agent” returns to its home place with the obtained results.
Mobile agent migrated certificate	The security agent in each CSCs system generates a digital certificate for the mobile agent before it is in order to facilitate their identification and authentication at the remote systems (Cloud service providers) since it only accepts agents that fall into their circle of trust.

Table 1. Evidence of Authorization

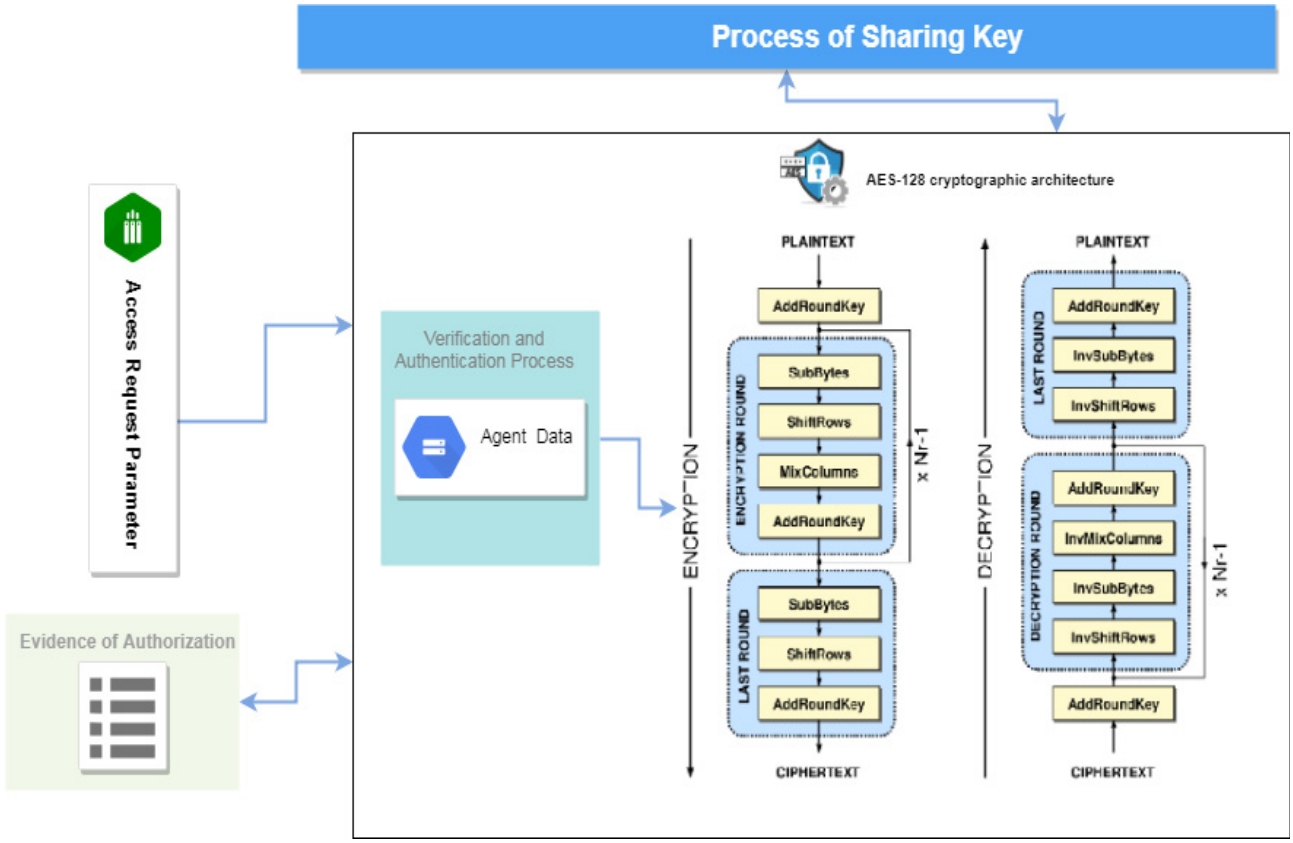

Figure 2. Security Agent Architecture

4.2.5. Observer Agent: It is responsible for sending procedures (dispatching) of the agent. It is also responsible for managing and monitoring the changes in the network. Moreover, it reports all events of network occurrences and periodically transmits them to the Access Manager Agent. It is an agent that is responsible for automatic notifications of organizations across platforms. It can send a notification to the requester (CSCs) at the time the recipient CSPs agree to process the request. This notification is useful for tracking the mobile agent. It is also responsible for creating the communication channel between the two layers by activating a mobile agent and sending it to the CSP site.

4.2.6. Access Provider Agent: It is head of information access commission for CSPs. It is the manager of resource access and personal document protection of CSCs. Its functions are as follows: it is responsible for acquiring CSC's requests (Mobile Agent). It communicates with the Security Agent to verify the Mobile Agent's authentication and the trust degree.

In our proposed model, the CSP gathers a set of agents such as access provider agents security policy agent and security agent, acting to achieve the global goal which is satisfying a customer's service request. Access Provider Agent accept service requests from customers (Mobile Agents) dynamically and communicate with the Security Agent to check the Mobile Agent's authentication and the trust degree. In doing so, and since the mobile agent has been accepted, an authentication process will be launched again, to prevent against the fact mobile agent's behaviors are changed during its mission. Then it composes a collection of resources to satisfy customers' requirements.

In a CSP, when a mobile agent (Requester Agent) arrives, the Security Agent decrypts it and checks the mobile agent identity by the usage of the Shared Key (Diffie-hellman, AES256). Thereafter, the Security agent negotiates with the Security Policy Agent in order to verify the mobile agent's evidence of authorization to define which permissions will be granted to the visitor agent according to the access control policy.

Depending on the type of request, the external access control needs an approval from an internal member (Security Policy Agent) of the CSP, in order to process the request. In such cases, the Security Agent provides to the visitor Agent an identification number that can be used later to query the status of its requirement. This identification number improves the visitor Agent flexibility since this mobile agent can continue its itinerary to other external resource providers and return later to consult the request status.

5. Use Case

To illustrate how the proposed model can be mapped to real-world use cases, we utilize example applied to the healthcare domain. The amount of Health data is quickly increasing, imposing great challenges on hospital archive infrastructures, which must ensure high data availability, security and regularity. Electronic Health Records are a preferred method to store patients' health records. In this context, a cloud-based solution can help address these challenges.

The emergence of cloud computing services provides users with flexible access, large storage capability and low costs, which motivate Health records maintainers to consider migrating Health data from their own storage to the cloud, knowing that archiving in the cloud helps simplify the data management and hospital archive infrastructure. Through our proposed approach, a secure and scalable framework for Health data sharing is guaranteed in the cloud. Using our suggested approach a fine-grained distributed access control scheme can be enforced, and scalable access between different clouds is enabled, besides a novel design to address the problem of improper data access caused by a user with multiple roles and access rights to health data.

It is worth stating that using our approach, each CSC can also define their security policies, such as how other CSCs can access their data. Equally, two intelligent agents that are dedicated to data security and security policy management will prevent any unprivileged access to data based on security policies defined by each CSCs. In addition, the possibilitie to guarantee and verify the security policies coherence, thanks to the transformation of any authorization evidence format sent with the mobile agent, in an appropriate format used by the CSP to store the rules of the security policy.

Similarly, in the proposed solution, which is an oriented mobile agent, a public key infrastructure is established to improve security by ensuring integrity, confidentiality and non-repudiation through the use of digital certificates for signing and encrypting data and mobile agents and by ensuring authentication users and mobile agents on our Jade platform by exchanging trusted public keys belonging to a trust chain and verifying the signatures of the visitor agents.

As an example of suggested model applications, we propose this case scenario: As depicted in Figure 5, in a cloud environment, using our proposed model Cloud MA-MOrBAC, we choose as CSCs two hospitals (A, B) that share a private cloud to store and manage their clinical data. The workflows of these hospital systems are elaborated as follows.

Suppose that a doctor from **hospital A** needs to manage patient's clinical data, which is stored on the hospital platform using a CSP.

• At CSC

Step 1: The doctor sends an access request to the hospital platform they belong to, with a set of parameters such as its Role in their Organization and the invoked object. At this moment, the "Access Manager Agent " launches the creation of a mobile agent called the "Requester Agent" who will be responsible for dealing this access request (1 and 2 in figure 3).

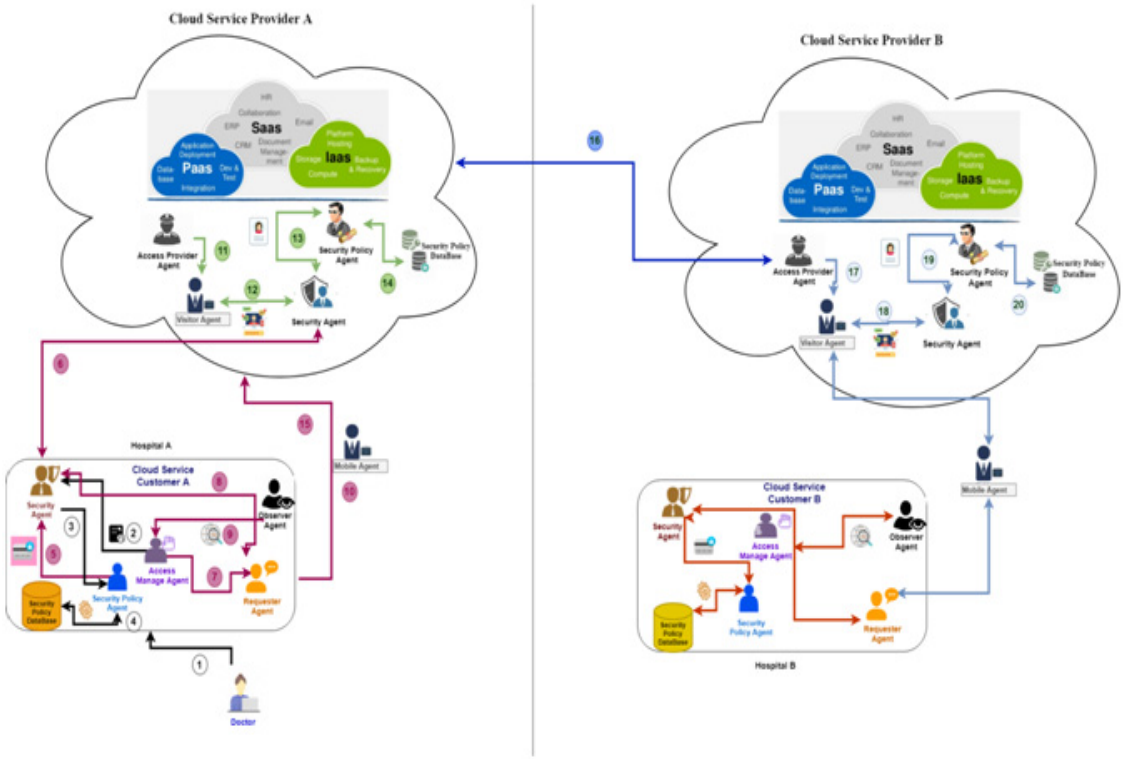

Figure 3. Access request scenario in cloud environment

Step 2: When the Requester Agent is created, the Access Manager Agent tells the security agent to check the access requester's (doctor) credentials, information and authentication. Thereafter, the Security Agent asks the Security Policy Agent about the different rule details associated to the doctor, whose goal is to have an adequate response to the access request and to proceed to the encryption process (3 and 4 in figure 3).

Step 3: In turn, the Security Policy Agent interprets this access request by checking the security policy contained in different format (database, XML file) and extracts the rules for deciding in current cases (which contain the rules sent with the query parameters). Then it combines the various possible rule sequences and evaluates the request parameters in these rules, resolves any conflicts and takes decision. For suitable access, it generates an evidence of authorization (table 2), in order to guarantee the access requester identification (4 in figure 3).

Step 4: The Security Agent receives the access decision. If the doctor does not have enough permission, the Security Policy Agent refuses the access request. Otherwise, if the doctor has sufficient permissions, the security agent receives an evidence of

authorization to execute the action, and then a shared key process is run between the two "security Agents" of both platforms. After that, it encrypts the evidence of authorization using the public key of the recipient platform Security Agent. Once the Requester Agent is ready to be migrated, the Observer Agent sends it after analyzing networks and receiving the confirmation opinion of the Access Manager Agent (steps 5, 6, 7, 8, 9 and 10 in figure 3).

• At CS P

Step 5: Afterwards, at the Cloud service provider system, when the Requester Agent arrives, the Access Provider Agent receives its request details, and then it asks the security agent to check the credential's information. In this case, the Security Agent runs the process authentication to decrypt the visitor agent and their evidence of authorization using the sharing public key used by the security agent of the CSC, in order to check whether there is permission to run its code. Since the Authentication process succeeds, and the security policy agent checks the visitor agent evidence of authorization following the security policy data base, the recipient CSP platform provides it all the resources needed to do its mission and a notification "Good received" is sent back to the CSC platform (11, 12, 13,14 and 15 in figure 3).

Step 6: Once finished, the Requester Agent receives the results of the query and depart from the first CSP, to continue its itinerary towards other CSPs so as to complete its missions (16, 17, 18, 19 and 20 in figure 3).

As a final step, when the "Requester Agent" returns at its home place, it goes through the authentication process again, to prevent against the fact that behaviors are changed during its mission.

6. Analysis and Evaluation of Proposed Model

In this section, in order to validate our model, we provide a security and performance property analysis and the benefits of our model compared with conventional access control models.

Throughout our model preparation, we have reviewed almost every proposed access control system for cloud computing. Most of them have not been validated or applied in a real cloud computing environment. Moreover, part of the suggested schemes target data outsourced and provisioned over the cloud (Li W, 2012)], others adapt the conventional access control models and their extensions in cloud computing (Andal Jayaprakash H, 2011) (Tsai W-T, 2011).

Our proposed scheme can achieve a high level of security in terms of fine-grained access control and prevention of improper access and securing sharing data. It provides secure interaction with a high level of confidence between all stockholders of cloud computing. This scheme interconnects diverse heterogeneous systems and solves interoperability issues. Equally, it can manage and define a coherent, dynamic access control policy independently of the implementation system and ensure the consistency of different access control policies.

➢ Ensuring the Consistency of Different Access Control Policies

In distributed environments, heterogeneity can happen in access control systems using various types of mechanisms, domains and policies.

One of the contributions of our proposed framework is that we pinpoint the access control policy conflict problem. As we used a responsible agent to handle this type of problem in our two main actors the CSP and the CSC.

Securing sharing data and interaction with a high level of confidence between all stockholders of cloud computing

In open and distributed systems like cloud computing, the exchange of data and information is quite important. When searching for or requesting a service in multi-organizational environments, all data will be transported over the networks. In this case, utilizing and sending mobile agents in our model instead of data reduces network traffic, as mobile agents encapsulate all their data. Thus, when an agent migrates to the CSP's platform, it has all the information necessary to perform its task (evidence of authorization (Table 2)).

➢ Scalability

We are confident that our model is scalable and can deal with large number of cloud service customer and cloud service provider through mobile agents associated with evidence of authorization presented in Table 1.

➢ **Dynamic Adaptation to Environments**

Among the strengths of mobile agents is self-adaptability. They are able to detect changes in their environment, react autonomously and adapt accordingly. The cloud computing environment is a complex, evolving and dynamic environment, and the need for an entity that adapts well with these environments is important. Mobile agents can evenly spread among different systems in a network to solve a complex problem optimally.

7. Conclusion and Future Work

In this paper we have put forward a novel access control model for cloud computing, entitled **Cloud MA-MOrBAC**. It is a new distributed access control model developed to meet distributed access control requirements in cloud computing. The novelty of our approach lies in the integration of the mobile agent technology as a communication entity. This is to reduce traffic on the network, to decrease work load at the CSP, and to reduce the amount of information exchanged between CSCs and CSPs, so it minimizes the chance to intercept the exchanged information across the network. The CSC can also monitor the privacy of its data without relying on CSP information, where the mobile agent migrates to the source information and performs local negotiations to get the information.

Furthermore, our Cloud MA-MOrBAC model can manage secure data access and data sharing between all stakeholders of cloud computing thanks to the mobile agent's technology, while controlling that the interactions between these stakeholders are in conformity with their needs and their internal security policies specified by MA-MOrBAC. Additionally, with our proposed approach, an evidence of authorization is used during a distributed access request to enhance the integrity of sharing data and resources. Using the set of attributes listed in this evidence of authorization can make the management and control of access request more flexible and scalable, especially for the increasing number of access requests from and to C SPs.

Consequently, we believe that our proposed access control model can also be utilized in domains other than healthcare, such as e-commerce or university environments.

Finally, for security reasons, each agent of our model must be encrypted before migrating by the "Security Agent" and decrypted as soon as it arrives to the sender. All transactions between cloud stakeholders are encrypted using the public key infrastructure. The communications between cloud stakeholders are performed through messages using the Agent Communication Language with the Message Transport Protocol.

Until now, an important part of our work has been done, but some issues remain open to in-depth analysis.

References

[1] Cloud Security Alliance Guidance Version 3.0. (2011), https://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[2] Safiriyu, E., Olatunde, A., Ayodeji, O. (2011). A User Identity Management Protocol for Cloud Computing Paradigm, *Int. J. Communications, Network and System Sciences*, 2011, 4, 152-163

[3] Zhang, Xuan., Wuwong, Nattapong., Li, Hao. (2010). Information Security Risk Management Framework for the Cloud Computing Environments, 10th *IEEE Int. Conf. on Computer and Information Technology* CTI 2010.

[4] Min, Y.G., Bang, Y. H. (2012). Cloud Computing Security Issues and Access Control Solutions, *Journel of Security Engineering*, volume 2, 2012.

[5] Khan, A. R. (2012). Access Control in Cloud Computing Environment, *ARPN Journal of Engineering and Applied Sciences*, 7 (5) MAY 2012

[6] Yahya, Zeineb Ben., BarikaKtata, Farah., Ghédira, Khaled (2017). MA-MOrBAC: A Distributed Access Control Model Based on Mobile Agent for Multi-organizational, *Collaborative and Heterogeneous Systems*. CRiSIS 2017. 101-114

[7] Ferber, J. (1999). Multi-Agent Systems: An Introduction to Distributed Artificial Intelligence. Addison – Wesley.

[8] Tang, Zhuo., Zhang, Shaohua, Li, Kenli., Feng, Benming. (2010). Security Analysis and Validation for Access Control in Multi-domain Environment based on Risk, *Information Security, Practice and Experience*, LNCS, Vol. 6047, 2010, p 201-206

[9] Sandhu, R. S., Samarati, P. (1994). Access controls, principles and practice. *IEEE Communications Magazine*, 32 (9), p

40-48, 1994.

[10] Wang, Z. (2011). Security and privacy issues within the cloud computing. In: 2011 *International Conference on Computational and Information Sciences*. IEEE; 2011. p 175e8. http://dx.doi.org/ 10.1109/ICCIS.2011.247.

[11] Dan Hubbard, W., Michael Sutton, Z. (2012). Top threats to cloud computing V1.0. Cloud Security Alliance; 2010. Retrieved June 20, 2012, from, https://cloudsecurityalliance.org/topthreats/ csathreats.v1.0.pdf

[12] Wang, C., Wang, Q., Ren, K., Lou, W. (2009). Ensuring data storage security in cloud computing. *In:* 2009 17th International Workshop on Quality of Service. IEEE; 2009. p 1e9. http://dx.doi.org/10.1 109/IWQoS.2009.5201385.

[13] Subashini, S., Kavitha, V. A. (2011). Survey on security issues in service delivery models of cloud computing. *J Netw Comput Appl* 2011, 34 (1) 1e11. http://dx.doi.org/10.1016/j.jnca.2010.07.006.

[14] Lombardi F., Di Pietro R. (2011). Secure virtualization for cloud computing. *J Netw Comput Appl* 2011, 34 (4) 1113e22. http:/ / dx.doi.org/10.1016/j.jnca.2010.06.008.

[15] Choudhury, AJ., Kumar, P., Sain, M., Lim, H., Jae-Lee H. (2011). A strong user authentication framework for cloud computing. In: 2011 *IEEE Asia-Pacific Services Computing Conference*. IEEE; 2011. p 110e5. http://dx.doi.org/10.1109/APSCC.2011.14

[16] Keromytis, AD, Smith, JM. (2007). Requirements for scalable access control and security management architectures. ACM Trans Internet Technol 2007, 7 (2) 22. http://dx.doi.org/10.1145/1239 971.1239972.

[17] Crago, S., Dunn, K., Eads, P., Hochstein, L., Kang, D-I., Kang, M., et al. (2011). Heterogeneous cloud computing. *In*: 2011 *IEEE International Conference on Cluster Computing*. IEEE; 2011. p. 378e85. http://dx.doi.org/10.1109/CLUSTER.2011.49.

[18] Patil, V., Mei, A., Mancini, L. (2007). Addressing interoperability issues in access control models. *In*: ASIACCS '07 Proceedings of the 2nd ACM symposium on Information, computer and communications security, vol. 389-391; 2007. Retrieved from, http://dl.acm.org/citation.cfm?id¼1229337; 2007.

[19] Almutairi, A., Sarfraz, M., Basalamah, S. (2012). A distributed access control architecture for cloud computing. *Softw IEEE* 2012, 29(2):36e44. Retrieved from, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arn umber¼6095492.

[20] Hasebe, K., Mabuchi, M., Matsushita, A. (2010). Capability-based delegation model in RBAC. In: Proceeding of the 15th ACM symposium on Access control models and technologies e SACMAT '10. New York, New York, USA: ACM Press; 2010. p 109e18. http:// dx.doi.org/10.1145/1809842.1809861.

[21] Kuhn, D. F. (1992). Role-Based Access Controls. 15th National Computer Security Conference, 554 - 563.

[22] Suhendra, V. (2011). A survey on access control deployment. SecurTechnol 2011, 259:11e20. Retrieved from,

[23] Munawer, Q. (2000). Administrative models for role-based access control. George Mason University; 2000. Retrieved from, http://citesee rx.ist.psu.edu/viewdoc/download?doi¼10.1.1.92.9150&rep¼r ep1&type¼pdf.

[24] Almutairi, M. I., Sarfraz, S., Basalamah, W. G. Aref Ghafoor, A. (2012). A Distributed Access Control Architecture for Cloud Computing, *IEEE Software*, 29 (2) March-April 2012

[25] Ruj, S., Nayak, A., Stojmenovic, I. (2011). DACC: Distributed Access Control in Clouds, *In*: Proceedings of the 10th IEEE International Conference on Trust, *Security and Privacy in Computing and Communications*, p 91-98, 2011.

[26] Al-Kahtani MA, Sandhu R. (2002). A model for attribute-based user-role assignment. In: 18th Annual Computer Security Applications Conference, 2002. *In*: Proceedings. *IEEE Comput. Soc*.; 2002, 353e62. http://dx.doi.org/10.1109/CSAC.2002.1176307.

[27] Karp, A., Haury, H., Davis, M. (2009). From ABAC to ZBAC: the evolution of access control models. HP Laboratories-2009-30; 2009. Retrieved from, http://www.hpl.hp.com/techreports/2009/HP L-2009-30.pdf?jumpid¼reg_R1002_USEN.

[28] Brucker, A., Bru¨ gger, L., Kearney, P., Wolff , B. (2011). An approach to modular and testable security models of real-world health-care applications. *In*: SACMAT'11. Proceedings of the 16th ACM symposium on Access Control Models and Technologies.133e42. Retrieved from, http://dl.acm.org/citation.cfm? id¼1998461; 2011;

[29] Suhendra V. (2011). A survey on access control deployment. SecurTechnol 2011; 259:11e20. Retrieved from, http://www.springerlink.com/index/J31010242555W867.pdf.

[30] Varsha, D., Mali, Patil, Pramod. (2011). Authentication and Access Control for Cloud Computing using RBDAC Mecha

nism, *International Journal of Innovative Research in Computer and Communication Engineering*, 4 (11), November 20 16, DOI: 10.15680/IJIRCCE. 2 016

[31] Shantanu Pal, Khatua, Sunirmal., Chaki, Nabendu., Sanyal, Sugata(2012). A New Trusted and Collaborative Agent Based Approach for Ensuring Cloud Security; *Annals of Faculty Engineering Hunedoara International Journal of Engineering*; 10 (1) February, 2012. p 71-78. ISSN: 1584-2665.

[32] Almenarez, Florina., Marin, Andrés., Campo, Celeste., Carlos. (2004). PTM: A Pervasive Trust Management Model for Dynamic Open Environments, Proceedings of First Workshop on Pervasive Security, Privacy and Trust PSPT'04, Boston, USA, 2004.

[33] Priyank, S., Ranjita, S., Mukul, S. (2011). Security Agents: A Mobile Agent based Trust Model for Cloud Computing, *International Journal of Computer Applications* (0975 – 8887) 36 (12) December 2011.

[34] Alwesabi, A., Okba, K. (2014). Security Method: Cloud Computing Approach Based on Mobile Agents. *International Journal of New Computer Architectures and their Applications* (IJNCAA), 4 (1) 17- 29.

[35] Ali, Alwesabi., Abdullah, Almutewekel. (2013). Implementation of Cloud Computing Approach Based on Mobile Agents,".Computer science department, university of Batna, Algeria Batna, Algeria, *International Journal of Computer and Information Technology* (ISSN: 2279 – 0764) 02 (06) November 2013

[36] Standard, Nist-Fips. (2001). Announcing the ADVANCED ENCRY PTION STANDARD (AES), Federal Information Processing Standards Publication 197, NIST, 2001.

[37] Li, W., Wan, H. (2012). A refined RBAC model for cloud computing. In: 2012 IEEE/ACIS 11th International Conference on Computer and Information Science. IEEE; 2012. p 43e8. http://dx.doi.org/ 10.1109/ICIS.2012.13.

[38] Andal Jayaprakash, H., HadiGunes, M. (2011). Ensuring access control in cloud provisioned healthcare systems. In: Consumer Communications and Networking Conference (CCNC), 2011 IEEE. p 247e51. Retrieved from, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber¼5766466; 2011.

[39] Tsai, W-T, Shao, Q. (2011). Role-based access-control using reference ontology in clouds. In: 2011 *Tenth International Symposium on Autonomous Decentralized Systems,* vol. 2. IEEE; 2011. p 121e8. http://dx.doi.org/10.1109/ISADS.2011.21