ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

To Protect Virtual Machine Images of Cloud by Kerberos

Deepesh Shrivas[1], Prof. Ajeet Singh[2]

M.Tech. Scholar, Department of Computer Science & Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[1]

Assistant Professor, Department of Computer Science & Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[2]

ABSTRACT: The accelerated outgrowth of virtualization in cloud computing has brought organizations to adopt this technology for its cost-effectiveness, ease of deployment and high availability of resources. Ensuring the security of virtual machine images is a big concern to cloud providers as well as the companies which own applications and servers in the cloud. Industry and academia have accompanied extensive research to ensure the security of a virtualized cloud environment. Any compromise of disk images can result in loss of data confidentiality and integrity. There are lots of security threats related to the retrieval and storing of virtual machine (VM) images into cloud storage. Kerberos protocol has been used in many areas for its superior authentication and authorization services. This paper proposes a novel security architecture for the protection of stored virtual machine images in clouds by employing encryption, decryption mechanisms, and Kerberos.

I.INTRODUCTION

No need to install any software. Cloud architecture, the systems architecture of the software systems involved in the delivery of cloud computing, typically involves multiple cloud components communicating with each other over loose coupling mechanism such as messaging queue. Cloud computing services are broadly divided into three categories as follows:

Software as a Service (SaaS): In this model, a complete application is offered to the customer, as a service on demand. A single instance of the service runs on the cloud & multiple end users are serviced. On the customers‟ side, there is no need for upfront investment in servers or software licenses, while for the provider, the costs are lowered, since only a single application needs to be hosted & maintained. Today, SaaS is offered by companies such as Google, Salesforce, Microsoft, etc.

Platform as a Service (PaaS): PaaS vendors offer a development environment to application developers. The provider typically develops toolkit and standards for development and channels for distribution and payment. In the PaaS models, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. Such as Google App Engine, Yahoo Open Strategy, Microsoft Azure etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

Infrastructure as a Service (IaaS): This is the base layer of the cloud stack. It serves as a foundation for the other two layers, for their execution. The keyword behind this stack is Virtualization. The application will be executed on a virtual computer (instance). There is choice of virtual computer, where a configuration of CPU, memory & storage can be selected that is optimal for our application. The whole cloud infrastructure viz. servers, routers, hardware based load-balancing, firewalls, storage & other network equipment's are provided by the IaaS provider. Some common examples are Amazon, GoGrid, 3 Tera, etc.

Deployment Models were classified as:

- Private cloud: The cloud infrastructure is owned or leased by a single organization and is operated solely for that organization.
- Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, and policy).
- Public cloud: The cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group.
- Hybrid cloud: The cloud infrastructure is a composition of two or more clouds that remain unique entities but are bound together by standardized or proprietary technology.

Cloud computing has long been predicted to fundamentally revolutionize the way resources and services are managed. In fact, it has emerged as a technological phenomenon with huge benefits for businesses and consumers. Cloud computing is a promising paradigm for delivering computing utilities as services. A large number of commercial cloud providers have entered the utility computing market which led to the proliferation of different types of pay-as-you-go services. With this shift, computing marketplace environment [1] a n d e-infrastructures [2] made a leap forward towards better adaptation of usage strategies which are based not only on users' demand and market supply but also on a sustainable, public, and ubiquitous cloud computing infrastructure.

Cloud computing faces many security challenges. Access control systems are often seen as the most effective tool pro- viding the control of users' actions and operations on re- sources stored in cloud servers. Traditional access control models are based on the assumption that the resources' owner and the servers providing resources are in the same trusted domain. The servers are then entirely entrusted as monitors responsible for applying access control policies. This assumption is no more valid in cloud computing since the data owner and the cloud servers are likely to be in different domains. Hence, data and resources are not physically under their owners' control. Furthermore, the cloud servers are not allowed to access the stored data for reasons of confidentiality. All these reasons make traditional access control systems un- able to manage access control in the cloud.

In this paper, we address this issue and propose a generic Kerberos-based single sign on (SSO) access control system for the cloud. The remainder of this paper is organized as follows: Section 2 summarizes the literature review related to access control systems for the cloud and proposes a classification of these systems. Section 3 presents the architecture of our proposal. Section 4 shows the performance evaluation results obtained via simulations. In Section 5, we describe a proof of concept of the proposed solution implemented over Openstack combined with Kerberos. Finally, Section 6 concludes the paper and presents ongoing work.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

II.RELATED WORKS

In this section, we recall traditional access control models to emphasize the need for new schemes targeting the cloud environment and identify the main requirements of access control systems for the cloud. First, we examine access control systems implemented in the widely used public clouds. Then, we review related works in the research field and propose a classification of the studied models.

A traditional categorization divides access control models into three types: discretionary (DAC), mandatory (MAC), and role-based access control models (RBAC). In the DAC models, the objects' owner decides and sets the access permissions for the other users. DAC models are usually used with legacy applications and have a non-negligible management overhead in the context of distributed environments such as cloud systems. MAC models abstract the need for resource- user mapping. Compared to DAC models, they are more suited for distributed systems. The MAC models are typically used in multi-level security systems where the access permissions are set by the systems' administrators. Subjects and ob- jects are identified and classified according to different security levels [3]. In RBAC models, users have access to objects based on their assigned roles. Roles are defined according to job functions while permissions are set according to job authorities and responsibilities. Operations on objects are invoked according to the permissions. RBAC models are more scalable than the DAC and MAC access control models. They are more suitable to cloud computing environments, especial- ly when the users of the services cannot be tracked with fixed identities. However, in large systems, memberships, role in- heritance, and the need for finer-grained customized privileges make their administration potentially unmanageable.

2.1 Requirements for cloud-based access control systems

We refer to the studies in [4–13] to identify the following requirements.

1. Scalability: Access control as well as policy evaluation mechanisms have to support an increasing number of users [6].
2. Authentication and trust: Cloud-based access control models need a reliable, strong user authentication mechanism [7]. A mutual trust relationship between users and service providers must be established. Trusted behaviors between these two entities must be defined [8].
3. Heterogeneity and interoperability: Heterogeneity in cloud computing is defined as the large number and the diversity of technologies and mechanisms used to deliver services by cloud providers [9]. The interoperability and collaboration between specialized providers when users move from one provider to another is required [10].
4. Fine-grained access control: The data owners should be able to define and enforce expressive access structures for each user. Furthermore, the distribution and the definition of access policies and permissions for each protected re- source or service should be secure and reasonable [11].
5. Quality of service: Access control systems in cloud computing are assumed to have a significant number of consumers to authenticate and serve. They have to grant access decisions in a reasonable time and according to the enterprises' requirements. The computational complexity of access control rules remains a hard task for any access control system [12]. Indeed, this complexity can affect the efficiency and quality of service as it might delay the decision making process.
6. Delegation of capabilities: Cloud computing is an environment where users collaborate to fulfill their general tasks. To ensure flexibility and dynamic resource management, delegation of permissions and roles is required [13].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

2.2 Classification of cloud-based access control models

Various studies proposed access control systems for cloud computing. Some target outsourced and provisioned data over the cloud while others adapt the conventional access control models for the cloud. In this section, we present a classification of the proposed access control models in three classes: role-based, token-based, and encryption-based.

2.2.1 Role-based access control models

Google proposes an RBAC model for the Google Cloud Storage.1 This system is based on roles and access control lists (ACL). Three roles can be assigned to an entity accessing data: Reader, Writer, and Owner. An ACL consists of one or more entries, where each entry grants permissions to a scope. Permissions define the actions that can be performed over an object or a bucket. The scope defines whom the permission applies to (for example, a specific user or group of users). The uniqueness of the identities is ensured by using unique and previously verified identities such as Google storage ID and Google e-mail addresses. Many types of access lists can be specified. This gives more flexibility in the privileges granting for a large number of users and objects in the cloud. However, there is no use of cryptographic
mechanism that can protect data. This can be an issue when privileges are abused by malicious parties. Encryption would avoid access to user's sensitive data.

TRBAC is a temporal RBAC with the possibility to enable or disable a role at run-time depending on user requests [14]. Authors of [15] present generalized temporal RBAC (GTRBAC) which advocates role activation instead of role enabling. A role is activated if at least one user assumes that role. GTRBAC supports the enabling and disabling of constraints. It is based on the maximum active duration allowed to a user as well as the maximum number of activations of a role by a single user within a particular interval of time. This model fits with multi application domain environments where multi- ple organizations interoperate.

Authors in [16] present an XML-based RBAC policy specification framework (X-RBAC). This framework is composed of a policy decision point, a policy enforcement point, and a policy base. To allow interoperation between access policies, they propose the use of service-level agreement (SLA) which performs role mapping. This scheme represents authorization design for access management and satisfies interoperability, scalability, and quality of service. However, several issues have to be addressed regarding the design of the authentication mechanism, cryptography, and key management as well as the mediation for conflict resolution related to heterogeneity in policies and architectural choices for SLAs. This model is intended for collaborative environments sharing resources across multiple clouds and considers the three types of collaboration, i.e., federated, loosely coupled, and ad hoc.

An enhanced hybrid approach, named X-GTRBAC, combining XML-based RBAC and GTRBAC, is presented in [17]. It relies on certificates provided by trusted third parties. In fact, these certificates assign roles to users. The access control decision is based on users' trust levels which are determined using users' context (i.e., time, location, or environment) during the access requests. This feature suits web-based cloud computing environments with diverse users' activity profiles. The limitations of this model lie in the fact that the cloud is assumed to be honest. Data authenticity is supposed to be checked by the users. This causes an excessive computational overhead for data access. The X-GTRBAC is mainly intended for data storage services in the cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

In [18], a single sign on (SSO) scheme is proposed. This scheme is known as profile-based access control model (PrBAC). It relies on users' profiles maintained by cloud service providers. User's profile is composed of the user's parameters such as the type of data he/she wants to access, for how much time he/she wants to access it, etc. The cloud service providers create and manage temporary access control lists containing the users' profiles for data access. The SSO feature reduces the access time but requires a huge scope of work to improve the system's security. The PrBAC model is designed for controlling access to data stored in the cloud.

Authors in [19] propose a security framework that includes an access control model and a cloud resources security layer on top of the Open Nebula Ruby cloud application- programming interface (API). The access control component is based on users, groups, and access control lists. Users can have roles and delegate them to other users. During authorization, the users' assigned roles are activated in the implicit session. The roles are checked, and users with valid permissions are allowed access. Moreover, for fine-grained granular- ity, permissions are defined as triplets (access mode, resource type, resource ID). The test of this proposal shows that the overhead depends on the system's load as well as on the action requested by the users.

2.2.2 Token-based access control models

In these models, tokens are generated for specific access levels and then assigned to users. In Windows Azure [20], the access control relies on identity statements. The access control decision is based on tokens of statements sent by users. A statement may contain the user's name, for example, while another contains the user's age or the group he/she belongs to. Tokens are issued by identity providers (IDP). Different IDPs may use different token formats and represent identity statement in different ways. Each application can decide which IDP to trust and which tokens to accept. Hence, an application that accepts identities from Google, Facebook, and Yahoo, for example, has to manage the different tokens associated to these IDPs. The goal of this access control scheme is to make it easier for developers to create secure applications that support identity statements from various providers; these applications can be easily deployed in the cloud.

The authors in [21] propose a token-based access control system that is implemented in Hadoop (an open-source cloud computing framework). This model is designed for large Resource Description Framework (RDF) data storage. It de- fines six types of access levels and an enforcement strategy for the resulting access control policies. The enforcement strategy is implemented at three levels: Query Rewriting, Embedded Enforcement, and Post-processing Enforcement. In the Embedded approach, enforcement is done during data selection using Map Reduce, whereas in the Post-processing Enforcement approaches, it is performed during the data presentation to users. The problem with this construction is that it is not generic regarding token structures and policy conflicts can be identified.

2.2.3 Encryption-based access control models

These models target access to stored data. Data owners are able to outsource and store data into the cloud. Mostly, data has various degrees of sensitivity which is considered as a factor for either granting or denying access to data. The data is encrypted then outsourced to cloud servers. Encryption-based access control models use cryptographic algorithms depending on the availability of computing resources. Numerous cryptographic access schemes have been defined and implemented in cloud computing.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

In [22], the authors propose an approach that helps data owners achieve a scalable access control for their files stored in cloud servers. Data owners are given the capability to en- force a single access structure for each user, i.e., the set of files he/she is authorized to access. This procedure prevents the cloud servers from reading the contents of data files or the users' grants. This approach is based on data attributes and uses key-policy attribute-based encryption (KP-ABE) combined with proxy re-encryption (PRE) [23] and lazy re- encryption [24, 25]. This construction causes a computation overhead to the data owner since he/she is responsible for all the cryptographic operations and data management. This concern is mainly caused by users' revocation operations. The data owner has to re-encrypt all the files that were accessible to the revoked users. Data owners have to remain online in order to update the users' keys when required. To solve this problem and make a suitable construction, the combination of PRE with KP-ABE is considered to allow data owners to delegate most intensive calculations to the cloud servers with- out having to disclose the contents of encrypted files. In addition, the creation of dummy attributes is proposed to prevent the data decryption by the cloud servers. The problem with KP-ABE scheme is that the encrypting side cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data. This feature might be unsuitable in some applications since a data owner has to trust the key issuer. In addition, KP-ABE scheme is designed for one- to-many communications, which may cause inadequacies with other communications types.

Authors in [26] portray an efficient multi-authority cipher- text-policy attribute-based encryption (CP-ABE) scheme that does not require a global authority and can support any linear secret sharing scheme access structure. They propose a new solution to solve the problem related to attributing revocation in multi-authority CP-ABE systems. The proposal suggests moving the re-encrypting task to the server side by using a proxy encryption method. By doing so, there is no more need for the server to decrypt the data before re-encryption. The pro- posed scheme is scalable and efficient but it shows limitations in terms of policy specification and user attributes management. Furthermore, it is strongly dependent on the oracle model, so it must be extended to meet standard model requirements.

Authors in [27] focus on the issue of constructing a secure cloud storage service over untrusted service providers to which users outsource sensitive data. They adopt attribute- based encryption (ABE) as the main encryption primitive, attribute-based signature (ABS) as authentication mechanism, and eXtensible Access Control Markup Language (XACML) as policy descriptive language. The main contribution is to propose a privacy-preserving data access control scheme, by extending cipher-text-policy attribute-based encryption with multi authorities' hierarchical structure. This scheme supports Write privilege on outsourced data in the cloud and provides authentication to both users and cloud servers. It also relies on XACML framework to improve the scheme's scalability with more data and policies. The proposed solution is expected to have the same security property as CP-ABE and ABS, which have been proven to be secure under the generic bilinear group model and the random oracle model. The limitation is that the signature policy is known by the cloud servers which may compromise the privacy of verification.

In [5], the authors construct a lightweight cipher-text access control mechanism for mobile cloud storage. The proposal relies on authorization certificates for access control to encrypted data in the cloud. The Lagrange interpolation polynomials are used for the decryption key reconstruction which simplifies the distribution of the decryption key and enables fine-grained access control. The proposed access control scheme consists of five functional modules: setup, operations on a file, authorization, file access, and authorization revocation. The evaluation of the solution considering security, granularity, dynamicity, scalability, and accountability shows that it has significant advantages in terms of authorization revocation compared to existing solutions.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

2.2.4 Trust-based access control models

Access control models usually check users' identities authenticity without taking into account the trustworthiness of users' behaviors. To address this issue, researchers propose to integrate trust mechanism into traditional access control models [8]. Various users' trust features are calculated and integrated into access control to ensure more secure permissions distribution.

The work in [28] proposes a mutual trust based access control model (MTBAC) combining access control model and trust management. MTBAC takes into consideration both users' behavior and cloud service nodes trust in order to secure both users and cloud servers efficiently. Mutual trust between users and servers is established through a trust mechanism inspired by the ant colony optimization algorithm [29]. Users' behavior is divided into three weighted types of trust models. User's trust level is determined through trust quantification of user's behavior. MTBAC suits uncertainty, dynamism, and distribution features of cloud computing.

In [4], another type of access control model named risk- based access control is added to the characterization. Risk-based access control was proposed to cope with multinational organizations that face various kinds of policies and regulations [30]. This model uses different kinds of risk levels with environmental conditions and relies on the Boperational need^
principle in order to make access decisions [31].

Figure 1 presents a taxonomy of access control models for the cloud based on our classification of the studied models. From the domain specification perspective, the studied models can be divided into two categories. The first is composed of access control models applied only to outsourced data in cloud servers [5, 17, 18, 22, 26, 27]. The second category is com- posed of access control models considered generic in regard to the services and resources shared in the cloud [15, 16, 19–21,28]. In Fig. 1, the first category is presented in blue while the second is presented in white.

III.DESIGN OF THE ACCESS CONTROL MODEL

The heterogeneity in terms of resources and service types raises the need for generic access control model. Our goal here is to provide a generic solution to prevent unauthorized access to resources provided by the cloud. We present the architecture and the mechanisms of the proposed approach. In order to propose a solution as generic as possible regarding to the application domains and the service model, i.e., IaaS, PaaS, and SaaS, we propose a single sign on (SSO)-based approach.

SSO gives the ability for users to sign in once per session and subsequently, to get access to resources without having to re-authenticate. The authentication step is based on retrieving cached credentials rather than re-entering them. The motivations of the choice of SSO are (i) a mutual trust relationship between users and the different system components can be established to answer requirement 1, (ii) SSO also helps fulfill requirement 2 since it provides authentication and access to cloud resources independently of the technologies and mechanisms implemented by cloud providers, (iii) requirement 3 can be satisfied since SSO separates the authentication and the authorization phases. Access policies and permissions specific to each resource or service can, then, be taken into consideration, (iv) SSO permits the handling of authentication and authorization in separate functional components which con-tributes to enhancing the performances of the access control system (requirement 3), and (v) SSO can also support the evolution towards access control to federated cloud providers served by a common authentication server.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

3.1 Operation overview

Figure 2 presents the proposed system architecture which is composed of the following functional elements:

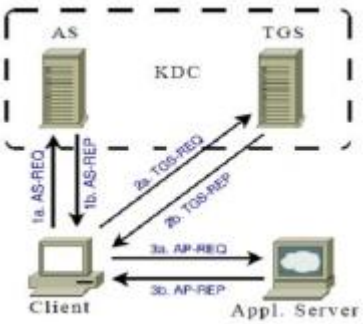
– The Kerberos server—its role is to authenticate users requesting access to cloud resources. It is composed of the authentication server and the ticket granting server (TGS). TGS issues tickets to users for access to resources.

– The frontal cloud server sets the connection between the user and the rules engine.
– The rules engine ensures the authorization.
– The shared resources.

A trust relationship is supposed to be established between the authentication server and the cloud server. This type of architecture is highly flexible since it can easily move from a centralized authentication model, where the authentication server and the cloud providers belong to the same organization domain, to a federated model. In this kind of models, multiple cloud providers belonging to different organization domains rely on the same authentication server.

3.2 The proposed mechanisms

Good load balancing makes more efficient and improve user fulfilment in cloud computing. Thus, one future work is how to speed-up the decryption operation at low-end devices. However, the decryption may be still slow for low-end devices because a modular exponentiation operation is required. The load balancing in cloud has imported collision on the performance. So, proposed a framework that will use RSA encryption algorithm to encrypt the data. To secure sensitive data kerberos is used for a user process protection method based on a virtual machine monitor. The basic set up of Kerberos protocol is as shown.



The Kerberos server consists of an Authentication Server (AS) and a Ticket Granting Server (TGS). The AS and TGS are responsible for creating and issuing tickets to the clients upon request. The AS and TGS
usually run on the same computer, and are collectively known as the Key Distribution Center (KDC). The Kerberos authentication process works in three phases as shown in Figure 3. Kerberos is a distributed, identity-based authentication system that provides a method for a user to gain access to an application server.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

Authentication is critical for the security Computer systems. Without knowledge of a principal requesting an operation, it is difficult to decide whether the operation should be allowed. Traditional authentication methods are not suitable for use in computer networks where attackers monitor network traffic to intercept passwords.
The use of strong authentication methods that do not disclose passwords is imperative. So, the proposed Kerberos authentication system is well suited for authentication of users in such environments.

As for the authentication protocol, we rely on Kerberos2 which provides client-server authentication and mutual authentication based on SSO facility. Kerberos offers the ability to prove users' authenticity once in a period. The Kerberos server caches time-stamped and limited user's credentials and presents them on behalf of the user during service access re- quests. In addition, we propose the use of access control lists (ACL). As shown in Fig. 3, the ACL users consist of a two- dimensional table containing the set of the registered user's pairs of identifiers and their respective tickets (user-ID, ticket- ID). Users are added to ACL independently of the type of access permissions they have on resource. This list is setup during the project creation for each shared resource. When users are added or revoked the ACL is updated dynamically.
As for the medium for transferring the access control information, we rely on authorization tickets to prove users' rights to access resources. A ticket conveys a temporary set of credentials that verify the identity of a client for a particular resource. An authorization ticket is composed of the following fields:

– Ticket-ID: A unique value used to identify each authorization ticket.
– User-ID: A unique identifier for each user.
– Project-ID: A unique identifier of the project.
– Resource-ID: A unique identifier of the resource. The couple of project-ID and resource-ID provides information on the target field of the permission ticket.
– User public key: This key is used to encrypt the nonce
and the messages exchanged between the user and the different entities such as the rules engine.
– Permission: Type of permission. We define four types of permission: BRead,^ BWrite,^ BRead-write,^ and BTotalControl.

IV.SIMULATION AND PERFORMANCE EVALUATION

The goal here is to test and discuss the effectiveness and the performance of the proposed access control solution. The use of simulation techniques in the performance evaluation of communication networks and distributed systems is a consolidated research area. We used CloudSim as a cloud simulator. According to [32–34], CloudSim is a generalized and extensible framework allowing the modeling, the simulation, and the experimenting of new cloud computing infrastructures and applicative services. It is one of the most popular simulation environments and is widely used by the researcher community in the field of cloud computing. CloudSim is available as a java code-free source; it is structured into classes modeling the different cloud entities. It fits the layered feature as well as the abstraction of cloud computing architectures and shows a high flexibility in the manipulation of the different entities.

4.1 The simulation model

We implemented the authorization phase as well as the pro- posed mechanisms. We used SHA as hash function, RSA to encrypt the nonce, and the messages exchanged between the communicating entities and RSA signature for the tickets' signature generation and verification.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

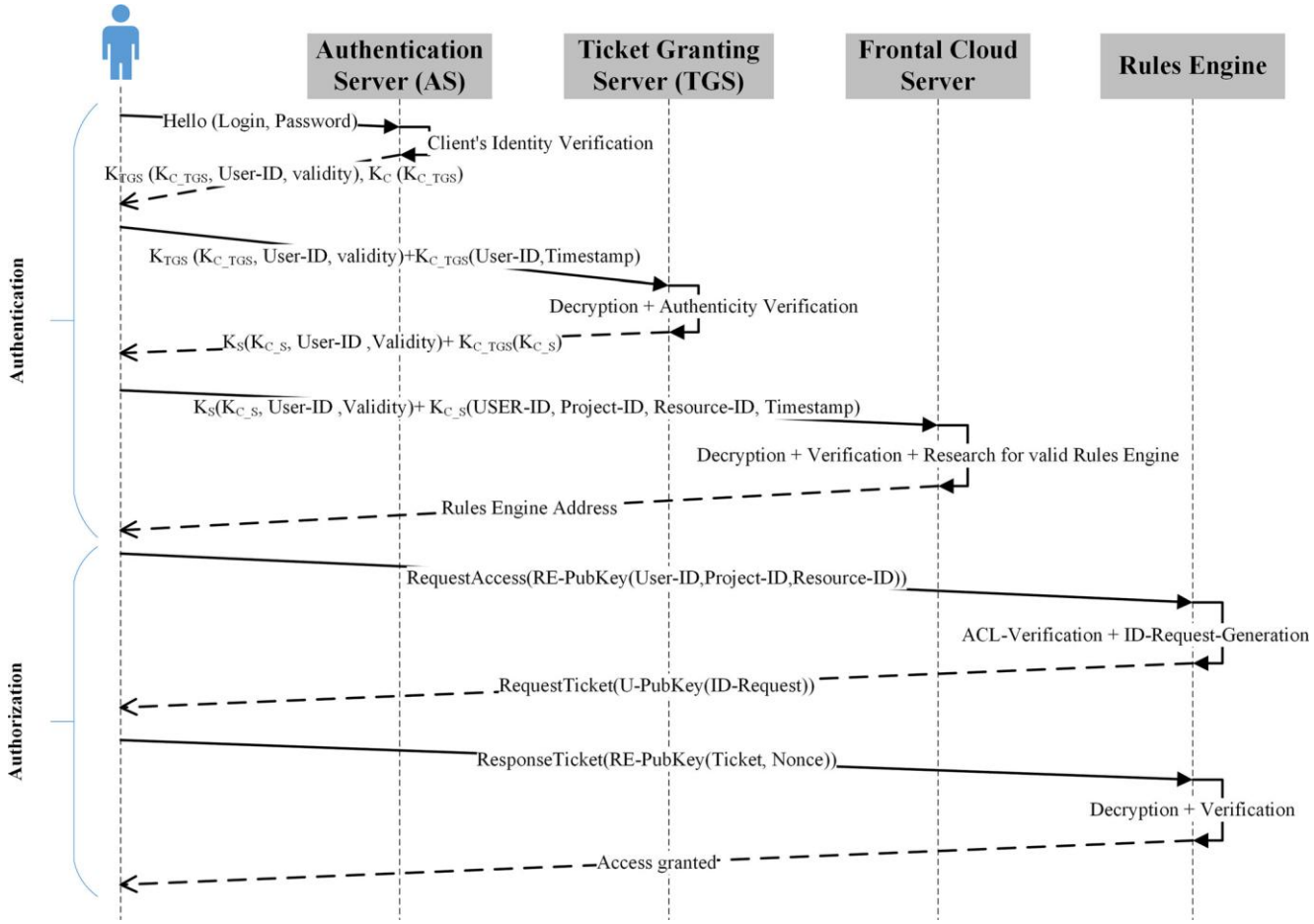
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

For the simulation model, we used the layered architecture of CloudSim. During the development phase, we modified some CloudSim classes and added other new classes to meet the requirements of the solution design. In our simulation



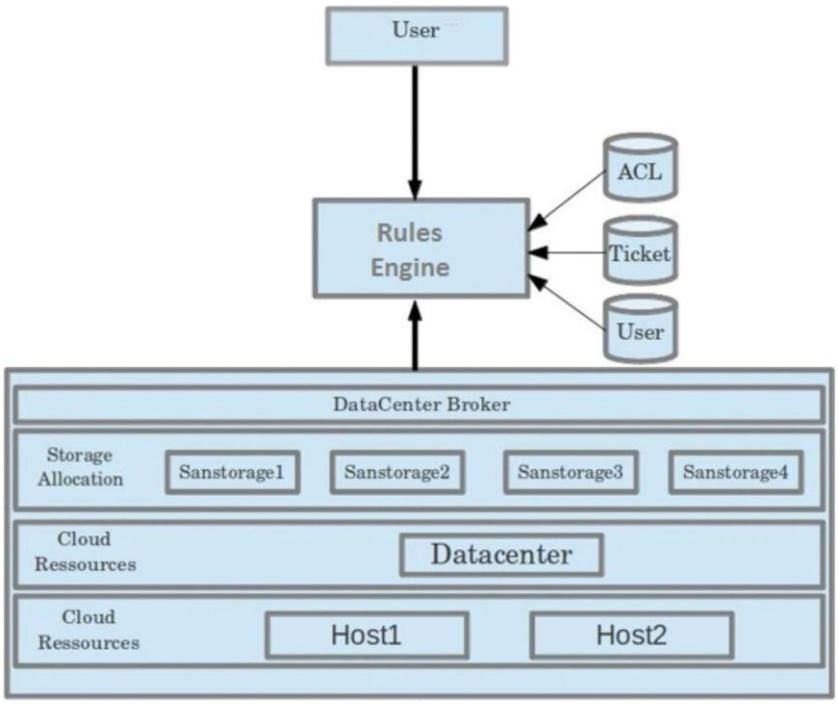
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020



In order to show the feasibility of our proposal, we implemented and integrated the authentication phase over a cloud platform. We used Openstack,3 a free open-source cloud computing platform which provides an Infrastructure-as-a-Service (IaaS) solution through a set of interrelated services. Each service offers an application-programming interface (API) which facilitates this integration. This version of Openstack includes a component named Keystone responsible for identity management ser- vice. Keystone is responsible for users, permissions, and services management. It permits to issue and verify bound tokens for the authentication mechanisms. Openstack to-kens were originally known as bearer tokens. This term has been adopted to mean that whoever has the token inherit all the rights of its owner. However, token replay attacks have been emphasized.

When Kerberos is combined with Keystone, a new type of token is created and named Bbound token. It is a combination of a Keystone token with other information, i.e., the BKerberos principal, to inform the system that the token must be used with an external authentication mechanism by which it is bounded. A Kerberos principal is the unique identity to which Kerberos can assign tickets. In the present study, every Kerberos principal identifies an owner of a Kerberos ticket. The resources provider within the cloud receiving the bound token must ensure that the Kerberos authentication is successful and that the user

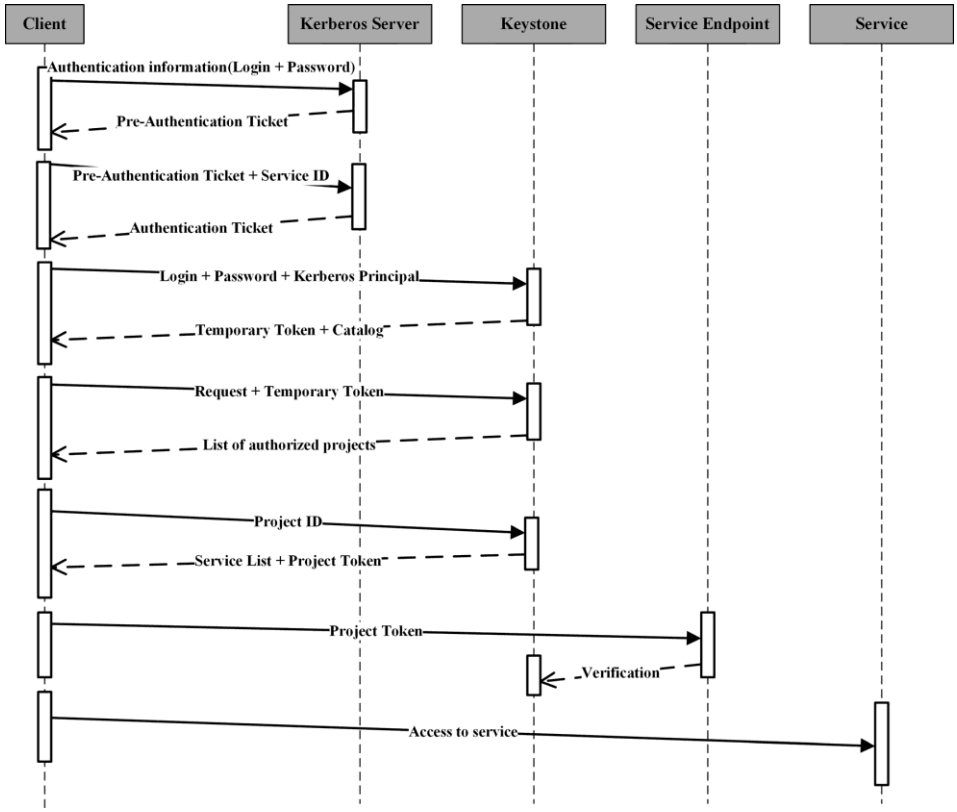
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020



Making the request is the same as the one who has been successfully authenticated.
The following steps permit to set up the Kerberos integration with Openstack:

– Creating resources on Openstack cloud server.
– Creating users and assigning access rights.
– Configuring Kerberos and virtual machines (KDC server and client).

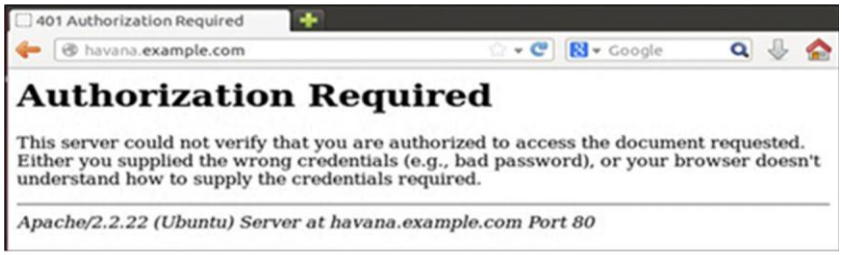
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020



a- Unsuccessful scenario

b- Successful scenario

V.CONCLUSION

In this paper, the focus is on access control for cloud computing. After reviewing the latest developments in access control systems, four categories have been identified: role-based, token- based, encryption-based, and trust-based access control. This classification shows that most approaches are designed for specific application domain targeting either data or resources. Consequently, a new single sign on (SSO) access control system is proposed. SSO offers various qualities which fulfill the cloud requirements of access control. The proposed solution relies on Kerberos, ACLs, and authorization tickets for the implementation of the access control and no replay. Kerberos provides authentication and mutual authentication based on SSO facility. Performance evaluations using CloudSim show that the pro- posed solution is efficient and has an acceptable access time to shared resources for different cloud computing architecture scenarios. They also show that the elasticity of the cloud resources has no significant impact on the access time. The overhead resulting from the implemented security mechanisms can there- fore be tolerated. In order to prove its feasibility, the proposed solution has been implemented over, an Openstack cloud plat- form to which Kerberos has been integrated.

REFERENCES

1. Altmann J, Courcoubetis C, Risch M (2010) A marketplace and its market mechanism for trading commoditized computing resources. Ann Telecommun 65:653–667
2. Mohammed AAB, Altmann J (2010) A funding and governing model for achieving sustainable growth of computing e-infrastruc- tures. Ann Telecommun 65:739–756
3. Maghanathan N (2013) Review of access control models for cloud computing. Comp Sci Info Sci 3(1):77–85
4. Younis YA, Kifayat K, Merabti M (2014) An access control model for cloud computing. J Info Secur Appl 19(1):45–60
5. Yao X, Han X, Du X (2014) A lightweight access control mecha- nism for mobile cloud computing. In: Computer Communications Workshops (INFOCOM WKSHPS), 2014, pp 380–385

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

6. Keromytis AD, Smith JM (2007) Requirements for scalable access control and security management architectures. ACM Trans Internet Technol (TOIT) 7(2):8
7. Choudhury AJ, Kumar P, Sain M, Lim H, Jae-Lee H (2011) A strong user authentication framework for cloud computing. In: Services Computing Conference (APSCC), 2011 I.E. Asia- Pacific, IEEE., pp 110–115
8. Wang W, Han J, Song M, Wang X (2011) The design of a trust and role based access control model in cloud computing. In: Pervasive Computing and Applications (ICPCA), 2011 6th International Conference on, IEEE., pp 330–334
9. Crago S, Dunn K, Eads P, Hochstein L, Kang D-I, Kang M, Modium D, Singh K, Suh J, Walters JP (2011) Heterogeneous cloud computing. In: IEEE International Conference on Cluster Computing (CLUSTER), 2011, pp 378–385
10. Patil V, Mei A, Mancini LV (2007) Addressing interoperability issues in access control models. In: Proceedings of the 2nd ACM symposium on Information, computer and communications securi- ty, ACM., pp 389–391
11. Lin G, Bie Y, Lei M (2013) Trust based access control policy in multi-domain of cloud computing. J Comp 8(5):1357–1365
12. Hu VC, Kuhn DR, Ferraiolo DF (2006) The computational com- plexity of enforceability validation for generic access control rules.
In: IEEE Internatio nal Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006, IEEE., p 7
13. Hasebe K, Mabuchi M, Matsushita A (2010) Capability-based del-
egation model in RBAC. In: Proceedings of the 15th ACM sympo- sium on Access control models and technologies, ACM., pp 109–118
14. Nurmi D, Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L, Zagorodnov D (2009) The eucalyptus open-source cloud-com- puting system. In: 9th IEEE/ACM International Symposium on Cluster Computing and the Grid, 2009. CCGRID'09, pp 124–131
15. Shafiq B, Joshi JB, Bertino E, Ghafoor A (2015) Secure interoperation in a multidomain environment employing RBAC policies. Knowl Data Eng IEEE Transactions 17(11):1557–1577
16. Almutairi AA, Sarfraz MI, Basalamah S, Aref WG, Ghafoor A (2011) A distributed access control architecture for cloud comput- ing. IEEE Softw 2:36–44
17. Ruj S, Nayak A, Stojmenovic I (2011) Dacc: distributed access control in clouds. In: 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 I.E., pp 91–98
18. Namasudra S, Nath S, Majumder A (2014) Profile based access control model in cloud computing environment. In: IEEE International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), 2014, pp 1–5
19. Musca C, Ion A, Leordeanu C, Cristea V (2013) Secure access to cloud resources. In: Eight IEEE International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013, pp 554–558
20. David C (2009) Introducing the Windows Azure Platform
21. Khaled A, Husain MF, Khan L, Hamlen KW, Thuraisingham B (2010) A token-based access control system for RDF data in the clouds. In: Second International Conference on Cloud computing technology and science (CloudCom), 2010
22. Yu S, Wang C, Ren K, Lou W (2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In: INFOCOM, 2010 Proceedings IEEE
23. Yu S, Ren K, Lou W, Li J (2009) Defending against key abuse attacks in kp-abe enabled broadcast systems. In. Security and Privacy in Communication Networks. Athens, Greece, 2009.
24. Ateniese G, Kevin F, Matthew G, Susan H (2006) Improved proxy re-encryption schemes with applications to secure distributed storage. In: ACM Transactions on Information and System Security., pp 1–30
25. Toshihiko M (2007) Proxy re-encryption systems for identity-based encryption. In. Pairing-Based Cryptography Pairing. Tokyo, Japan, LNCS, pp 247–267

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

26. Yang K, Jia X (2012) Attributed-based access control for multi- authority systems in cloud storage. In: 32nd International Conference on Distributed computing systems (ICDCS), 2012
27. Liu X, Xia Y, Jiang S, Xia F, Wang Y (2013) Hierarchical attribute- based access control with authentication for outsourced data in cloud computing. In: 12th IEEE International Conference on Trust, security and privacy in computing and communications (TrustCom), 2013, IEEE., pp 477–484
28. Lin G, Wang D, Bie Y, Lei M (2014) MTBAC: a mutual trust based access control model in cloud computing. Communications China 11(4):154–162
29. Eric S, Bruce D, Hégarat-Mascle SL (2002) Application of ant colony optimization to adaptive routing in aleo telecomunications satellite network. Ann Telecommun 57:520–539
30. Brucker AD, Brugger L, Kearney P, Wolff B (2011) An approach to modular and testable security models of real-world health-care ap- plications. In: Proceedings of the 16th ACM symposium on access control models and technologies, ACM., pp 133–142
31. Suhendra V (2011) A survey on access control deployment. In. Security Technology, Korea, Springer 2011, pp. 11–20.
32. Buyya R, Ranjan R, Calheiros R (2009) Modeling and simulation of scalable cloud computing environments and the CloudSim toolkit: challenges and opportunities, CoRR., pp 1–11
33. Buyya R, Calheiros R, Ranjan R, Rose CD (2009) CloudSim: a novel framework for modeling and simulation of cloud computing infrastructures and services, CoRR, Technical Report GRIDS-TR- 2001-1, Grid Computing and Distributed Systems laboratory, The University of Melbourne, Australia, March 2009
34. Calheiros R, Rajiv R, Anton B, César DR, Rajkumar B (2011) CloudSim: a toolkit for modeling and simulation of cloud comput- ing environments and evaluation of resource provisioning algo- rithms. Software: Practice and Experience 41:23–50