Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 14 Issue 1 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Kerberos: Secure Single Sign-on Authentication Protocol Framework for Cloud Access Control

By Yaser Fuad Al-Dubai & Dr. Khamitkar S. D
Swami Ramanand Teerth Marathwada University, India

Abstract- Cloud is a relatively new concept, so it is unsurprising that the security of information and data Protection concerns, network security and privacy still need to be addressed fully. The cloud allows clients to avoid hardware and software in Investments, gain flexibility, and cooperation with others, and to take advantage of sophisticated Services. However, security is a big problem for cloud clients especially access control; client profiles management and access services provided by public cloud environment. This article we are proposing an authentication model for cloud based on the Kerberos V5 protocol to provide single sign-on and to prevent against DDOS attacks in the access control system. This model could benefit by filtering against unauthorized access and to reduce the burden, computation and memory usage of cloud against authentication checks for each client. It acts as a trust third party between cloud servers and clients to allow secure access to cloud services. In this paper we will see some of the related work for cloud access control security issues and attacks. Then in next section we will discuss the proposed architecture.

Keywords: role based access control, authentication protocol, authentication server, key distribution centre, single sign-on.

GJCST-B Classification: C.2.2

Strictly as per the compliance and regulations of:

Kerberos: Secure Single Sign-on Authentication Protocol Framework for Cloud Access Control

Yaser Fuad Al-Dubai [α] & Dr. Khamitkar S. D [σ]

Abstract- Cloud is a relatively new concept, so it is unsurprising that the security of information and data Protection concerns, network security and privacy still need to be addressed fully. The cloud allows clients to avoid hardware and software in Investments, gain flexibility, and cooperation with others, and to take advantage of sophisticated Services. However, security is a big problem for cloud clients especially access control; client profiles management and access services provided by public cloud environment. This article we are proposing an authentication model for cloud based on the Kerberos V5 protocol to provide single sign-on and to prevent against DDOS attacks in the access control system. This model could benefit by filtering against unauthorized access and to reduce the burden, computation and memory usage of cloud against authentication checks for each client. It acts as a trust third party between cloud servers and clients to allow secure access to cloud services. In this paper we will see some of the related work for cloud access control security issues and attacks. Then in next section we will discuss the proposed architecture.

Keywords: role based access control, authentication protocol, authentication server, key distribution centre, single sign-on.

I. Introduction

Cloud computing and cloud technology is the dominant and highly paced technology of present scenario with the highly robust service infrastructure that can provide cloud based integrated services like service on demand for resource computation, storage or cumulative storage of resource or data and exceedingly vigorous network communications in the cloud technology[1], the calculations of possessed resources are assumed and are facilitated as the services over the communication channels or the internet services. Few specific scientific societies also states cloud computing in diverse description, such as "a service infrastructure that operates for facilitating an omnipresent, convenient, on demand resource access of certain distinct network to a collective collection of computing resources and system frameworks [2]. For getting the proficient cloud based services over internet services it can provide a swift and decidedly proficient system with least resource administration activities and minimum interface of service providers. Most of current application require the client to memorize and utilize different set of credentials (e.g. client name/password or tokens) for each application he/she wants to access. However, this approach is inefficient and insecure with the exponential growth in the number of applications and services a client has to access both inside corporative environments and at the internet. Mainly, it is difficult for a corporation to manage potentially multiple authentication solutions and databases individually used by each application. Furthermore, most clients tend to rely on the same set of credentials for accessing all of their systems, posing a serious security threat since an attacker who discovers these credentials can easily access all of the client's applications [3].

In a single sign-on platform, the client performs a single initial (or primary) sign-on to an identity provider trusted by the applications he wants to access. Later on, each time he wants to access an application, it automatically verifies that he is properly authenticated by the identity provider without requiring any direct client interaction. Single sign-on solutions eliminate the need for clients to repeatedly prove their identities to different applications and hold different credentials for each application. Furthermore, a well designed and implemented single sign-on solution significantly reduces authentication infrastructure and identity management complexity, consequently decreasing costs while increasing security [4].

The dominant problem with cloud computation is its access control mechanism for ensuring security information and overall system security. for controlling an assortment of time-sensitive actions frequent cloud utilities such as workflow management and the operations with real-time databases, the characteristics of access control are needed so as to be improved with the most favorable and efficient temporal constraints. in this paper work and the developed system framework the system optimization has been aggravated by the prerequisite of a decidedly vigorous and efficient access control scheme that could congregate and can assuage the protection concerns in cloud environment with enhanced trust intensity for abundant cloud based applications and numerous service segments.

Kerberos authentication protocol the ticket and the authenticator. This leads to a discussion of the two authentication protocols: the initial authentication of a client to Kerberos (analogous to logging in), and the protocol for mutual authentication of a potential

Authors α σ: School of Computational Sciences Swami Ramanand Teerth Marathwada University, Nanded India.
e-mail: yaseraldubai@gmail.com

consumer and a potential producer of a network service. This paper we are proposing an authentication model for cloud based on the Kerberos v5 protocol to provide single sign-on and to prevent against DDOS attacks in the access control system and benefit by filtering against unauthorized access and to reduce the burden, computation and memory usage of cloud against authentication checks for each client. it acts as a trust third party between cloud servers and clients to allow secure access to cloud services.

The rest of this article is organized as the following: section 2 discusses the problem statement challenges and issues, section 3 discusses the review related work, section 4 designed the Kerberos authentication with role based access control KARBAC framework for cloud applications, section 5 Kerberos for single sign-on authentication, finally in section 6 obtain the advantages of proposed framework.

II. Proplem Statement

In enterprise systems, a pressing issue is the lack of an efficient, generic application-level model that supports unified access control frameworks for client-to-system interactions. Traditional security models are not capable of addressing some of the new challenges posed by modern enterprise systems. One of the problems is that most of the existing security models are influenced by the subject operation object paradigm. A typical feature of the paradigm is that permissions are forwarded in state of the accessible permission to certain participants or beneficiary in particular access modes. Such kinds of type of permission representation have made the security management of enterprise systems more complicated because of the heterogeneous characteristics of the resources being available in authentication. Therefore, they are not appropriate for sustaining a integrated access control architecture that takes into consideration of diverse resources from numerous domains [5].

We important aspect of an access control model is the capability to prop up an extensive assortment of precautions policies. In a distributed system, a variety of security policies are specified to ensure data confidentiality and integrity, and to convey business rules, some of them must be specified in a fine-grained manner. As for one illustration, in case one cloud client ass or requests for access its allied service, but it can get access to once certain defined part of overall service, be delivering permission or unwelcoming the client request would be unfortunate. In a similar case, a service can only be accessed within a certain time frame. A security system is required to provide more precise authorization services to satisfy both business requirements and security requirements of the enterprise. However, current business applications/ systems do not have a systematic way of defining access control to such fine granularity. The existing RBAC models and their extensions are unable to provide fine-grained access control for enterprise systems, such as controlling the content of client input and system output.

III. Related Work

This is matter of fact that in any research activity the exploration and deep study of existing approaches plays a significant role, therefore consideration this factor in mind the author of this thesis has performed a deep rooted survey for the role based access control mechanism and specially the access control approaches to be employed for cloud environment. The study made on existing systems provides the well-defined and crisp knowledge about the strength as well as the weakness of the existing approaches and thus the new optimum system can be built. The literature survey conducted for role based access control and its allied processes has been given in this section, as follows:

Lan Zhou et al [6] addressed trusted administration and enforcement of role-based access control policies on data stored in the cloud. Role-based access control (RBAC) simplifies the management of access control policies by creating two mappings; roles to permissions and clients to roles. Recently crypto-based RBAC (C-RBAC) schemes have been developed which combine cryptographic techniques and access control to secured data in an outsourced environment [7]. In such schemes, data is encrypted before outsourcing it and the cipher text data is stored in the untrusted cloud. This cipher text can only be decrypted by those clients who satisfy the role-based access control policies. However such schemes assume the existence of a trusted administrator managing all the clients and roles in the system. Such an assumption is not realistic in large-scale systems as it is impractical for a single administrator to manage the entire system. Though administrative models for RBAC systems have been proposed decentralize the administration tasks associated with the roles, these administrative models cannot be used in the C-RBAC schemes, as the administrative policies cannot be enforced in an untrusted distributed cloud environment. In this paper, the researchers proposed a trusted administrative model AdC-RBAC to manage and enforce role-based access policies for C-RBAC schemes in large-scale cloud systems. The AdC-RBAC model uses cryptographic techniques to ensure that the administrative tasks such as client, permission and role management are performed only by authorized administrative roles. Their proposed model uses role-based encryption techniques to ensure that only administrators who have the permissions to manage a role can add/revoke clients to/from the role and owner-

can verify that a role is created by qualified administrators before giving out their data. We show how the proposed model can be used in an untrusted cloud while guaranteeing its security using cryptographic and trusted access control enforcement techniques.

IV. Designed Framework

After an analysis of the relevant existing work we have designed the Kerberos Authentication with Role Based Access Control KARBAC framework for cloud applications. Figure 1 shows the design of the it's easy for clients to protect their resources in accordance with its security and access control requirements.

The designed framework provides a policy specification module to Cloud clients to define access control on its resources using RBAC policy format then the Kerberos authorization server component stores and generate access control decisions based on the RBAC policy file [8].

The framework implements various time-based semantics of temporal hierarchies and separation of duty constraints or that is effective to perform well even in minimality situations. It explained the detailed of the components and the Kerberos protocol required for communication between these components as follows:

a) Cloud Client

a cloud client is a person or entity who uses various cloud applications deployed by vendors of various cloud services to its customers. Cloud client creates stores and shares resources with other applications or clients. Module specifications policy exists on the client's computer to provide client interface and tools to create, edit and manage access control to resources. And policies are dynamically formed in back end using RBAC policy. Policy specifications module act as policy information point (PIP) in Designed System.

b) Authentication Protocol

The authentication protocol is responsible for verifying client identities. Authentication is provided as a guest service in the system design, and can be achieved via any standard authentication protocol. In this solution, we recommended Kerberos V5 authentication protocol also at the same time called as Key Distribution Centre (KDC). Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server have used Kerberos to prove their identity, they can also encrypt all their communications to assure privacy and data integrity, as they go about their business[9,10]. The KDC contain of two main steps as we illustrate as the following :

- Authentication Server (AS): The first step of the KDC is AS. Cloud client (principal) initially requests a ticket to the KDC by giving it is name, an expiration time until when the authentication will remain valid, the cloud service required (tgs) and some other information, is not mentioned here for clarity the KDC if found the cloud client in it is database, replies with two steps:

– Cloud client ticket contains a session key SA, KDC, the expiration time and it is tgs cloud service name, all encrypted using the secret key of the principal KA. The expiration time usually working day or eight hours, gives a period of time during which the tickets will be valid.

– Granting ticket contains the session key SA, KDC, the expiration time and the name of the cloud customer, all encrypted using the secret key for the KDC. This is what is known as a TGT. The principal unable to decrypt the TGT, and will be used later to request tickets for the other cloud services. As it is encrypted the cloud customer cannot read the data inside. If tries to modify it, the KDC will not be able to decrypt it and it will be refused.

- Ticket Granting Server (TGS): The second step of the KDC is the distribution of tickets it called the TGS. Once authenticated the cloud client who requests a specific application such as telnet or FTP first asks the KDC. It does not query the cloud service directly. This request to the KDC it contains several fields:

– An authenticator consist of: a timestamp and checksum encrypted with the session key SA, KDC, which was obtained earlier in the KDC, shared between the cloud customer and the KDC. This proves the identity of the cloud customer since he is the only one to know this session key. The checksum proves the authentication message has not been modified during the transiting. The timestamp confirms the message is recent, and is used to prevent "reply" attacks, since anyone can Interception of data across the network and use it at a later time. Typically, the KDC must responds within five minutes for a message to be accepted. This is why it is important to have a good time synchronization across your network where is implemented the Kerberos AS to the cloud computing. Consider the use of Protocol such as NTP (Network Time Protocol) to keep it accurate.

– TGT received during the authentication exchange with the KDC. It is used by the KDC to verify the cloud customer's name. If the cloud client name present in the TGT does not match with related the session key and this means the cloud client has been impersonated and the KDC is unable to decrypt the authenticator. Also the KDC verifies the validly by checking the expiration time of the authentication.

– The Cloud Server name to which the cloud client wants to establish a connection.
– An expiration time for the TGT.

The KDC responses to the cloud client (principal) with two tickets:

– The cloud client ticket contains a new session key SA, B that the cloud customer and the cloud server will be used to verify each other's identity and to encrypt their sessions. The ticket also encloses the cloud service name and the expiration time of the new ticket. All of these items encrypted using the key SA, KDC shared between the cloud client and the KDC, known only to the cloud client.
– The server ticket that contains the same session key SA , B as mentioned above , the cloud client's name and time of the expiration of the ticket . The server ticket being encrypted with the cloud service's secret key KB, only known to the server. It is then under the responsibility of the cloud client to send a server ticket to the cloud server.

c) Gateway

This component acts as a proxy between the clients of cloud and the components designated for the security services. It manages connections and sessions for cloud clients and deal with access requests to the cloud applications and gets access control decisions from the authorization server. Since this component intercepts all messages between the various components, so we also added Policy Enforcement Features in it.

d) Authorization Server

The Authorization server then stores access control policies defined by the clients of cloud (in terms of resources) and cloud applications (regarding registered clients). It also generates access control decisions based on those policies stored using RBAC policy engine. It consists of a policy storage module that stores and manages access control policies, and working as a Policy Administration Point (PAP) and Policy Retrieval Point (PRP) in System Designer. Authorization server also contains a policy decision module which is a Policy Decision Point (PDP), it creates access control decisions by evaluating access request against the stored policies. It also implements various time-based semantics of temporal hierarchies and separation of duty constraints or SoDs that is effective to perform well even in minimality situations.

e) Cloud Application

the cloud application provides cloud clients different services. It allows them to create, upload and share resources (documents, files, images, etc.) with other clients or applications. The designed framework the cloud application has a delegated it access control functionality to the client and authorization server. All access control decisions are created by authorization server on behalf of a cloud application. It contains a repository of resources, and is only responsible for storage resources that are created or uploaded by clients.

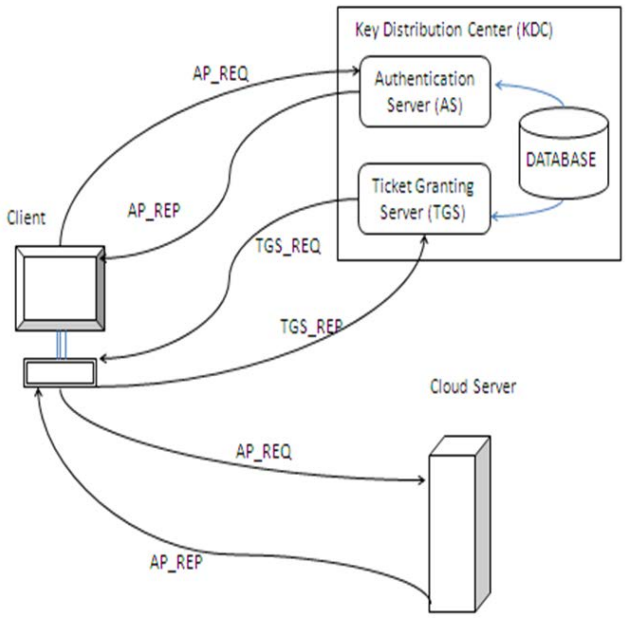

Figure 1 : Kerberos Authentication with Role Based Access Control

V. Kerberos for Single Sign-on Authentication

The main Aim of this model is for the authentication clients before access to the service and to find the source of the attack DDOS. Check your client name and password just is not enough for the cloud computing environment, such as distributed and shared. Kerberos is a network authentication protocol and provides a single sign-on facility to clients as well. Kerberos was one of the first single sign-on solutions proposed in the literature and implemented as a network service. It is formally described as a network authentication system, initially designed for providing single sign-on to network services.

A Kerberos "realm" infrastructure is composed by an Authentication Server, a Ticket Granting Server and a set of service providers. The Authentication Server is responsible for verifying the user's identity while the Ticket Granting Server generates tickets for authenticated users [11]. The service providers are simply networked servers that authenticated users are allowed to access. The two servers act together as an identity provider, handing the user an authentication ticket that he can use to sign-on to the relying service providers. In fact, the sign-on process in Kerberos is extremely complex, requiring several interactions between the user and the servers (which can be combined into an identity provider).

Although it provides a nice practical single sign-on solution, Kerberos infrastructure management is extremely complex, being prone to several mistakes that may severely compromise security. Both the identity provider (composed by the Kerberos servers) and all the service providers must be tightly time synchronized. These rules out the utilization of Kerberos as a single sign-on framework for distributed applications that may reside in the internet or the cloud. Furthermore, Kerberos relies solely on unproven symmetric encryption mechanisms to authenticate users and maintain session state. It may also be possible to impersonate users and steal authentication tickets through simple network based attacks.

VI. Advantages of Proposed System

- All the encryptions could be done using the proposed cryptographic algorithm. Since the current Kerberos system uses a standard symmetric key encryption algorithm.
- It is easy for an intruder to find out the key and decrypt. But when the proposed system is used, only the authorized persons, who have the decryption algorithm, could only decrypt the encrypted text. Any other intruder, who wants to perform off-line attack, will not be able to do so because this algorithm protects the message in a much stronger way using variable block cipher with cipher block chaining mode.
- It is very difficult to decrypt the message even with the algorithm available. Because this algorithm gives an extra layer of protection with a password. The chances of password guessing approach for any intruder are nullified because the proposed system does not store the password of the client anywhere in the hard disk. Hence no attempt can be made to find it out.
- By integrating the proposed system with the smart card technology, some of the Kerberos systems problems may be overcome.
- The whole idea is to enhance the security of Kerberos authentication by authenticating the client directly at the beginning and before the granting of the initial ticket, so that one client cannot have the ticket of another. And, the use of smart card requires client logging into the system not only by recalling a password, but also to be in possession of a token.

Another way to enhance security is to use biometric technology with the proposed system in the smart card. Biometrics information of the cardholder can be placed on the card, so that the smart card can corporate with biometrics scanner to authenticate the client directly at the first stage of processing. Before granting the initial ticket, this authentication could take place, to avoid any intruder to pretend as the cardholder. The proposed system, which combines the techniques of cryptography and steganography, could be applied to embed the biometrics information of the cardholder into his photograph in the smart card. Since this algorithm provides a robust protection to the information against attacks, the biometrics details could not be easily trapped by any fraudulent.

VII. Conclusion

In this paper we have designed the Kerberos Authentication with Role Based Access Control framework for cloud applications also we present the problem of the access control security which effected on cloud environment , which is Essentially easy for clients to protect their resources in accordance with its security and access control requirements. The proposed framework provides a policy specification module to cloud clients to define access control on its resources using RBAC policy format then the Kerberos authorization server component stores and generate access control decisions based on the RBAC policy file .also we are designed an authentication framework for cloud based on the Kerberos V5 protocol to provide single sign-on and to prevent against DDOS attacks in the access control system. Although benefit by filtering against unauthorized access and to reduce the burden, computation and memory usage of cloud against authentication checks for each client. It acts as a trust third party between cloud servers and clients to allow secure access to cloud services.

References Références Referencias

1. Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing V3.0”, http://www.Cloudsecurityalliance.org/guidance/csaguide.v3.0. pdf.
2. Wayne Jansen, Timothy Grance, “Guidelines on Security and Privacy in Public Cloud Computing” NIST, NIST Special Publication 800-144; December 2011.
3. D. Catteddu and G. Hogben, “Cloud Computing: Benefits, risks and recommendations for information security”, ENISA2009, http://www.enisa.europa.eu/activities/riskmanagement/files/de liverables/Cloud-computing-risk-assessment/at download/fullReport.
4. Todd Steiner, Hamed Khiabani “An IntroductionTo Securing a Cloud Environment”, SANS institute 2012.
5. H. Takabi, J. B. D. Joshi, and G. J. Ahn, “Security and Privacy Challenges in Cloud Computing Environments”, IEEE Security and Privacy, Vol. 8, No. 6, pp. 25-31, 2010.
6. Lan Zhou; Varadharajan, V.; Hitchens, M., "Trusted Administration of Large-Scale Cryptographic Role-Based Access Control Systems," Trust, Security and Privacy in Computing and Communications

(TrustCom), 2012 IEEE 11th International Conference on , vol., no., pp.714,721, 25-27 June 2012.

7. Jin Wang; Daxing Li; Qiang Li; Bai Xi, "Constructing Role-Based Access Control and Delegation Based on Hierarchical IBS," Network and Parallel Computing Workshops, 2007. NPC Workshops. IFIP International Conference on , vol., no., pp.112,118, 18-21 Sept. 2007.
8. R. S. Sandhu, E. 1. Coyne, H. L. Feinstein, and C. E.Youman., "Role based access control models" IEEE Computer, Vol. 29, No.2, pp. 38-47, February 1996.
9. Armbrust M., Fox A., Griffith R., Joseph A.D., Katz R.H., Kon-winski A., Lee G., P " Above the Clouds: A Berkeley View of Cloud Computing" URL: http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf . 2009.
10. S. M. Bellovin and M. Merritt. "Limitations of the Kerberos Authentication System". Usenix Conference. URL:http://academiccommons.columbia.edu/download/fedora_content/download/ac:127107/CONTENT/kerblimit. usenix. pdf. January 1991.
11. http://www.datadirect.com/solutions/security/kerberos/index.html.