KERBEROS AUTHENTICATION WITH CLOUD COMPUTING ACCESS CONTROL

[1]SANTOSH KHAMITKAR, [2]YASER FUAD AL-DUBAI, [3]PARAG BHALCHANDRA, [4]PAWAN WASNIK

[1,2,3,4]School of Computational Sciences, S.R.T.M. University, Nanded, MS, 431606
E-mail: srtmun.parag@gmail.com

Abstract- Cloud computing 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 computing 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 computing clients especially access control; client profiles management and access services provided by public cloud computing environment. This article we are proposing an authentication model for cloud computing 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 computing against authentication checks for each client. It acts as a trust third party between cloud computing servers and clients to allow secure access to cloud computing services. In this paper we will see some of the related work for cloud computing access control security issues and attacks. Then in next section we will discuss the proposed architecture.

Keywords- Cloud, Role Based Access Control, Authentication Protocol, Key Distribution

I. INTRODUCTION

Cloud computing technology is the dominant and highly paced technology of present scenario with the highly robust service infrastructure that can provide cloud computing 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 computing 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 computing 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 applications 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. Kerberos 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 computing computation is its access control mechanism for ensuring security information and overall system security. For controlling an assortment of time-sensitive actions frequent cloud computing 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 computing environment with enhanced trust intensity for abundant cloud computing 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 consumer and a potential producer of a network service. This paper we are proposing an authentication model for cloud computing 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 computing against authentication checks for each client. It acts as a trust third party between cloud computing servers and clients to allow secure access to cloud computing 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 computing applications, and finally in section 5 obtain the results of proposed framework.

II. PROBLEM 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 computing client assignment 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 computing 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 un-trusted 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 un-trusted distributed cloud computing 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 computing 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 un-trusted cloud computing 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 computing applications. Figure 1 shows the design of the KARBAC 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 computing 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 minimalist 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 computing client is a person or entity who uses various cloud computing applications deployed by vendors of various cloud computing services to its client. Cloud computing 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:

I) Authentication Server (AS): The first step of the KDC is AS. cloud computing 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 computing service required (tgs) and some other information, is not mentioned here for clarity the KDC if found the cloud computing client in it is database, replies with two steps:

1. cloud computing client ticket contains a session key SA,KDC, the expiration time and it is tgs cloud computing 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.
2. Granting ticket contains the session key SA, KDC, the expiration time and the name of the cloud computing client/user, 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 computing services. As it is encrypted the cloud computing client/user cannot read the data inside. If tries to modify it, the KDC will not be able to decrypt it and it will be refused.

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

1. An authenticator consists of a timestamp and checksum encrypted with the session key SA, KDC, which was obtained earlier in the KDC, shared between the cloud computing client/user and the KDC. This proves the identity of the cloud computing client/user 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.

2. TGT received during the authentication exchange with the KDC. It is used by the KDC to verify the cloud computing client/user's name.

If the cloud computing client name present in the TGT does not match with related the session key and this means the cloud computing 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.

3. The cloud computing Server name to which the cloud computing client wants to establish a connection.
4. An expiration time for the TGT.

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

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

C. Gateway

This component acts as a proxy between the clients of cloud computing and the components designated for the security services. It manages connections and sessions for cloud computing clients and deal with access requests to the cloud computing 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 computing (in terms of resources) and cloud computing 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 SoD that is effective to perform well even in minimalist situations.

E. Cloud computing Application

The cloud computing application provides cloud computing client's 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 computing 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 computing application. It contains a repository of resources, and is only responsible for storage resources that are created or uploaded by clients.

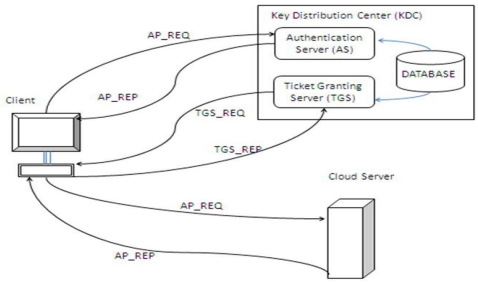


Figure 1: Kerberos Authentication with Role Based Access Control

V. RESULTS AND DISCUSSIONS

In this research work a Kerberos Authentication with Role Based Access Control "KARBAC" model has been developed for highly competitive and secured cloud computing environment. The system model existing has been developed with C# programs and Visual Basic 2010 framework. The overall system has been developed and implemented with Amazon S3 cloud platform. The developed system has been simulated for different performance parameters like Kerberos authentication, induction of roles and user creation. The relative study for these all factors has been performed. The model performance has been verified for various user size with dynamic role assignments and the relative throughout as well as performance parameters have been checked for its robustness justification.

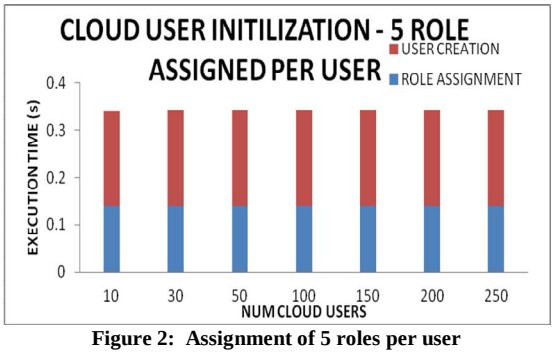


Figure 2: Assignment of 5 roles per user

The above mentioned figure (Figure 2) depicts the initialization of users for five respective role assignments and here from the figure it is clear that the role assignments could be better as per the number of increased users. Referring to (Figure 3) and comparing it with previous figure it could be found that with higher users the time for user creation varies linearly but there occurs certain variation in user creation time with increase in assignment of role. The creation time decreases as per increase in higher count of cloud users.

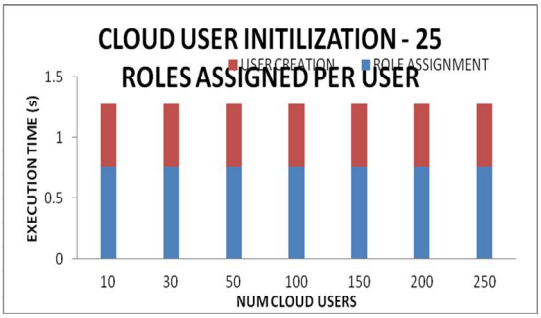


Figure 3: Assignment of 25 roles per user

Going through the results obtained and performing a cloud environment analysis, it could be easily figured out that in real time operation of cloud environment, the system could be made more flexible and it could be operated even with the minimalist of constraints and the expressiveness of the system makes it high robust in terms of secure and efficient user creation, role generation and its allied permission assignment. Thus, the proposed KARBAC approach has exhibited better in terms of numerous performance parameters in real time cloud environment and not only the performance but this system has achieved optimum solution for security in multiple user cloud applications.

CONCLUSIONS

In this paper we have developed the Kerberos Authentication with Role Based Access Control framework for cloud computing environments 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 computing 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 developed 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

[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. 2011.

[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”, http://www.enisa. europa.eu/activities/riskmanagement/files/de liverables/ Cloudcomputing risk-assessment/at download/fullReport, ENISA2009,.

[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, 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_conten t/download/ac:127107/CONTENT/kerblimit. usenix. pdf. January 1991.



Parag Bhalchandra is an Assistant Professor at School of Computational Sciences, SRTM University, Nanded, MS, India. He has 10+ research papers in international journals and conferences. He has participated in more than 20 conferences and workshops. His research interest includes Algorithms, Data mining



Dr.Santosh Khamitkar is an Associate Professor at School of Computational Sciences, SRTM University, Nanded, MS, India. He has 30+ research papers in international journals and conferences. He has participated in more than 10 conferences and workshops. His research interest includes Network Security, Algorithms and ICT. He is a research supervisor and has guided 5 PhD students


Mr.Yaser Al Dubai is a PhD Research Scholar at School of Computational Sciences, SRTM University, Nanded, MS, India. He has 9+ research papers in international journals and conferences. He has participated in more than 05 conferences and workshops. His research interest includes Cloud Computing and Network Security


Mr.Pawan Wasnik is a M.Phil Research Scholar at School of Computational Sciences, SRTM University, Nanded, MS, India. He has 3+ research papers in international journals and conferences. He has participated in more than 03 conferences and workshops. His research interest includes Data Mining and Algorithms.

★★★