International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Kerberos Authorization with Hybrid Access Control Model in Public Cloud

Ashok Kumar J, Gopinath Ganapathy

Abstract: ***Access control and Data confidentiality are key technology to ensure the security of system and to protect the privacy of the users. The modified Collaborative Trust Enhanced Security (CTES) model has an inbuilt access control mechanism for Kerberos protocol itself to enforce the access control policy directly into the Client system node. This paper explains the hybrid access control model with Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC) for modified CTES framework through Kerberos protocol. Hence, it retains the concept of "role", "group" and "attributes" for the user which are necessary to protect data privacy in the system. Data confidentiality for the stored data in Cloud is achieved by cryptographic techniques. Gnu Privacy Guard (GnuPG) based certificate is capable enough to verify the identity of the correspondent in information exchange as well as the information integrity. It is a strongest authentication technique where the user is asked to provide his/her digital ID for validation in the Server and enables Single sign-on services for Kerberos Authorization in modified CTES model. In this paper, it is proposed for a new Kerberos Authorization with Hybrid Access Control Model (KAHAC) for single-domain systems and multi-domain systems in Public Cloud based on roles, attributes, groups, access modes and the type of resources.***

Keywords: Public Cloud, Kerberos Authentication, Role based Access Control, Attribute based Access Control, GnuPG.

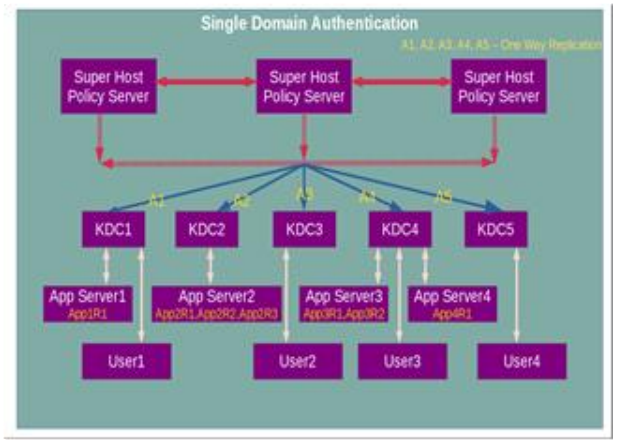
I. INTRODUCTION

The Cloud computing is a distributed computing paradigm, it provides the application services and resources to the users on pay-per use basis. The users outsource their data for computation in public cloud server and it results they are losing the physical control over the data. They are unable to resist certain type of attacks and threats over them. To secure the users data in public cloud, the Cloud Service Providers (CSP) shall protect the cloud server from different type of threats and attacks. It should be ensured that the CSP is trusted with the user before outsourcing the user's data. In paper [1], a novel framework was proposed for authentication and authorization of cloud services and resources, by modifying the CTES model. This proposed approach for the framework of CTES model has inbuilt access control policy for Kerberos protocol and altered the authentication based on secret image.

Manuscript published on November 30, 2019.
* Correspondence Author
Ashok Kumar J*, Research Scholar, Bharathidasan University, Engineering and Applications, School of Computer Science, Tiruchirappalli, Tamilnadu, India.
Dr. Gopinath Ganapathy, Registrar, Bharathidasan University, Tiruchirappalli, Tamilnadu, India.

II MODIFIED KERBERBEROS V AUTHENTICATION

In paper [2], the Kerberos protocol incorporates with Visual cryptography and GnuPG Public key Cryptography for client-based authentication (Fig I). The Visual cryptography is utilized for enforcing access control mechanism for authenticated user through secret image. For securely exchanging the secret image between the client and KDC, the GnuPG public key is used to encrypt and decrypt it. Moreover, the client private key is available in the client system itself and so the only responsibility of client to decrypt the image. It is more secure than the traditional authentication and secret image can hold enough data for access control information about the authenticating user to enforce it into the client system directly. In this paper, RBAC policy will be enforced through this secret image and ABAC policy is enforced with GnuPG Certificates.



(Fig I: A Modified Kerberos V Authentication)

III ACCESS CONTROL POLICY

It is used to restrict the user's access based on the set of procedures defined by CSP. Only an admitted user is able to access the resources and operation can be performed by him only on a particular resource [3]. In modified CTES model, super host records all the attempts made to access a system and provides the two kind of access control policy namely RBAC model and ABAC model. The RBAC policy is enforced through the secret image and ABAC policy is enforced through the Kerberos Single Sign-On techniques with GnuPG Certificates.

It also identifies the unauthorized access attempt by the user. This proposed KAHAC access control policy is designed to control each process with their own attributes, roles and capabilities in order to restrict the user and to protect the user's data and computation, cloud resources by controlling access to the resources and the system itself.

IV ROLE BASED ACCESS CONTROL (RBAC) MODEL

In RBAC model, Access control policy decisions are taken on the pre-defined set of roles for the user [4]. The idea in this model is to enable the user privileges based on their access permission and roles. A role is related to collection of users that have the same set of permissions or access mode. The permissions for the users can be enforced dynamically at role level and it has two advantages

a. Users can access their resources based on the role permission.

b. There is no need to do the redefining of role permission for each user and it makes easier the system administration task.

RBAC policy can be used to enforce the below two models in the system level.

1. Mandatory access control (MAC):

It is a procedure that a central authority can restrict the multiple level of access controls for the system resources or operating system's security kernel based on the information security clearance of the user or device to deny or grant permission [5].

2. Discretionary access control (DAC):

In the system, access control policy is decided by owner or administrator that who or what is authorized to access their resources [4].

In the proposed KAHAC model, the RBAC role permissions can be enforced with MAC model and DAC model for accessing their resources within an organization.

V. ATTRIBUTE BASED ACCESS CONTROL (ABAC) MODEL

In ABAC model, access control policy is taken on the user's attribute and it relates to below entities [4].

1. The set of users
2. The resources
3. The environment

All the above entities have specific user attributes for enforcing the access privileges into this. Thus, the users attribute may be the location, age, data of birth, role or all of them. Each attribute takes unique and discrete values. This proposed KAHAC model checks the users attribute with Kerberos Single Sign-on technique against the predefined policy of a particular systems or organization in order to make allow or deny access.

VI PRETTY GOOD PRIVACY (PGP)

PGP was developed by Philip R. Zimmermann [6]. GnuPG is an open source compatible encryption system based on OpenPGP. GnuPG encryption, uses combination of public key cryptography, data compression, hashing and symmetric-key cryptography. It is used in several security constraints such as confidentiality, integrity and authentication for electronic mail and file storage applications etc., [7]. GnuPG creates the digital signature for the given data to verify the authenticity of the sender. Sender sends the hash digest along with the given data to the receiver. Then receiver uses the sender's public key to verify the digital signature. If it matches the digital signature, it will be confirmed that it is from the expected sender. GnuPG subkeys [8] are like the normal key pair associated with the main key pair used for signing or for encryption except they're bound to a master key pair. It can be revoked independently of the master keys, and also stored separately from them.

The four trust levels are existing in users certificate holder's signature to introduce other users' certificates:

1. Mode Level 4: Fully trusted
2. Mode Level 3: Marginally trusted, but to confirm with full trust
3. Mode Level 2: Untrustworthy
4. Mode Level 1: Don't Know

It is proposed a new Kerberos Authorization with ABAC model and RBAC model for modified CTES framework through Kerberos protocol. This proposed hybrid access control policy retains the concept of" role", "group" and" attributes" for the user which are required to protect data privacy in the system nodes.

VII RELATED WORKS

Many of the research have adopted the benefit of using the RBAC model and ABAC model based on the announcement from the NIST organization and the security of the both models are derived by them [9].

Different access policy is proposed by Ryan et al. [10] for the different users and groups in the desktop operating system to access the cloud server. The main problem of this scheme is to maintain the whole system.

The minimum amount of role permissions is proposed by David et al. [11] to complete a job based on the RBAC model. The main problem of this scheme is to extend the RBAC model across administrative domain of the organization.

This paper [12] Role-centric Attribute-Based Access Control (RABAC) avoids the problem of role-explosion by assignment of roles with permission filtering policy (PFP) based on user and object attributes.

AERBAC (Attributes Enhanced Role-Based Access Control) is proposed to overcome the difficulties of incorporating the environment attributes and frequently changing attributes in the RABAC approach. It uses contextual information and exploits the contents of the resources to provide fine-grained access control mechanism [13].

The secure communication is proposed by Xiaowei et al. [14] between user and CSP. The main problem of this scheme is that the Data Owner (DO) should be always online when user wants to access data. A purpose-based access control model is purposed by Lili et al. [15] to check the access request purpose with respect to intended purposes and grants access based on the authorization. It does not deal with further operations needed for accessing the data.

VIII PROBLEM STATEMENTS AND THEIR SOLUTIONS FOR ABAC AND RBAC

1. The cloud users are subscribed to multiple services in Public Cloud. It results multiple user authorization policy. The possible solution is to user Kerberos single sign-on with the user authorization.

2. The CSP can define RBAC policy based on their roles instead on an individual basis for small or medium-sized organization. But it is not feasible to setup the policy for the lager organizations.

4. In ABAC model, the user policies are pre-defined access policy whereas the RBAC model, the user policies are defined dynamically. The possible solution is to integration of cross-grained and fine-grained access control policy helps to process the different level of security for the organization.

5. The access policy of the outsourced data can be changed in local site only by the data owner for updating a newly defined access policy. It also needs the encryption of data with this newly defined access policy. It results in heavy computation and communication overhead. The KAHAC model incorporates mutual authorization policy for data user and data owners to define access policies.

6. The Data Owner must be always online when the user accesses the data in the Public Cloud.

IX IDEA BEHIND THIS PROPOSED KERBEROS AUTHORIZATION WITH HYBRID ACCESS CONTROL MODEL (KAHAC)

The authorization is the process of allowing the access policies to the services depending on user authentication. Kerberos Single Sign-On allows user to authenticate only once and allows to use all services and resources available to them afterwards. In public cloud, CSP can define the policies for the user through super host and Kerberos Single Sign-On technique. Only the authorized user can access the services and resources defined by the CSP. Thus, Kerberos Single Sign-On access privileges are managed properly to access SSO-enabled services and resources.

It is proposed a new Kerberos Authorization with Hybrid Access Control Model (KAHAC) for single-domain systems and multi-domain systems with the following considerations.

1. A role can be user attributes such as an email id. The “role” attribute is used to mark a set of attributes required for a certain position. It is to be designed for RBAC, to accommodate additional constraints being placed on a role. The possible solution to enforce the RBAC policy is with the secret image for modified CTES model.

2. Attributes are added to constrain roles. Role can be named as attribute and reduced the permissions to the user. This approach strengthens the security of the shared data in the Public Cloud. The possible solution to enforce the ABAC policy is with the GnuPG based certificates. A GnuPG subkey can be created in the Client system based on the attribute name for encrypting the data. This subkeys are like a separate key pair and associated with the main key pair. This encrypted data based on attribute name data can be shared with the CSP and it resolves to identify the user data by using ABAC policy in the storage server.

X PROPOSED MODEL KERBEROS AUTHORIZATION WITH HYBRID ACCESS CONTROL MODEL (KAHAC)

Whenever the user login into the system node, GnuPG user process is started and Kerberos authentication is performed automatically for the modified CTES framework, then the embedded secret image (contains RBAC access policy) from superhost is downloaded in to client node. This embedded RBAC user policy in the secret image changes the behavior of the user policies including roles, groups and access modes in the system. The later Kerberos authorization called as Singl Sign on (SSO) enables to validate the ABAC policy model with the GnuPG based certification key from the super host. Thus, the ABAC access policy is dynamically apply the rules based on roles, attributes and the type of resources in the Public Cloud. This proposed Kerberos Authorization with Hybrid Access Control Model (KAHAC) can be used in single domain as well as multiple domain authorization for enhancing the security in the Public Cloud.

1. Single Domain authorization

a. RBAC model with embedded Secret Image:

Client can access the services of the cloud environment to authenticate with Kerberos Server and then download the embedded secret image (RBAC policy) from the SuperHost. The picture (Fig 2) describes the top-level view of interaction in between the SuperHost and KDC systems. The CSP can define the access policy in SuperHost to manage the registered Application server and client. The KDC system is placed in front of the SuperHost to authenticate the users for the application services and to provide the access control rights for accessing the cloud resources in the cloud environment. The changes in each user access right privileges through secret image will be replicated in one-way direction that is from the SuperHost to the KDC system.

Within an organization, RBAC roles are created for various job functions by the CSP Administrator. This permissions like access modes (based on DAC model) and roles (based on MAC model) are performed for certain operations which are assigned to specific roles. The system users are assigned particular roles, and through those role assignments acquire the permissions needed to perform particular system functions. The user appropriate roles are assigned to the user’s account through this secret image; this simplifies common operations, such as adding a user, or changing a user's privilege rights.

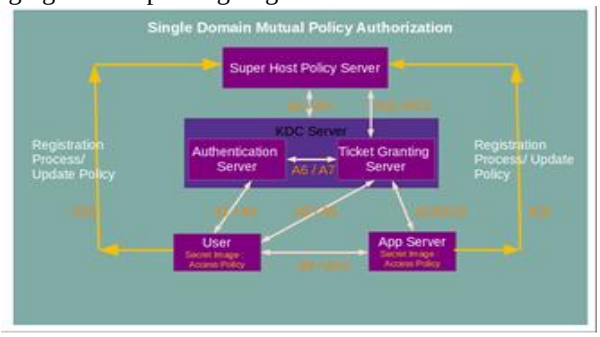


Fig 2: Single Domain Mutual Policy Authorization

The interacting messages (Fig 2) used among the different servers are:

1. The message A4 carries the secret image for RBAC Policy from super host through KDC. This new access policy can be defined dynamically by the cloud service provider at SuperHost and it will get update in to the client system immediately.

2. The messages A10, A11, A12 and A13 validates the role attributes in the super host and update the Kerberos SSO message A6/A7 for user authorization in KDC. This new access policy gets validated and allowed to access the specific applications or resources in the Public Cloud.

b. ABAC model based on GnuPG Certificates:

ABAC is based on dynamic policy to define the access permission in the Public Cloud. It evolves from RBAC to consider additional attributes in addition to roles and groups. Attributes can be about anything and anyone. ABAC attributes are

1. Subject attributes (user attempting the access): It is based on attributes like age, department, role and job title.

2. Action attributes (action being attempted): It is based on attributes like read, delete, view and approve.

3. Object attributes (object or resource): It is based on attributes like medical record, bank account, the department and the location.

4. Contextual (environment) attributes: It is based on attributes like time, location or dynamic aspects of the access control scenario

Authorization in a cloud environment with the use of Kerberos Single Sign-On allows the CSP to define the access control policies with ABAC model. GnuPG subkey enables to restrict the role hierarchy, user privileges and business rules that are defined by CSP. In modified CTES model, the Data Owner and Data Consumer in the Public Cloud are considered as the user and authorized to upload or download the shared data in the cloud storage. The CSP Public Subkey is utilized for uploading/downloading the encrypted data from Data Owner. The Data Consumer can compute the data and upload the encrypted data with the CSP Public subkey. Here the Data Owner does not want to be always online when Data Consumer wants to access data from cloud server. The available encrypted data in the CSP shared storage is validated against the resources and attributes associated with a user certificate. Thus, the privileges of each entities are reviewed automatically with the Kerberos SSO and not by any human intervention.

The interacting messages (Fig 3) used among the different servers are:1. The messages A10, A11, A12 and A13 (from Fig 2) validates the role attributes in the super host and update the Kerberos SSO message A6/A7 (from Fig 2) for user authorization in KDC. This new access policy gets defined in the super host (Fig 3) and it allows to access the specific resources like App2R2, App2R1 based on the GnuPG subkey validation and along with Kerberos SSO. These two kinds of validation ensure that the shared data in the Public cloud can be accessed to the user or not.

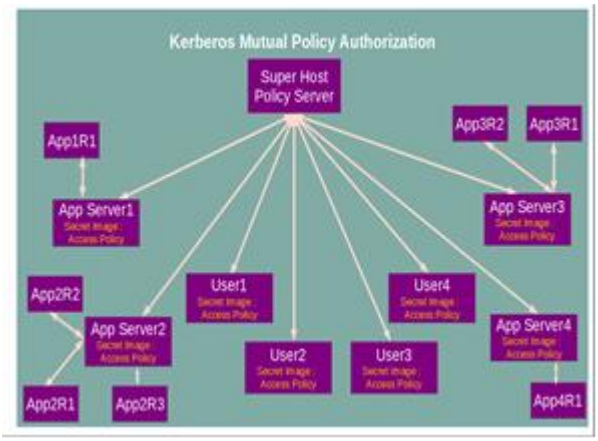


Fig 3: Kerberos Mutual Policy Authorization with GnuPG subkey

2. ABAC Policy in MULTI-DOMAIN AUTHENTICATION

An effective access control is necessary for the cloud services in different security domains. GnuPG Certification is the process of verifying the links between users, roles, groups, attributes and resources to ensure that they are true and correct (Fig 4). A GnuPG subkey can be created separately in each domain based on their attribute name for encrypting the data. The CSP can validate the other domain subkey's fingerprint and signing his public key with user's private key. This subkeys are like a separate key pair and associated with the main key pair. Then the encrypted data can be shared with the multiple domain and GnuPG resolves to identify the user data by using ABAC policy in the storage server. GnuPG subkey enables to review the role hierarchy, user privileges and business rules that are defined by CSP.

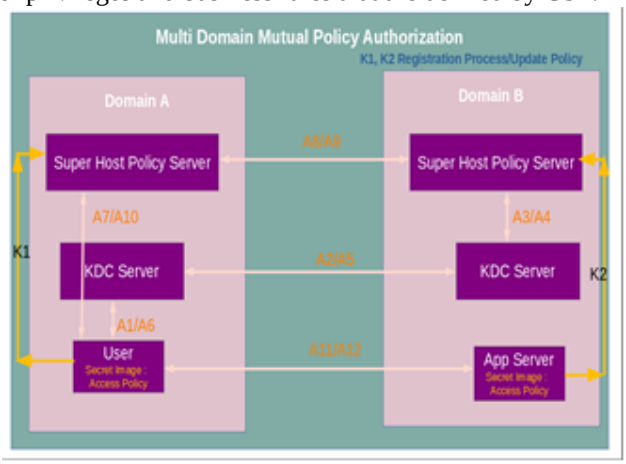


Fig 4: Multi Domain Mutual Policy Authorization

XI ANALYSIS OF THE PROPOSED KERBEROS AUTHORIZATION WITH HYBRID ACCESS CONTROL MODEL (KAHAC) & RESULTS

1. Use of Kerberos single sign-on technique for user authorization helps to minimize the multiple login requirements and multiple authorization policy.

2. ABAC model helps the user to access the single domain and multiple domain for different service providers with different security levels.

3. Authorization privileges from third-party vendors are restricted with DAC, MAC and RBAC rule in the system. The proposed KAHAC model is designed for RBAC and ABAC to accommodate additional constraints which are placed on a role attribute.

4. KAHAC model resolves the limitation of RBAC and ABAC model by validating the assigned roles and privileges of each user dynamically.

5. The integration of cross-grained (RBAC) and fine-grained (ABAC) policy helps to process the different level of security for the organization with the CTES model.

6. The proposed KAHAC model strengthens the security of the data by reducing permission in attributes for the user.

7. The main problem of re-encryption of shared data in the cloud storage is resolved with the use of Public Key signing of Data owner and Data Consumer in the CSP Public Key. The Data owner need not be online during the user accesses the data in the cloud server.

8. The Data Owner can outsource their data into the cloud without keeping the copy in local systems. The data owner can change the access policy and there is no need of data transfer back to the local site from the cloud. This avoids a computation of data and communication overhead in public cloud.

XII CONCLUSION

In this paper, KAHAC model is proposed with the Hybrid policy of RBAC and ABAC for single domain and multi domain access control based on attributes, access modes, roles and the type of resources. This has two concepts, role and attribute. This model also considers the DAC and MAC model for the access mode like read, write, etc, objects like private to particular user or sharing between the many users. The modified Collaborative Trust Enhanced Security (CTES) model integrates this new access control model with the inbuilt access control mechanism for Kerberos protocol itself to enforce the Cloud Service Provider access policy directly into the Client system node.

REFERENCES

1. Ashok Kumar J & Gopinath Ganapathy. (2017). An Enhanced CTES Design for Authentication and Authorization to Cloud Services and Resources. International Journal of Applied Engineering Research, 12(24), 15693-15698.
2. Ashok Kumar J & Gopinath Ganapathy. (2017). A Modified Approach for Kerberos Authentication Protocol with Secret Image by using Visual Cryptography. International Journal of Applied Engineering Research, 12(21), 11218-11223.
3. Abdul Raouf Khan. (2012). ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT. ARPN Journal of Engineering and Applied Sciences, 7(5), 613-615.
4. Natarajan Meghanathan. (2013). Review of Access Control Models for Cloud Computing. David C. Wyld (Eds): ICCSEA, SPPR, CSIA, WimoA, pp. 77-85.
5. J. H. Saltzer and M. D. Schroeder. (1975). The Protection of Information in Computer Systems. Proceedings of the IEEE, 63(9), 1278-1308.
6. Kamarudin shafinah & Mohammad mohd ikram (2011). File Security based on Pretty Good Privacy (PGP)Conce. Computer and Information Science, 4(4), 10-28.
7. Michael louie loria. (2014). Pretty Good Privacy. Retrieved 21 August, 2017, from http://slidedeck.io/michaellouieloria/pgp
8. DonArmstrong. (2018). https://wiki.debian.org/Subkeys
9. R. Sandhu, D. Ferraiolo, R. Kuhn, "The NIST Model for Role-Based Access Control: Towards A Unified Standard".
10. Ryan Ausanka-Crues. Methods for Access Control:Advances and Limitations. (2001). https://pdfs.semanticscholar.org/6192/f0308dc8d7782b55a0557dfb66f323638853.pdf
11. David F. Ferraiolo and D. Richard Kuhn. (2012). https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1992/10/13/role-based-access-controls/documents/ferraiolo-kuhn-92.pdf
12. Xin Jin1, Ravi Sandhu1and Ram Krishnan. (2012). RABAC: Role-CentricAttribute-Based Access Control. I. Kotenko and V. Skormin (Eds.): MMM-ACNS 2012, LNCS 7531, 84-96.
13. Rajpoot, Q. M., Jensen, C. D., and Krishnan, R. (2015). Attributes enhanced role-based access control model. In International Conference on Trust and Privacy in Digital Business, pages 3-17. Springer.
14. Xiaowei Gao, Zemin Jiang, Rui Jiang. (2012). A Novel Data Access Scheme in Cloud Computing. 2nd International Conference on Computer and Information Application (ICCIA 2012).pp 0124-0127.
15. Hua Wang, Lili Sun, Vijay Varadharajan. Purpose-based access control policies and conflicting anal-ysis. 25th IFIP TC 11 International Information Security Conference (SEC) / Held as Part of WorldComputer Congress (WCC), Sep 2010, Brisbane, Australia. pp.217-228.