Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Enhanced User Access Control Architecture for Cloud Storage

R. Kalaichelvi[*]
Research Scholar, Dept. of Computer Science
Karpagam University, Coimbatore, India

Dr. L. Arockiam
Associate Professor, Dept. of Computer Science
St. Joseph's College, Tiruchirappalli, India

Abstract*—Currently, Cloud Computing is ubiquitous as the IT deployment resource in networks. Conversely, there are some critical issues in cloud security. One of the significant concerns in cloud security is User Access Control. As user's data is processed somewhere at a remote place, the user has concerns about the confidentiality of their data. The research proposes a new model by federating authentication, authorization and auditing with cryptography. The owner of the data encrypts the data prior to uploading the data in cloud. When a user tries to access one or more services, if the user's strong authentication credentials match that of legal user, then he is allowed to access the encrypted data from the cloud with SSO service. With the authorization token, the user can access the resources that he is entitled to access. Effective auditing management monitors the authentication and authorization processes. The proposed scheme imposes a combination of strong authentication system, a novel role based authorized mechanism and an effective auditing management along with the cryptography technique for an efficient user access control in cloud.

Keywords*— Cloud security, User Access Control, Confidentiality, Authentication, Authorization, Auditing, Cryptography.

I. Introduction

According to Alvin Toffler, there are three waves evolved in the universe viz i) agricultural age ii) industrial age and iii) information age [15]. There are many sub waves in all these three waves. The cloud computing is a sub wave of "information age" wave. In this modern era, using cloud computing paradigm, any organization can just plug in to the cloud world, like people plug into the electrical grid. Cloud Computing [1] is a system where essential resources are accessed by the public as a service. It delivers services to public in the form of hardware, software and storage etc.

The services [1] offered by cloud computing are:

- Infrastructure as a Service (IaaS): This model supplies infrastructures such as storage, database to the users.
- Software as a Service (SaaS): Various applications are delivered to the users.
- Platform as a Service (PaaS): Developing and hosting applications to the clients.

There are lots of cloud service providers (CSP) available. Amazon, Google, Rackspace and Microsoft are the popular cloud service providers [13].

The cloud models can be implemented as:

- Public Cloud: The cloud models are offered to public.
- Private Cloud: This infrastructure is available only for specific organizations.
- Hybrid Cloud: It can be in the structure of private or public cloud.

Many enterprises such as government organizations, hospitals, business and banks store a massive amount of data in cloud. Data is asset for their business. However, there are some security concerns in the evolution of cloud paradigm. A significant barrier for growth of cloud is that the users fear possible privacy intrusion of their sensitive data. The threats to organizations are at network level, host level and application level. The security level requirements vary according to the delivery models (public, private and hybrid) and also vary according to the service models such as SaaS, PaaS and IaaS. Access control [2] is the most crucial mechanism to be considered in cloud security. Access control is referred to as controlling access to computer resources, applying procedures and supplying information for services in cloud computing via identification, authentication, authorization and accountability. An essential factor to be considered in having up-coming cloud computing environment is authentication [3] and authorization [3]. Permitting users in accessing the confidential information over cloud paradigm is done through a crucial User Authentication, Authorization and Auditing (UAAA) system [6].

A. Access Control Components

Authentication is the instrument that is used to identify the authorized users. Authentication mechanism may be a simple or a complicated system. In any system, shared secret information is known only by the user. The distinctive information such as a password, or a smartcard or fingerprint of the user provided by the user is to identify that the user is the authorized user by the authentication system. If the shared secret is correct then the user is the authenticated user.

Once the identity is found, the authenticated users' privileges should be defined. The rights of use would vary from user to user. This level of access to the system by an authenticated user is known as authorization. Authorized system is used to identify whether the user is permitted to access the resources, execute some operations or execute operation on a specific resources. Henceforth, authentication and authorization mechanisms are two different systems that work together in cloud computing to avert illegal users from accessing secured resources. After the establishment of authentication & authorization, auditing i.e. examining of authentication and authorization processes is imposed. This is mainly to establish security policies in cloud environment.

There are two essential categories of authorization and authentication in cloud Computing [4]. They are creating and managing virtual machines and logging into virtual machines once they are running. Identifying authorized users and preventing abuse are accomplished by authentication. Classifying users and permitting privileges to the users are achieved by authorization mechanism. User Access Control in Cloud Computing (UACCC) goal [5] is to prevent the access of private or network information from illegal users, sniffers, and masqueraders.

II. Related literature

Cloud computing is an emerging powerful technology of this decade. Various schemes of access control systems are available in cloud paradigm. However, cloud computing faces numerous security issues and challenges. Hence, a vigorous authentication and authorization system should be incorporated. A study [2] in cloud computing presented a various access control methods in cloud computing that help in accessing resources in elastic and scalable manner. Another study [8] explored on cloud security issues. Access control and cryptography mechanisms are integrated and proposed as a new model by the researchers to protect data in cloud environment. Almutairi, A. et al. [9] presented an architecture that covers the security management and software engineering techniques to offer a flexible access without having unnecessary procedure to access data which resides on cloud.

Role based access control is described in another study [10]. The researchers define user role, owner role and service provider role in access control mechanisms. With their proposed model the security problems are reduced in a drastic way. Another study in cloud access control [14] explored the role based policies in cloud computing environment. The projected system improves access control system in cloud paradigm by eliminating the unnecessary procedures of establishing connection. Several methods of attribute based access control are present in IT industry. Nevertheless, they are not elastic in their nature as well; they have weak and complex access control policies. To overcome these attributes, a study [11] proposed a hierarchical attribute based access control mechanism by enlarging cyber text based attribute mechanism in a novel system. The enhanced novel system offers flexible and scalable control system. Researchers Yanzhe che et al. [12] described a structured "*Behaviors and attributes based access control*". Behaviors and attributes are the factors considered for their new model. Also, two different steps: pre-access control and post-access control are taken into account for constructing a new model.

The cloud computing services are available to various types of users. Different users must have different roles or unique access profile. The policies and privileges management were addressed in this research. Also, the weaknesses and the complexities of existing mechanisms were explored. As a result, a holistic User Access Control in Cloud Computing model is proposed to identify genuine users, and verifies rights of every user who accesses the data in cloud.

III. Conceptual framework

Cloud computing is a means to store data for small or medium or big enterprises. As there is very small or no up-front money involved, many businesses are moving towards cloud to store their vast amounts of data. However, handling identity and access management weakens the adoption of cloud computing by many organizations [8]. One of the potential concerns in cloud storage is storing data at a greater risk. The research aims to find out the issues involved in cloud access control of stored data. In addition, the study aims to compare existing traditional architectures and proposes a new architecture that overcomes flaws in existing architectures. The Fig. 1 shows the conceptual framework of User Access Control in Cloud Computing. It illustrates an outline of access control elements via authentication and authorization.

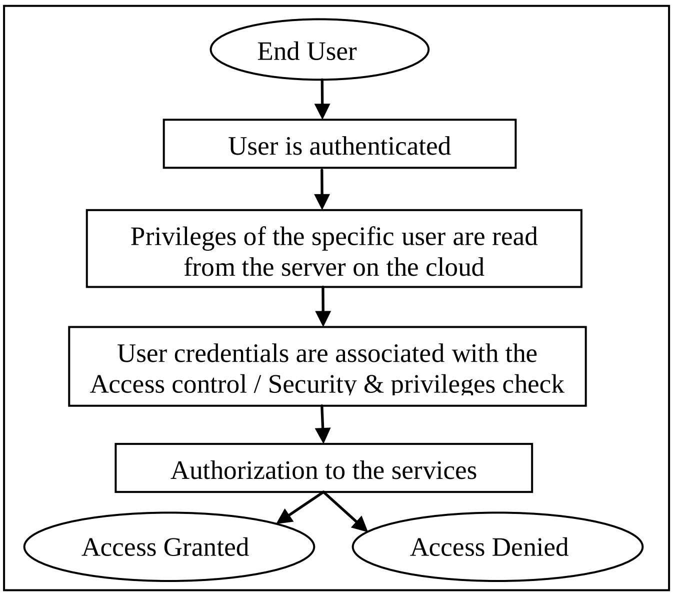
End User
User is authenticated
Privileges of the specific user are read from the server on the cloud
User credentials are associated with the Access control / Security & privileges check
Authorization to the services
Access Granted
Access Denied

Fig. 1. Coceptual framework of UACCC

IV. Identity and Access Management (IAM)

The adoption of cloud computing relies on Identity and Access Management. The main aspects of IAM are Authentication, Authorization and Auditing (AAA). There are six processes [15] of IAM involved in improving efficiency and having effective compliance management. The Fig. 2 inspired from Cloud Security and Privacy [15] shows the important processes in IAM architecture.

Features that supports Identity and Access Management:

a. Authentication
b. Authorization
c. Access Control
d. Accountability
e. Cryptography
f. Key Management

IAM Processes:

a. User management
b. Authentication management
c. Authorization management
d. Access management
e. Data management
f. Auditing management

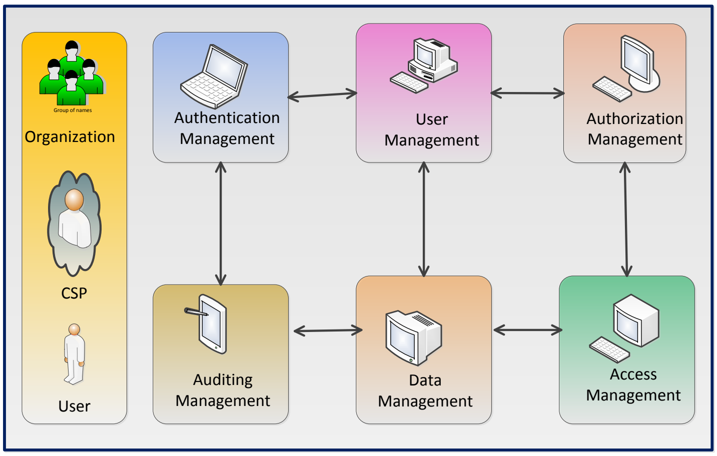

Fig. 2. Processes of IAM architecture

V. Data Security

The adoption of cloud services involves moving data among customers, cloud service provider and users. Hence, data security becomes a vital part of cloud at network, host and application levels. The data in cloud can be in any of the following forms [15]:

- in transit,
- at rest
- processing
- lineage,
- retention
- destruction.

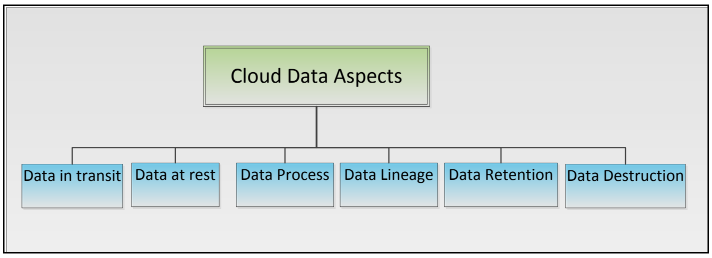

Fig. 3. Cloud data forms

The data security of the customer and the cloud service providers is of utmost importance. The main concerns on data security are CIA - Confidentiality, Integrity and Availability of stored data in cloud. The two potential concerns of CIA are:

- Access control in protecting data in cloud.
- The mechanism that protects the data in cloud.

When an organization stores its data in public cloud, it is vulnerable to attacks by unauthorized users. There are mainly four parties involved in processing of data on cloud, namely, the organization which owns the data, the user who uses the cloud data, the cloud service provider and the third party vendor who does the intermediate job. Hence, protecting data from the unauthorized user is a very significant factor to be considered.

A. Data Protection

The major concern in data security is the mechanism used in protecting the data stored on cloud. The technique used in data protection is encryption. Since, most of the CSPs do not encrypt organizations' data; organizations should encrypt their data before it is stored on the cloud. Encryption involves algorithm, key length and key management.

B. Data Storage Encryption

There are two types of encryption algorithm available namely symmetric encryption and asymmetric encryption algorithms. Symmetric algorithm has only a single key for both the encryption and decryption of data. When a customer sends the plain text, the shared secret key is used to encrypt the plain text to cipher text at the customer end. Then the encrypted data is uploaded on to the cloud. When a user attempts to access data, the same key is used to decrypt the data to convert the cipher text to plain text. But, asymmetric algorithm uses two keys. The public key is used for encryption where as the private key is used for decryption. The main cryptographic algorithms are Rivest-Shamir-Adleman (RSA) algorithm, Data Encryption Standard (DES) algorithm, Advanced Encryption Standard (AES) and so on.

Generally, organizations store a huge volume of data on cloud. The computational efficiency and speed of symmetric algorithm is comparatively higher than the asymmetric algorithm. Hence, it is highly suitable to use a symmetric algorithm, whilst using asymmetric algorithm is not appropriate in cloud environment.

C. Key Length & Key Management

The two important considerations in encryption are key length and key management. The deployed applications in organization level are within trust boundary as they implement highly effective secured mechanisms such as Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and many more security controls. But the CSP is not in the trust boundary, the complex task of key management could be given to third party vendors in cloud environment.

As a response to the related studies, it is understood that the enterprises' trust boundary in cloud environment may not be under control. Due to this loss of control, many enterprises may not adopt cloud services. To overcome this situation, more attention should be given to the access control aspect in cloud services. Mainly cryptographic technique should be combined with authentication and authorization mechanisms in this research. The architectural frame work of prototype to be proposed is shown in Fig. 4 [7].

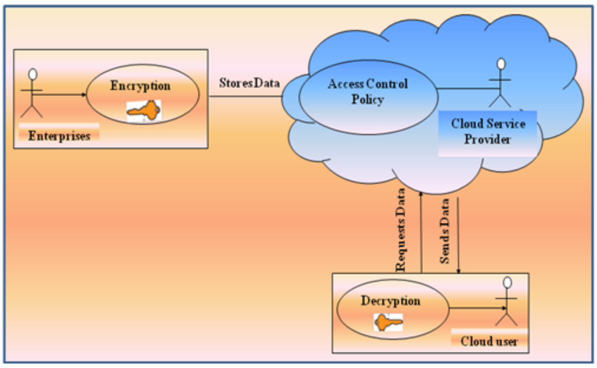

Fig. 4. Use case - Architecture of UACCC

VI. HOLISTIC APPROACH TO ACCESS CONTROL

There are three steps to be followed before accessing the data by any legal user viz. authentication, authorization and auditing in order to mitigate risks in data security.

A. Architecture of UACCC

The Fig. 5 describes the proposed model of user access control in cloud computing which incorporates features such as authentication, authorization and auditing.

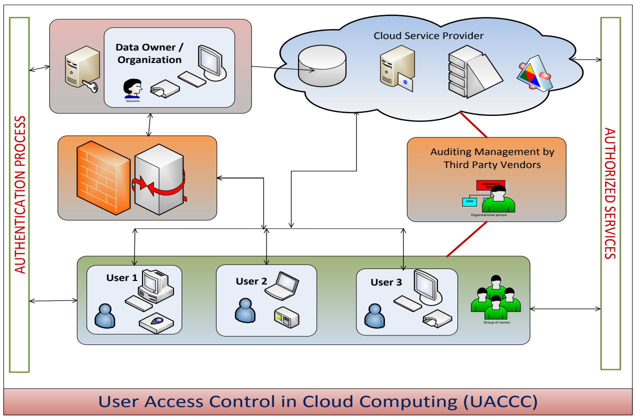

Fig. 5. Architecture of UACCC

B. Authentication Process in UACCC

Cloud service provider generally gives very weak authentication mechanism. The traditional username and password can be easily interpreted by any illegal users. In this proposed system, strong authentication mechanism is used to access the data. This includes 1) user name and password, 2) One Time Password (OTP), 3) biometric authentication. After the successful authentication by this type of strong authentication, Single Sign On & Single Sign Off (SSO) feature will be given by the CSP to the user to reduce the time required to integrate with service provider. With SSO service, user can access multiple, independent data or certain operations on cloud in a single authentication process.

The user, one who wants to access the data on cloud, sends an authentication request to the provider through any web browser. The user request is encoded prior to being sent for accessing SSO service. The encoded user request is sent to the organization to access the cloud data. The data owner authenticates the user after the identity of user's valid user name and password. After the verification of identity of the user, the data owner sends encoded authentication information as a response with keys to the browser. Now, the browser resends this response to the user with the keys. Using the keys provided by the organization, the user decodes the authentication information with SSO service. The user uses the strong authentication for accessing the data or the resources of organization stored on cloud.

C. Authorization Process in UACCC

Most of the CSP provides only two authorization levels viz. administrator level authorization and user level authorization level. As there are no intermediate levels of authorization, the data or resources can be accessed by any user or any organization, this coarse authorization has noteworthy amount of security risk in it. The UACCC provides a policy based access decisions. The privileges of accessing storage services would vary from user to user. Some user can only view data; some user can retrieve while some others can modify data. Access decisions and policies are managed by UACCC. It allows or denies certain operations or functions based on those allocated to the user. It provides a strong policy obligation across the cloud environment based on the access decisions. Additionally, it grants multiple services with SSO.

D. Auditing & Monitoring Management in UACCC

If the successful authentication and authorization take place, then the compliance of auditing and monitoring is necessary in order to access the resources based on the defined policies. Accountability should be accomplished by enforcing policies and standard procedures by the people who are connected with the cloud storage. The organization can provide auditing and monitoring mechanisms to third party vendors to avoid any security risks from CSP. Further implementation of Federal Information Security Management Act (FISMA), European Union Data Protection Directive (EU Directive), Organization for Economic Cooperation and Development (OECD), Gramma-Leach-Bliley Act (GLBA) and National Institute of Standards Technology (NIST) standards to the cloud storage and access of resources is critical to deliver a proper authentication and authorization services [15].

E. Pseudo Code of UACCC

1. The owner of the data i.e. organization encrypts the data prior to uploading the data in cloud.
2. User contacts the organization's service to access one or more services.
3. The cloud service provider responds the user with an unauthorized credential.
4. The application requests the user to give their authentication credentials as a token to access service.
5. As an authentication process the user is asked to log into the services with his credentials.
6. The owner of data grants or denies the access to the services based on the credentials which are provided by the user.
7. If the user's strong authentication credentials are from the legal user, he is allowed to access the encrypted data from the cloud with SSO service.
8. Additionally, the application checks his authorization that he is entitled to access the resources and other operation.
9. After the verification of his rights, the valid token is sent to the user.
10. With the authorization token, the user can access the resources that he is entitled to access.
11. Third party vendors monitor the implemented authentication and authorization process.

The Fig. 6 demonstrates the steps incorporated in the proposed model of UACCC. It encompasses the processes and the sequences of authentication, authorization and auditing. Additionally the establishment of data encryption by owner is depicted.

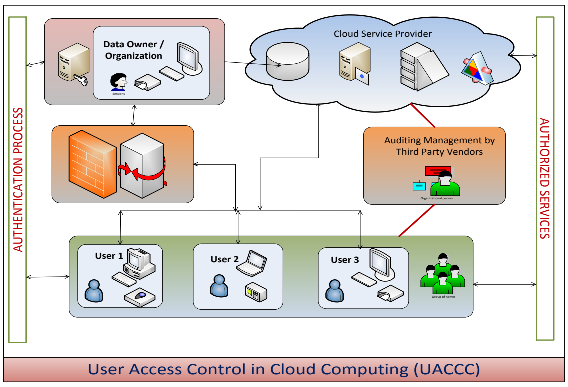

Fig. 6. The protocol for UACCC

VII. CONCLUSION

This research presents the access control model (UACCC) involving a set of data security protocols. In this study, a holistic approach to access control with encryption scheme is proposed. The proposed scheme imposes a combination of strong authentication system, a novel authorization mechanism and an effective auditing management along with shared key encryption techniques for an efficient user access control on cloud. Moreover, the complex aspects of encryption, namely, key length and key management are incorporated in this study. The future work encompasses converting the above proposed protocol into simulation. Additionally, a specific encryption algorithm which improves the speed and computational efficiency of accessing data on cloud will be pursued. Further extension will cover the policies and procedures for the inclusion of trusted third party vendors in dealing with the key management and monitoring and auditing management.

REFERENCES

[1] R. Kalaichelvi et al., "Research Challenges and Security Issues in Cloud Computing", *International Journal of Computational Intelligence and Information Security*, Vol. 3, No. 3 pp 42-48, March 2012.

[2] Abdul Raouf Khan, "Access control in cloud computing environment" *ARPN Journal of Engineering and Applied Sciences*, VOL. 7, NO. 5, MAY 2012, ISSN 1819-6608 pp 613- 615

[3] Authentication and authorization on the web at http://www.duke.edu/~rob/kerberos/authvauth.html

[4] Categories on the web at http://www -fermicloud.fnal.gov/CHEP_2010_FermiCloud_b.pdf

[5] Goals on the web at http://www.cloudera.com/blog/2012/09/understanding-user-authentication-and-authorization-in-apache-hbase/

[6] Hyokyung Chang and Euiin Choi, "User Authentication in Cloud Computing", *Ubiquitous Computing And Multimedia Applications Communications in Computer and Information Science*, 2011, Volume 151, 338-342.

[7] R. Kalaichelvi et al. "Secure and Robust Cloud Storage with Cryptography and Access Control", *Elixir Comp. Sci. & Engg*. 56 (2013) 13481-13484, March 2013, ISSN: 2229-712X

[8] Sonam Chugh et al. "Access Control Based Data Security in Cloud Computing", *International Journal of Engineering Research and Applications (IJERA*), vol 2, issue 3 Jun 2012, ISSN: 2248-9622 pp.2589-2593 2589

[9] Almutairi, A. et al., "A Distributed Access Control Architecture for Cloud Computing" *Software, IEEE*, vol 29, issue 2, March-April 2012, pp 36-44

[10] Zhuo Tang et al. "A new RBAC based access control model for cloud computing" *GPC'12 Proceedings of the 7th international conference on Advances in Grid and Pervasive Computing*, Springer-Verlag Berlin, Heidelberg ©2012 ISBN: 978-3-642-30766-9, pp 279-288

[11] Zhiguo Wan et al., "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", *Information Forensics and Security*, *IEEE Transactions*, Vol 7, Issue 2, Apr 2012, pp 743-754

[12] Yanzhe Che et. al, "BABAC: An Access Control Framework for Network Virtualization Using User Behaviors and Attributes", *Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on & Int'l Conference on Cyber*, Physical and Social Computing (CPSCom), dec 2012, pp 747-754

[13] Cloud Providers on the web at http://www.cloudreviews.com/top-ten/cloud-hosting-services.html

[14] Zhu Tianyi et al. "An Efficient Role Based Access Control System for Cloud Computing", *Computer and Information Technology (CIT),* 2011 *IEEE 11th International Conference,* sep 2011, pp 97-102

[15] Tim Mather, Subra Kumaraswamy, and Shahed Latif “Cloud Security and Privacy”, Published by O’Reilly Media, Inc., First Edition, 2009.

BIOGRAPHY

Engr. R. Kalaichelvi is working as an Asst. Professor in AMA International University, Kingdom of Bahrain. She is currently pursuing her research in Karpagam University, Coimbatore, India. She has published 7 research articles in the International / National Journals. Her areas of research interests are in Cloud Computing, Data Security, Cryptography and Data mining.

Dr. L. Arockiam is working as an Associate Professor in St.Joseph’s College, India. He has published more than 140 research articles in the International / National Conferences and Journals. He has also authored two books: "Success through Soft Skills" and "Research in a Nutshell". He has presented two research articles in the Software Measurement European Forum in Rome. He has chaired many technical sessions and delivered invited talks in National and International Conferences. His areas of research interests are: Software Measurement, Cloud Computing, Cognitive Aspects in Programming, Web Service, Mobile Networks and Data mining. He has been awarded “Best Research Publications in Science” for 2010, 2011, & 2012 and ASDF Global Awards for “Best Academic Researcher” from ASDF, Pondicherry for the academic year 2012.