IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 5, May 2018

# Cloud Data Security using Trust based Mutual Authentication: A Survey Paper

**Rina Patil[1], Mr. Pritesh Jain[2]**

Department of Computer Science & Engineering Patel College of Science and Technology, Indore, India[1,2]

**Abstract:** With the quick expansion of Cloud computing, more and more users place their data and application on the cloud. But the growth of Cloud computing is stuck by many Cloud security problem The development of the cloud system, large number of vendors can visit their users in the same platform directing their focus on the software rather than the underlying framework. This necessity requires the distribution, storage and analysis of the data on cloud for accessing virtualized and scalable web services. Access control policy can selectively restrict access to sensitive information stored by third-party sites on the Internet. Attribute-based encryption (ABE) schemes can strengthen the effective combination of flexibility and operability of access policy mechanism. Therefore, this survey paper is demonstrating secure mutual authentication for public cloud data and the need to prepare security solution using a strong cryptographic approach.

**Keyword:**Cloud Computing, Access Control, Mutual Trust, Attribute based Encryption, Cryptography Authentication

## I. INTRODUCTION

Cloud technology is an efficient storage and computational platform for providing high scalable solution. But now in these days that is also used for preserving the confidential and sensitive data over cloud too. Therefore the security as well as strong authentication mechanism required for managing the data owner and their confidential data. The main aim of designing the cloud computing system is to provide a scalable, on-demand services to the end users in a cost effective manner. Users do not need to be worry about the installation of high cost application on their system. In addition to this, the users do not need to maintain their own physical infrastructure and obtain their services on demand. The services provided by the cloud service provider (CSP) is called cloud services and these services are infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) [1].

Since, users outsource their data and computation to the cloud server, they may lose the physical control over their data and computation. Loss of physical control means the users are unable to resist the certain type of threats and attacks.

Access control mechanism has become important issue in cloud computing to ensure the security of resources and users updates on the cloud [2]. The user can make use of various cloud resources with the acceptance of the certificate from the authorization center for accessing the cloud [3].

This survey paper focused on exploring the domain of cloud data storage techniques and their authentication techniques. During the investigation there a number of secure techniques for cloud data storage is observed but there are very fewer work are noticed that providing the solution for authentication.

*Rest of the paper is organized as follow: Section II describe relative background details of the work. Section III introduces some prior work in this domain. Finally, the paper is concluded in section IV.*

## II. BACKGROUND

The background of a study is an important part of our research paper. It provides the context and purpose of the study. Hence there is need for background study that contribute to prepare proposed system.

### *A. Cloud Data Storage Security*

Moving data into the cloud offers great convenience to users since they don’t have to care about the complexities of direct hardware management. The pioneer of Cloud Computing vendors, Amazon Simple Storage Service (S3) and Amazon Elastic Compute Cloud (EC2) [4] are both well-known examples. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. As a result, users are at the mercy of their cloud service providers for the availability and integrity of their data. Recent downtime of Amazon’s S3 is such an example [5]. The data stored in the cloud may be frequently updated by the users, including insertion, deletion, modification, appending, reordering, etc.

DOI 10.17148/IJARCCE.2018.758

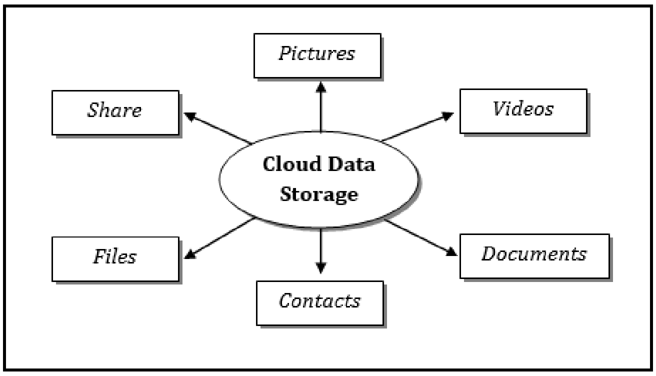

Figure 1: Cloud Data Storage

*B. Client Server Mutual Authentication*

Most web services presently use passwords to authenticate the user. However, regardless of the strength of the passwords, this type of authentication is proving to be no longer sufficient, mainly because it can be easily exposed to attacks such as key logging and phishing. Strong electronic authentication is the identification of users based on two or more factors: something the user knows, such as a password; something the user possesses, such as a chip card, device (mobile); or something that characterizes the user, such as a fingerprint. Such strong authentication mechanisms already exist but, unfortunately, most of them have the drawback of being costly. They often use security tokens that are expensive to deploy and quite impractical for users. Hence, there is a need to create stronger authentication mechanisms while still maintaining a good level of usability [6].

"Mutual Authentication is a security feature in which a client process must prove its identity to a server, and the server must prove its identity to the client, before any application traffic is sent over the client-to-server connection". Mutual authentication is that security feature in which both the entities of communication link authenticate each other by providing or proving his/her own identity to one another.

*C. Trust Based Access Control Model*

Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system.

Access control is a set of procedure which can be used to restrict the user's access to a particular system. Access control system monitors and record all the attempts made to access a system. Access Control also identifies the unauthorized access attempt by the user. The access control system can be designed using the models, algorithms and different administrative capabilities. So each access control systems have their own attributes, methods and capabilities in order to restrict the user [7].

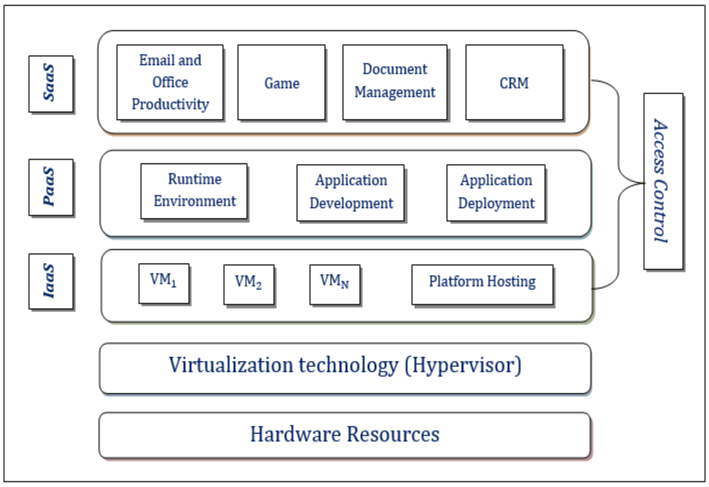

Figure 2: Positioning of Access Control in Cloud Architecture

Since cloud computing is very popular form of Internet application, the number of users is very large and the user behaviour is always uncertain and dynamic. So, there is more risk of affecting cloud resources. Some researcher introduces the concept of trust mechanism [8] and applied this trust mechanism into cloud environment. The trust based access control model takes the user behaviour parameter for access control decision. There are several parameters is to be defined in order to evaluate the trust value. The trust value is evaluated for both users and cloud resources before they interact with each other.

DOI 10.17148/IJARCCE.2018.758

### *D. Attribute based Encryption*

Attribute based encryption (ABE) is a relatively new perception of public key encryption for data-centric security solutions. Traditionally, view encryption as a way for a user to cipher data to a specific target recipient. The user encrypts the data under the recipient's public key such that only the exact recipient holding the matching private key can decrypt it. However, in various real-world applications, it is essentially provide access and share data confidentially and in a trusted manner according to a given policy without prior knowledge of who the recipient is. This is where ABE comes into place and offers a more scalable approach than existing public key cryptosystems. ABE can advance trusted sharing and access of data by basing access and decryption on a person's role / privileges within an organization or in other contexts, rather than by a person's specific identity [9].

### *E. Cryptographic Cloud*

Advances in networking technology and an increase in the need for computing resources have prompted many organizations to outsource their storage and computing needs. This new economic and computing model is commonly referred to as cloud computing and includes various types of services such as: infrastructure as a service (IaaS), where a customer makes use of a service provider's computing, storage or networking infrastructure; platform as a service (PaaS), where a customer leverages the provider's resources to run custom applications; and finally software as a service (SaaS), where customers use software that is run on the provider's infrastructure. Cryptography in the cloud employs encryption techniques to secure data that will be used or stored in the cloud. It allows users too conveniently and securely access shared cloud services, as any data that is hosted by cloud providers is protected with encryption. Cryptography in the cloud protects sensitive data without delaying information exchange [10].

Cryptography in the cloud allows for securing critical data beyond your corporate IT environment, where that data is no longer under your control. In other terms, "information in motion and information at rest are best protected by cryptographic security measures. In the cloud, we don't have the luxury of having actual, physical control over the storage of information, so the only way we can ensure that the information is protected is for it to be stored cryptographically, with us maintaining control of the cryptographic key." [11].

## III. LITERATURE SURVEY

The given section provides the understanding about the cloud data storage security of mutual authentication of user access control algorithm that are recently contributing in cloud environment therefore a number of research articles and research papers are included in this section.

**SushmitaRuj et al. [12]** propose a new privacy preserving authenticated access control scheme for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing information. This scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

**SushmitaRuj et al. [13]** propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the ser without knowing the user's identity before storing data. This scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Authors also address user revocation. Moreover, this authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

Cloud computing has become a part of the competitive market today. Various cloud computing service providers are available with their services in the cloud environment. Techniques adopted by various providers to achieve security are of varying nature. To analyze and measure a particular service based on its security properties is a challenge**.**

**RizwanaShaikha et al. [14]** presents such a measurement by using a trust model. A trust model measures the security strength and computes a trust value. A trust value comprises of various parameters that are necessary dimensions along which security of cloud services can be measured. CSA (Cloud Service Alliance) service challenges are used to assess security of a service and validity of the model. Adequacy of the model is also verified by evaluating trust value for existing cloud services. Trust model acts as a benchmark and ranking service to measure security in a cloud computing environment.

DOI 10.17148/IJARCCE.2018.758

**Ayad F. Barsoum et al. [15]** propose a cloud-based storage scheme that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual trust between them. The proposed scheme has four important features: (i) it allows the owner to outsource sensitive data to a CSP, and perform full block-level dynamic operations on the outsourced data, i.e., block modification, insertion, deletion, and append, (ii) it ensures that authorized users (i.e., those who have the right to access the owner's file) receive the latest version of the outsourced data, (iii) it enables indirect mutual trust between the owner and the CSP, and (iv) it allows the owner to grant or revoke access to the outsourced data. Authors discuss the security issues of the proposed scheme. Besides, authors justify its performance through theoretical analysis and experimental evaluation of storage, communication, and computation overheads.

The countless advantages of cloud computing has brought a massive change to the lifestyle and the way to cope with the world today, yet the cloud has to reach maturity. However, the main barrier to its widespread adoption is the security and privacy issues. In order to create and maintain mutual trust among the customers and the cloud service providers, a well – defined trust foundation should be implemented. The data stored in the cloud remotely by individual customer or an organization, so they lost control over the data, thus creating a security dilemma. The most challenging and hot research area in cloud computing now a day is the data security and access control. An effective measure to protect cloud computing resources and services in the start is to implement an access control mechanism.

**Sultan Ullah et al. [16]** discussed the features of various access control mechanisms and a novel framework of access control is proposed for cloud computing, which provides a multi - step and multifactor authentication of a user. The model proposed is well-organized and provably secure solution of access control for externally hosted applications.

## IV. PROBLEM FORMULATION

A problem domain is the area of expertise or application that needs to be examined to solve a problem. A problem domain is simply looking at only the topics of an individual's interest, and excluding everything else. In this paper, we focus on the problem of user authorization, security, and privacy for end user applications. Cloud computing is an advance form of the computational domain, which includes the high performance computational engines, sharable resources, scalable with problems and solutions. The cloud server storage security problem is foremost and fundamental requirement and it is sensitive area, many of cloud storage are using direct storing techniques to store data on server which is very insecure, some of cloud storage techniques are implemented in manner to resolve this problem but they also using it on server side but still it is very poor and insecure idea, well also the time consumption is fairly high when faced with larger-scale data. In this series of security, the security requirement of public cloud data is essential requirement for protecting user sensitive information.

## V. CONCLUSION

Public clouds are popular nowadays, where they are generally used in the storage and retrieval of the user's information. With the advent of cloud computing, more and more sensitive data are outsourced to the cloud server to reduce the management cost and enjoy the ubiquitous access..Privacy and security in cloud can be said to be achieved when users have control over information they want to reveal to cloud and who can access their information. Without guarantee of security and privacy users can't make shift to cloud only on the basis of lower cost and faster computing. Trust based access control model is one of the efficient mechanism for the security in cloud computing.An access control mechanism is required to restrict unauthorized access to the data. In this paper, survey of various trust based model in cloud computing were studied and analyzed. Hence the security of cloud computing environment can be enhanced using trust models.

## REFERENCES

[1] Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J., & Fu, C. (2010). Cloud computing: a perspective study. New Generation Computing, 28(2), 137-146.

[2] Abdul Raouf Khan, "Access Control in Cloud Computing Environment", ARPN Journal of Engineering and Applied Science, Volume-7, No.-5, 2012

[3] Guoyuan Lin, YuyuBie and Min Lei, "Trust Based Access Control Policy in Multi domain of Cloud Computing" , Journal Computers, Vol.8, No.5,pp.1357 -1366, 2013

[4] Amazon.com, "Amazon Web Services (AWS)," Online at http://aws, amazon.com, 2008.

[5] N. Gohring, "Amazon's S3 down for several hours," available online at: http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html, 2008.

[6] Seema P. Nakhate and R. M. Goudar, "Secure Mutual Authentication Protocol", International Journal of Computer Networks and Communications Security, Volume 2, Number 4, April 2014, pp. 142–145

[7] GurmamatHelil, MucheolKimand and Sangyong Han "Trust and Risk based Access Control andAccess Control Constraints", KSII Transaction on Internet and Information Systems, Volume.5, Number 11, November 2011

DOI 10.17148/IJARCCE.2018.758

[8] Mustapha Ben Saidi, AbderrahimMarzouk, “Access Control Protocol for Cloud Systems Based on the Model TorBAC”, International Journal of soft Computing and Engineering (IJSCE)”, Volume-2, Issue-5, November-2012.

[9] Thomas Ristenpart, EranTromer, HovavShacham, and Stefan Savage, Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds, In Proceedings of the 16th ACM conference on Computer and communications security, pp. 199–212, ACM, 2009.

[10] Rajanikanthaluvalu, lakshmiMuddana “A Survey on Access Control Models in Cloud Computing” Springer International Publishing, Advances in Intelligent Systems and Computing.

[11] Nate Lord, “Cryptography in the Cloud: Securing Cloud Data with Encryption”, available online at: https://digitalguardian.com/blog/cryptography-cloud-securing-cloud-data-encryption

[12] Ruj, Sushmita, Milos Stojmenovic, and Amiya Nayak, "Privacy preserving access control with authentication for securing data in clouds", In Cluster, Cloud and Grid Computing (CCGrid), 2012 12th IEEE/ACM International Symposium on, pp. 556-563, IEEE, 2012.

[13] Ruj, Sushmita, Milos Stojmenovic, and Amiya Nayak, "Decentralized access control with anonymous authentication of data stored in clouds", IEEE transactions on parallel and distributed systems 25, no. 2 (2014): pp. 384-394.

[14] Shaikh, Rizwana, and M. Sasikumar. "Trust model for measuring security strength of cloud computing service." Procedia Computer Science 45 (2015): pp. 380-389.

[15] Barsoum, Ayad, and Anwar Hasan, "Enabling dynamic data and indirect mutual trust for cloud computing storage systems", IEEE transactions on parallel and distributed systems 24, no. 12 (2013): pp. 2375-2385.

[16] Sultan Ullah, Zheng Xuefeng and Zhou Feng, “TCLOUD: A Multi – Factor Access Control Framework for Cloud Computing”, International Journal of Security and Its Applications Vol. 7, No. 2, March, 2013, pp. 15-26.

[17] Guoyuan Lin, Danru Wang, YuyuBie, and Min Lei, "MTBAC: a mutual trust based access control model in cloud computing", China Communications 11, Number 4, (2014): pp. 154-162.