ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 3, pp: (15-19), Month: July - September 2017, Available at: www.researchpublish.com

Cloud Computing Security Guidance for Encrypted Data Transfer

S.Kalaivani[1], A. Senthil Kumar[2]

[1]Research Scholar, [2]Asst. Professor, Dept. of Computer Science, Tamil University, Thanjavur, Tamilnadu, India

Abstract: **Cloud computing is fast growing technology that enable the users to store and access their data remotely. Using cloud services user can enjoy the profit of on-demand cloud applications and data with limited local infrastructure accessible with them. While contact the data from cloud, changed users may have connection among them depending on some attributes, and thus sharing of data along with user privacy and data safety becomes important to get effective results. Most of the research has been done to secure the data authentication so that user's don't lose their private data stored on public cloud. But still data sharing is an important hurdle to overcome by researchers. Research is going on to provide secure data sharing with enhanced user privacy and data access security. In this Project various research and challenge in this area are discussed in detail. It will definitely help the cloud users to understand the topic and researchers to develop a method to overcome these challenges.**

Keywords: **Cloud Computing, Security, Privacy.**

1. INTRODUCTION

Cloud computing is a alternative to traditional IT services that provide ubiquitous, convenient, on demand remotely accessed shared pool of computing resources(e.g. Networks, storage, application and services) [1]. Cloud computing has become a successful and popular business model due to its charming features. The former features of cloud results in security challenges, due to which the users hesitate to transfer their data to cloud. So security challenges are the main obstacle of the advancement of cloud computing. The Cloud Security Alliance has summarized five essential characteristics [2] that spotlight the relation to, and differences from, traditional computing paradigm.

On-demand self-service's cloud user may unilaterally acquire computing resources, like the server access and cloud storage, as on demand, without collaborating with the cloud provider.

• **Broad Network Access:** Cloud services are conveyed to users through Internet using standard mechanism that allow users to access the services using heterogeneous thin or thick client tools (e.g., PCs, mobile phones, and PDAs).

• **Resource Pooling:** The cloud providers pool the computing resources to serve the multiple users through multitenant model, in which resources (physical or virtual) dynamically assigned or reassigned according to users demand. Some resources are storage, processing, memory, network bandwidth, and virtual machines.

• **Rapid Elasticity.** Users may increase the capabilities of services rapidly and elastically to quickly scale out or rapidly released the services capabilities to quickly scale in. Users have the ability to purchase unlimited capabilities of services in any quantity at any time.

• **Measured Service:** The cloud services purchased by users are quantified and measured. For both the provider and customers, resource usage will be monitored, controlled, metered, and reported.

The main challenges for building a secure and truthful cloud data storage system: (1) Outsourcing: Outsourcing reduces both capital investment and operational expenses for cloud users. However, in outsourcing the users don't have physical control on their data and tasks as the data is in other hands. The loss of control on own data is the main challenge in cloud security. To overcome the outsourcing security challenges, first, the cloud provider shall be truthful by providing privacy and secure services second; users can verify the outsourced data and computation in terms of confidentiality, integrity and other security measures. (2) Multi-Tenancy: Multi-tenancy means that the multiple users can share and utilize the cloud platform using virtualization. Moreover, in a virtualized environment, data of different users may be stored on the same physical machine by using some resource allocation strategies. Antagonist who may also be legitimate cloud users of same provider having data on same physical machine may exploit the coresidence issue. Some security issues such as data breach [3,4], computation breach [3], flooding attack [5], etc., are incurred. Due to economic efficiency multi-tenancy is preferable by cloud vendors. Without changing the multi-tenancy paradigm, it is imperative to develop new security mechanisms to deal with the security issues. (3) Massive data and intense computation: Cloud computing can easily handle mass data storage and intense computing tasks. Therefore, traditional security mechanisms are not acceptable due to intolerable computation or communication overhead. For example, to verify the integrity of data stored on cloud, it is impractical to hash the entire data set stored on cloud. To this end, new strategies and protocols should be design. (4) Sharing: Data sharing provide higher efficiency to users. But data are stored on multi-tenant environment, so sharing of data stored on cloud is become less secured. So it is imperative to design new mechanisms and strategies to deal with the security issues of data sharing on cloud. As the internet is expanding the size of data is also expanding. So users are shifting to cloud storage service for convenient and easily access of data anytime and anywhere. But still the privacy and security is the main challenges in cloud storage service. Traditional research mainly focused on secure data access by users to its own data. Users can gain the higher productivity by sharing their data stored on cloud and this will be a big benefit for organisations as well. Organisations can share their data with customers, suppliers or buyers directly from their cloud storage. As a group of students and a team working on project can share their data with a cloud based tool Google drive. It is a better way than sharing the newer version files by sending through mail attachment to other members.

2. LITERATURE REVIEW

Attribute Based Access Control (ABAC). In ABAC, users get the data access based on some attributes. Some combined attributes defines the access policies, and users get access to data only after proving that they have those attributes. The first attribute-based encryption (ABE) scheme was proposed in 2006 [6] based on the work in [7], and many other ABE schemes have been proposed afterwards. In these schemes, data is encrypted before uploading using combined attributes, and private keys associated with those combined attributes can decrypt the data. These proposed techniques provided a different approach to secure the data stored in a distributed environment. It is shown that RBAC policies can be enforce using ABE scheme. However, the size of user key in that approach is not constant, and the revocation of a user from a role will result in a key update of all the other users of the same role [8]. There are so many other techniques to secure the data and privacy of users using encryption and proxy re-encryption of data. In these encryption techniques, owner of the data encrypt the data directly to those with whom he wants to share the data [9], [10]. The permissions in these techniques are either in a flat out type or in a access matrix type, so these techniques can't be compare with RBAC as the access policies are different in RBAC model. In [11] the author proposed a technique to share the data through anonymous ID assignment algorithm (AIDA) for multi-tenant cloud and distributed computing architecture. In the AIDA, the author design an integer data sharing algorithm based on data mining operation, and the algorithm performs variable number of iterations to assign the anonymous id. The author use in the algorithm Newton's identities and Sturm's theorem to emphasize the scalability of algorithm and Markov chain representations helps in algorithm to know the number of iterations required. In [12] the author proposed a scheme for multi-owner architecture in cloud computing to share the data securely (Mona) for dynamic groups in the cloud model. The users can securely share their data and interact dynamically with other in un-trusted cloud environment using this scheme. In this scheme, a new user after getting the access can directly decrypt data without contacting the data owner, and the users access are revoked by updating a list of revoked users, secret keys of remaining users are not updated. User authentication to access resource is ensure by using access control policies and the identities are maintained using privacy policy in which only group manager can access the

real identities of the data owners in case of any dispute. In [13] the author proposed a broadcast group key management scheme (BGKM) which overcomes the vulnerabilities of symmetric key techniques in public clouds, and according to this technique the users can dynamically request to get the symmetric keys during decryption process. Attribute based access control (ABAC) technique is developed so that a user can get the access of data if and only if the attributes of user's identity fulfil the data owner access policies. In this technique an access control vector (ACV) assign secret keys to users according to their identity attributes, and the users can get the actual symmetric keys to access the data based on their secret keys provided by access control vector. The adding/revoking users and updating access control policies is more secure in this technique. In the above mentioned works, various security challenges are achieved. However, while accessing the data related to user's privacy problem and data sharing problem has not been studied yet in the literature. Here, we analyze a new privacy challenge, and propose a protocol which focus on authentication of users to realize the secure data accessing and also considering authorization to provide the privacy- preserving access authority sharing of data between other users and outsiders.

3. PROBLEM FORMULATION

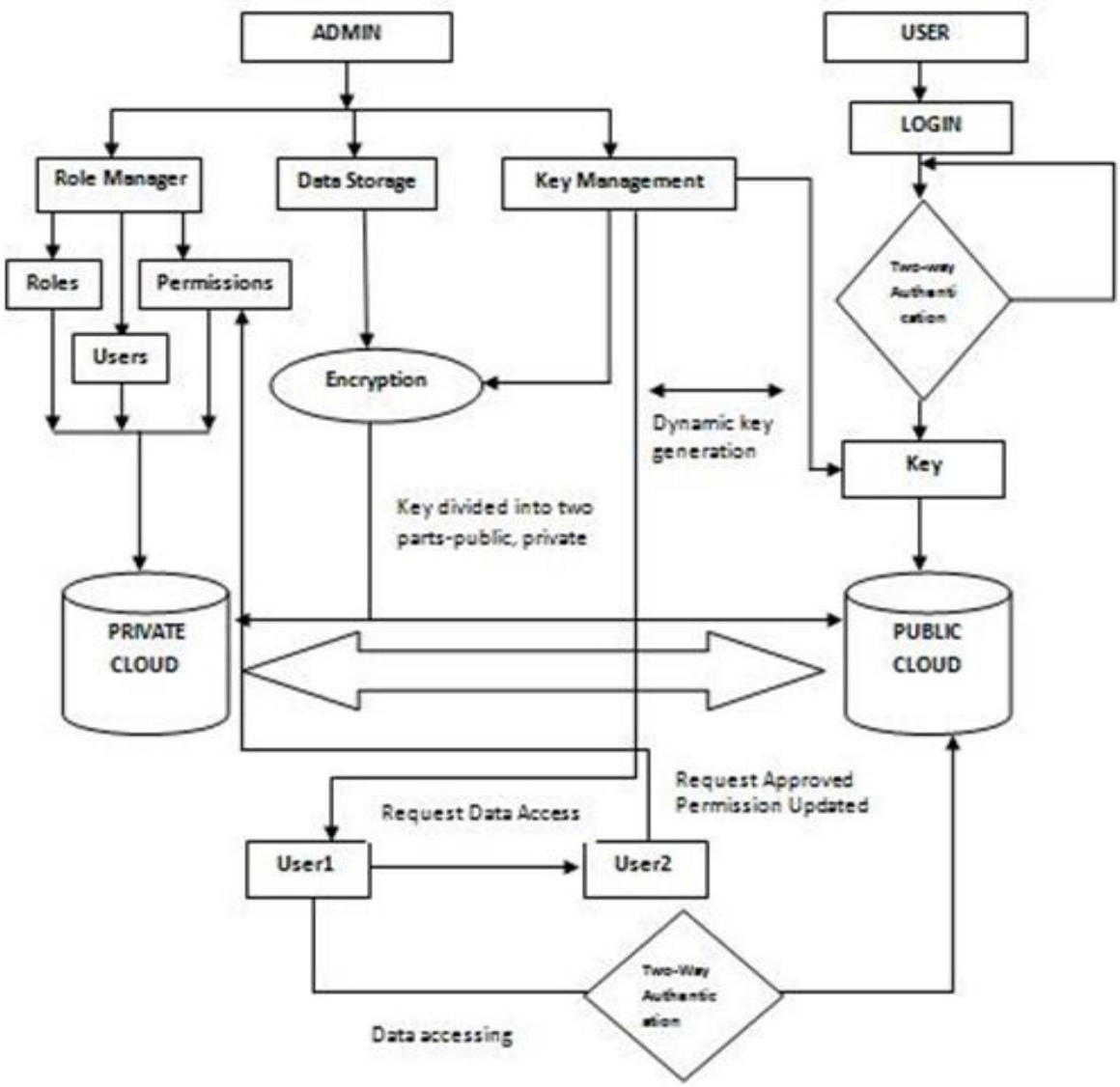
In public cloud, the user's data is stored in distributed data centres; so the control of data centres is not with single authority. Moreover the cloud providers are also able to access the data themselves if users stored the data in unencrypted format. Hence there is a need to design a mechanism to intensify the data security by using some cryptographic techniques to encrypt user's data before uploading to public cloud to prevent the misuse together by implementing hybrid cloud architecture by virtue of which the on one end the privacy and security can be achieved from private cloud and on the other end mass data storage feature of public clouds can be achieved. The hybrid cloud architecture should develop from private cloud and public cloud, where the user's sensitive data such as roles structure, security related data will be stored on private cloud while the actual data will be stored on public cloud in encrypted form and later all extended ABAC policies are to be apply on it to make more secure. In this hypothetical architecture, the authenticated users who have the access to particular data can interact with the public cloud only for that data with dynamically key provisioning only for limited time; there is no access for public users to access the private cloud where the sensitive data is stored, which greatly weaken the attack surface for the private cloud. Using the data sharing from public cloud also enhance the productivity of organisation, But security and user privacy is the main concern while sharing the user's data. This architecture not only will eliminate the organization's concerns about risks of leaking sensitive information, but will also takes full advantage of public cloud's power to securely store large volume of data with secure sharing of that data with enhanced privacy.

4. PROPOSED MODEL

To maintain the privacy of data and user while accessing data from cloud or sharing it to other users, some techniques should be designed so that data can be encrypted through some cryptographic techniques in such a way that only authentic users can access the data. The authentic users who want to access data from cloud can access the data using their authorizing key and no one can use that key, the key will be particular for particular file and user only which access policies can be enforced to implement the above. The design should be efficient for revocation of users from access list and this can be done only using dynamic key management. In this ABAC model only the data encrypted by owner of the data should be decrypted by only the authentic users who have the access policies and appropriate keys. The data is stored on cloud in encrypted format so the cloud provider will not be able to access the data until appropriate attributes are granted to him. The role hierarchy will also help in this model so that the access can be inherited from the other roles. If a level 2 role getting the access the level 1 users will.

Automatically get the access to that data. As dynamic key management is useful so data owner need not to encrypt the data again and also not need to change access keys after revoking some users. In the proposed model hybrid cloud can be used in a manner that power of the public cloud can be used to store the bulky data in encrypted form and security of private cloud can be used to store sensitive data regarding keys and other information to access that data. In this model the users can enhance the efficiency by means of sharing the data among internal or external users in a secure manner. Using sharing technique the replication of data can be prevented. Suppose the client of an organisation every time need the file whenever it is updated.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 5, Issue 3, pp: (15-19), Month: July - September 2017, Available at: www.researchpublish.com



As it is better to share that file which is stored in cloud that sends the file again and again by other means (email, ftp). The users need to request for access from the owner of the data, after the owner grant the access to that file only then the other users can access that data. In the proposed model, the administrator only can create users and manage their attributes to access the data. There are restrictions on user per role, data usage, changing roles all are managed by administrator. In this design the key management is introduced according to the bank key management system. The key will be divided into two parts and these will be placed on different places. The users want to access the data never get these keys, they only get the authorisation key which will be created dynamically for a particular time. The cloud provider or other user can never get the access to decryption keys. After the completion of design of this architecture this will be implemented on Microsoft Windows Azure, then only we can check the whole model against the access control based on attributes. The unauthorized users can't create new user id due to security measures.

5. CONCLUSION

The proposed model of ABAC addresses the security features for data access, privacy preserving and secure sharing of data in cloud environment and use the hybrid cloud storage architecture that allow the users to store their bulky data securely in a public cloud and store the sensitive information related to data access on private cloud. In this technique the privacy is managed by the owner of the data itself and the secure sharing of data is provided. It is believed that the proposed model has the potential to be helpful in commercial situations as it uses the practical access policies based on user's attributes in a flexible manner and provides secure data storage and sharing in the cloud environment.

REFERENCES

[1] P. Mell and T. Grance, The NIST Definition of Cloud Computing (2011).

[2] Cloud Security Alliance (CSA). Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 Released December 17 (2009).

[3] Google Docs experienced data breach during March (2009).

[4] N. Santos, K. P. Gummadi, and R. Rodrigues, Towards trusted cloud computing, Proc. 2009 Conference on Hot Topics in Cloud Computing (2009).

[5] C. Dovrolis, P. Ramanathan, and D. Moore, What do packet dispersion techniques measure? Proc. IEEE INFOCOM (2001), pp. 905–914.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Sec., Oct./Nov. 2006, pp. 89–98.

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc. EUROCRYPT, 2005, pp. 457–473.

[8] Y. Zhu, D. Ma, C. Hu, and D. Huang, "How to use attribute-based encryption to implement role-based access control in the cloud," in Proc. Int. Workshop Sec. Cloud Comput., 2013, pp. 33–40.

[9] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, "SiRiUS: Securing remote untrusted storage," in Proc. NDSS, 2003, pp. 1–15. 10. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. NDSS, Feb. 2005, pp. 29–43.