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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

Enhancing Security Of Data by Replacing Public Cloud with Hybrid Cloud

Harpreet Kaur [1], Er. Upinderpal Singh Bhathal [2], Er. Jagbir Singh Gill [3]

Research Student, Department Of Computer Science Eng., Chandigarh Group of Colleges, Landran., Mohali, India[1]

Assistant Professor, Department Of Computer Science Eng., Chandigarh Group of Colleges, Landran., Mohali, India[2,3]

Abstract: Recent advances have given rise to the popularity and success of cloud computing. However, outsourcing the data to a third party causes the security and privacy issues to become a critical concern. This has raised the important security issue of how to control and prevent unauthorized access to data stored in the cloud. In this paper the authors propose to develop hybrid cloud i.e. private cloud and public cloud, where the private cloud should store only the organization's sensitive structure information and the public cloud should store the actual data. This proposed architecture not only will dispel the organization's concerns about risks of leaking sensitive structure information, but will also takes full advantage of public cloud's power to securely store large volume of data. All data on public cloud is to be stored in encrypted form by employing cryptographic techniques which will save data from misuse and restrict data access to only those intended by the data owners.

Keywords: Outsourcing,Hybrid,Encryption, Cloud, Cryptography

I. INTRODUCTION

Cloud computing has begun to emerge as a hotspot in both industry and academia. It represents a new business model and computing paradigm, which enables on demand provisioning of computational and storage resources. The most cited definition of cloud computing is the one proposed by

The US National Institute of Standards and Technology (NIST). NIST provides the following definition [1]: "Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

Although cloud computing is a powerful means of achieving high storage and computing services at a low cost, it has not lived up to its reputation. Many potential users and companies yet lack interest in cloud based services [2]. One of the main reasons behind this lack of interest involves security issues. Cloud has several security issues involving assurance and confidentiality of data [3]. A user entrusting a cloud provider may lose access to his data temporarily or permanently due to an unlikely event such as a malware attack or network outage. On April 21, 2011, EC2's northern Virginia data center was affected by an outage and brought several websites down [4, 5]. Problems caused by this outage lasted till April 25, 2011 [4]. Such an unlikely event can do significant harm to the users. Confidentiality of user data in the cloud is another big concern. Cloud has been giving providers an opportunity to analyze user data for a long time. In addition, outside attackers who manage to get access to the cloud can also analyze data and violate

user privacy. Cloud is not only a source of massive static data, but also a provider of high processing capacity at low cost. This makes cloud more vulnerable as attackers can use the raw processing power of cloud to analyze data [6].Security issues have been the dominate barrier of the development and widespread use of cloud computing. There are three main challenges for building a secure and trustworthy cloud system:

- **Outsourcing** – Outsourcing brings down both capital expenditure and operational expenditure for cloud customers. However, outsourcing also means that customers physically lose control on their data and tasks. The loss of control problem has become one of the root causes of cloud insecurity. To address outsourcing security issues, first, the cloud provider shall be trustworthy by providing trust and secure computing and data storage; second, outsourced data and computation shall be verifiable to customers in terms of confidentiality, integrity, and other security services. In addition, outsourcing will potentially incur privacy violations, due to the fact that sensitive data is out of the owners' control.
- **Multi-tenancy** – Multi-tenancy means that the cloud platform is shared and utilized by multiple customers. Moreover, in a virtualized environment, data belonging to different customers may be placed on the same physical machine by certain resource allocation policy. Adversaries who may also be legitimate cloud customers may exploit the co-residence issue. A series of security issues such as data breach [7], [8], [9], computation breach [7], flooding attack [10], etc., are incurred. Although Multi-tenancy is a definite choice of cloud venders due to its economic efficiency, it provides new vulnerabilities to the cloud platform. Without changing the multi-tenancy paradigm, it is imperative to design new security mechanisms to deal with the potential risks.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

- **Massive data and intense computation** – cloud computing is capable of handling mass data storage and intense computing tasks. Therefore, traditional security mechanisms may not suffice due to unbearable computation or communication overhead. For example, to verify the integrity of data that is remotely stored, it is impractical to hash the entire data set. To this end, new strategies and protocols are expected.

II. LITERATURE REVIEW

Several recent surveys [11], [12] show that 88% potential cloud consumers are worried about the privacy of their data, and security is often cited as the top obstacle for cloud adoption. Authorization and access control has always been a fundamental security technique in systems like cloud computing in which multiple users share access to common resources. Several access control models have been proposed, such as, discretionary and mandatory access control models (DAC and MAC), Clark-Wilson model, Lipner's Integrity model, Chinese wall model, Task based models, and Role Based Access Control models and RBAC has further been extended up to some level. Among these models Role-based access control (RBAC) models have been receiving attention as they provide systematic access control security through a proven and increasingly predominant technology for commercial organizations. One of the main advantages of the RBAC over other access control models is the ease of its security administrations. RBAC models are policy neutral [13]; they can support different authorization policies including mandatory and discretionary through the appropriate role configuration. In spite of the success of the RBAC, researchers have determined that there are still many application security requirements that are not addressed by the existing RBAC models [14]. Sandhu et al [15] proposed RBAC 96 which is a family of four constitutes models. In RBAC permissions are associated with roles (the intermediate concept of roles can be seen as collections of permissions), and users are made members of appropriate roles. The notion of role is an enterprise or organizational concept. The definition of role is quoted from Sandhu et al. [15]: A role is a job function or job title within the organization with some associated semantics regarding the authority and responsibility conferred on a member of the role. Permissions are not directly assigned to users; instead they are assigned to roles. RBAC comprise a family of four references models: RBAC0, RBAC1, RBAC2 and RBAC3. RBAC0 contains the core concepts of the Model. It is the minimum requirement for any system that exploits features of RBAC. Users (U), roles (R), and permissions (P) are three sets of entities and the relations between these entities are defined by User-Role Assignment and Permission-Role Assignment [15]. These sets and relations are the main concepts of the RBAC. A user can be member of many roles and each role can have many users. A user can invoke multiple sessions within a session a user can invoke set of roles but each session belongs to only one user. Permission can be assigned to many roles and a role can have many permissions. RBAC1 adds to RBAC0 a role hierarchy (RH). Role hierarchies are an important concept for structuring roles to represent organization users responsibly and degree of authority. RBAC2 introduces the concept of constraints. RBAC adds static (not related to sessions) and dynamic (related to sessions) constraints between core concepts [15]. These constraints are considered to be the principle motivation for RBAC because constraints are powerful mechanism to lay out higher-level organizational mechanism [15].Constraints can be applied to User-Role Assignment, Permission-Role Assignment and session. RBAC3 includes all aspects of RBAC0, RBAC1 and RBAC2 and it is called a unified model of RBAC. RBAC3 combine RBAC1 and RBAC2 to combine both role hierarchy and constraints. In this model constraints can be applied to the role hierarchy in addition to the constraints in RBAC2.

In the literature, there exist many hierarchy access control schemes [16, 17, 18] which have been constructed based on hierarchical key management (HKM) schemes, and approaches using HKM schemes to enforce RBAC policies for data storage are discussed in [19, 20, 21]. However, these solutions have several limitations. For instance, if there is a large number of data owners and users involved, the overhead involved in setting up the key infrastructure can be very high indeed. Furthermore, when a user's access permission is revoked, all the keys known to this user as well as all the public values related to these keys need to changed, which makes these schemes impractical. An alternative approach for the management of keys is Hierarchical ID-based Encryption (HIBE), such as [22], [23]. However, in a HIBE scheme, the length of the identity becomes longer with the growth in the depth of hierarchy. In addition, the identity of a node must be a subset of its ancestor node so that its ancestor node can derive this node's private key for decryption. Therefore, this node cannot be assigned as a descendant node of another node in the hierarchy tree unless the identity of the other role is also the super set of this node's identity. Recently we have seen the development of schemes built directly on RBAC policies.

III. PROBLEM FORMULATION

In a public cloud, as data can be stored in distributed data centers; there may not be a single central authority which controls all the data centers. Furthermore the administrators of the cloud provider themselves would be able to access the data if it is stored in plain format. Hence there is a need of enhancing data security by employing cryptographic techniques to encrypt data from misuse together with some hybrid cloud architecture by which virtue of which the privacy and security of private cloud can be achieved on one end and mass data storage feature of public clouds on other end.

This hybrid cloud architecture should turn to be a composite of private cloud and public cloud, where the private cloud should store only the organization's sensitive structure information such as the role hierarchy and user membership information, and the public cloud should store the actual data that is in the encrypted form and later all extended RBAC policies are to be employed on it to

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 5, May 2014

make more robust. In this hypothetical architecture, the users who will access the data only- interact with the public cloud; there is no access for public users to access the private cloud, which greatly reduces the attack surface for the private cloud. This architecture not only will dispel the organization's concerns about risks of leaking sensitive structure information, but will also takes full advantage of public cloud's power to securely store large volume of data.

V. PROPOSED HYBRID CLOUD MODEL

To protect the privacy of the data, some measure needs to be designed by virtue of which data owners can employ cryptographic techniques to encrypt the data in such a way that only users who are allowed to access the data as specified by the access policies will be able to do so**.** The authorized users who satisfy the access policies will be able to decrypt the data using their private key, and no one else will be able to reveal the data content. For this to happen, the design of a secure RBAC based cloud storage system needs to be designed where the access control policies are enforced by a new role-based encryption that was mentioned earlier. This design should enforce RBAC policies on encrypted data stored in the cloud with an efficient user revocation using some broadcast encryption mechanism. In this proposed scheme, the owner of the data should encrypt the data in such a way that only the users with appropriate roles as specified by a RBAC policy can decrypt and view the data. The role should grant permissions to users who qualify the role and can also revoke the permissions from existing users of the role. The cloud provider (who stores the data) will not be able to see the content of the data if the provider is not given the appropriate role. This scheme should deal with role hierarchies also, whereby roles inherit permissions from other roles. A user should be able to join a role after the owner has encrypted the data for that role. The user will be able to access that data from then on, and the owner does not need to re-encrypt the data. Also user should be revoked at any time in which case, the revoked user should not have access to any future encrypted data for this role. Based on the proposed scheme, the authors need to develop a secure cloud data storage architecture using a hybrid cloud infrastructure. This hybrid cloud architecture should be composed of private cloud and public cloud, where the private cloud is used to store only the organization's sensitive structure information such as the role hierarchy and user membership information, and the public cloud is used to store the actual data that is in the encrypted form. In this architecture, the users who wish to share or access the data only interact with the public cloud; there is no access for public users to access the private cloud, which greatly reduces the attack surface for the private cloud. This architecture should not only dispel the organization's concerns about risks of leaking sensitive structure information, but also should take full advantage of public cloud's power to securely store large volume of data.

In this proposed model, the architecture is to be designed where administrator of the system can generate consoles for role manager and general clients. The role manager has to manage all the architectural aspects of the RBAC. All kinds of required roles and users creation for the system will be the main aspect to be covered by the role manager. Here all restrictions on users per role, add transaction limits for data usage, changing of permissions for roles are all covered by the role manager. In this architecture, the key management is added which will help the administrator to convert the data to be stored on the public cloud into the cipher text. This will result into privacy of this proposed hybrid architecture for which even Cloud Service Provider has to take membership from the administrator to access the data stored on the public cloud. Then users are to be generated per role and also access is provided to roles. Here restrictions are added for the generation of users per role. This is supported by adding restrictions on number of accesses per day over such roles. Once this designed architecture is developed and then used on windows Azure, after then the authors can make the authorization of any user in terms of login over such architecture. This will act as an access control for granting services for desired users. Next the challenge of unauthorized users is addressed in which a fake user will try to create a new id which is to be checked and denied as per our security policies. All these features are summed up in the following flow based figure 1.

VI. CONCLUSION

This proposed model has outlined a sketch for new RBAC which addresses the security features for any multi-centric application. Then the authors proposed a RBAC based hybrid cloud storage architecture which will allow an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud. Then authors have proposed secure cloud storage system architecture and have shown that the system has several superior characteristics in terms of encryption and decryption key and later the authors proposed to apply Extended RBAC for authentication on this proposed architecture. It is believed that the proposed system has the potential to be useful in commercial situations as it captures practical access policies based on roles in a flexible manner and provides secure data storage in the cloud enforcing these access policies.

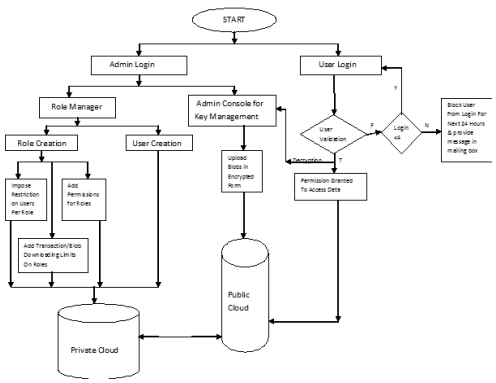

Figure 1 Hybrid Cloud for Secure Data with RBAC

REFERENCES

[1] P.Mell and T. Grance, "The NIST Definition of Cloud Computing", 2011.
[2] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud : Outsourcing computation without outsourcing control. pages 85–90, 2009.
[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. "Above the clouds: A berkeley view of cloud computing. Technical report, EECS Department, University of California, Berkeley", 2009.
[4] Wikipedia. Amazon elastic compute cloud — Wikipedia, the free encyclopedia, 2012.
[5] Amazon Web Services: Overview of Security Processes, may 2011.
[6] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: Outsourcing computation without outsourcing control. pages 85–90, 2009.
[7] Google Docs experienced data breach during March 2009. http://blogs.wsj.com/
[8] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds", Proc. 16th ACM conference on Computer and communications security, 2009, pp. 199-212.
[9] N. Santos, K.P. Gummadi, and R. Rodrigues,"Towards trusted cloud computing", Proc. 2009 conference on Hot topics in cloud computing,2009.
[10] C. Dovrolis, P. Ramanathan, and D. Moore, "What do packet dispersion techniques measure?" In Proc. IEEE INFOCOM, pp. 905-914, 2001.
[11] F. R. Institute. (2010). Personal Data in the Cloud: A Global Survey of Consumer Attitudes [Online].
[12] (2010). From Hype to Future: KPMG's 2010 Cloud Computing Survey [Online].
[13] R. Sandhu. "Role hierarchies and constraints for latice-based access controls." In E. Bertino, H. Kurth, G. Martella, and E Monotolivo Eds. LNCS 1146, Proceedings of the European Symposium on Research in Computer Security 1996, Rome, Italy.
[14] E. Bertino, P. A. Bonati, and E. Ferrari, "TRBAC: A temporal role-based access control model", ACM Transactions on Information and System Security, 4(3):191-233, 2001.
[15] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-Based access control models", IEEE Computer, 29(2):38-47, 1996.
[16] S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy", ACM Trans. Comput. Syst., vol. 1, no. 3, pp. 239–248, 1983.
[17] M. J. Atallah, K. B. Frikken, and M. Blanton, "Dynamic and efficient key management for access hierarchies", in Proc. ACM Conf. Comput. Commun. Sec., pp. 905-914.Nov. 2005.
[18] H. R. Hassen, A. Bouabdallah, H. Bettahar, and Y. Challal, "Key management for content access control in a hierarchy", Comput. Netw., vol. 51, no. 11, pp. 3197–3219, 2007.
[19] S. D. C. Di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data", in Proc. VLDB, Sep. 2007, pp. 123–134.
[20] C. Blundo, S. Cimato, S. D. C. Di Vimercati, A. D. Santis, S. Foresti, S. Paraboschi, et al., "Efficient key management for enforcing access control in outsourced scenarios," in SEC (IFIP), vol. 297. New York, NY, USA: Springer-Verlag, pp. 364–375, May 2009.
[21] P. Samarati and S. D. C. di Vimercati, "Data protection in outsourcing scenarios: Issues and directions", in Proc. ASIACCS, Apr. 2010, pp. 1–14.
[22] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," in ASIACRYPT, vol. 2501. New York, NY, USA: Springer-Verlag, , pp. 548–566 2002.
[23] D. Boneh, X. Boyen, and E.-J. Goh, "Hierarchical identity based encryption with constant size ciphertext", in EUROCRYPT, vol. 3494. New York, NY, USA: Springer- Verlag, pp. 440–456 May 2005.