International Journal of Advanced Trends in Computer Applications
www.ijatca.com

Privacy Model Access for Outsourced Data in Hybrid Clouds

[1]Er. Mamoon Rashid, [2]Er. Sanjay Madaan
[1]Assistant Professor,
School of Computer Science Engineering,
Lovely Professional University,
Jalandhar, India.
[2]Research Scholar (Ph.D), University College of Engineering,
Punjabi University, Patiala

Abstract: *The continuity in the evolution of Cloud computing has transformed into managed cloud offerings where providers are now completing those hands-on activities on behalf of the client in a cloud environment. Due to managed cloud providers turning hybrid cloud providers, cloud computing also continues to gain the outsourcing market in ways that are lifting traditional outsourcing from the forefront. Outsourced storage make shared data and resources much more accessible as users can retrieve them anywhere away from the rich in terms of personal computers to smart phones. 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 proposed and implemented the access control and authentication mechanism for hybrid cloud architecture 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 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,Managed,Encryption, Cloud, Cryptography.*

I. INTRODUCTION

Cloud computing is the utility, where cloud customers can remotely store their data into the cloud to enjoy the high quality networks, servers, applications and services from a shared pool of configurable computing resources [1]. 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 [2]: “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.”

Cloud computing offers a value proposition that is different from traditional enterprise IT environments. By providing a way to exploit virtualization and aggregate computing resources, cloud computing can offer economies of scale that would otherwise be unavailable. With minimal upfront investment, cloud computing enables global reach of services and information through an elastic utility computing environment that supports on-demand scalability. Cloud computing can also offer pre-built solutions and services, backed by the skills necessary to run and maintain them, potentially lowering risk and removing the need for the organization to retain a group of scarce highly skilled staff.

Along with the widespread enthusiasm on cloud computing, however, concerns on data security with cloud storage are arising due to unreliability of the service and malicious attacks from hackers. Recently more and more events on cloud service outage or server corruption with major cloud infrastructure providers are reported [3–5]. Data breaches of noteworthy cloud services also appear from time to time [6]. Besides, the cloud service providers may also voluntarily examine customers' data for various motivations. Therefore, we argue that the cloud is intrinsically neither secure nor reliable from the view point of the cloud customers. Most of the cloud services users have concerns about their private data that it may be used for other purposes or sent to other cloud service providers [7]. The user data that need to be protected includes four parts [8] which are usage data, sensitive information, personally identifiable information and unique device identities

The remainder of the paper is organized as follows. Section II discusses the related work. In Section III presents the details and the flow of the major work to be covered in this architecture. The authors introduce the construction of the new cloud security model and architecture with two tier encryption. In Section IV, the authors provide implementation of the proposed architecture. In Section V the authors discuss results and comparison study of implemented architecture with other models. Finally, Section VI discusses future extensions and concludes the paper.

II. RELATED WORK

Several recent surveys [9], [10] 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.

In the literature, there exist many hierarchy access control schemes [11, 12, 13] which have been constructed based on hierarchical key management schemes, and approaches using HKM schemes to enforce RBAC policies for data storage are discussed in [14, 15, 16]. 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, such as [17-18]. 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. PROPOSED PRIVACY ALGORITHM FOR HYBRID CLOUD MODEL

To protect the privacy of the data, some measures need 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 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.

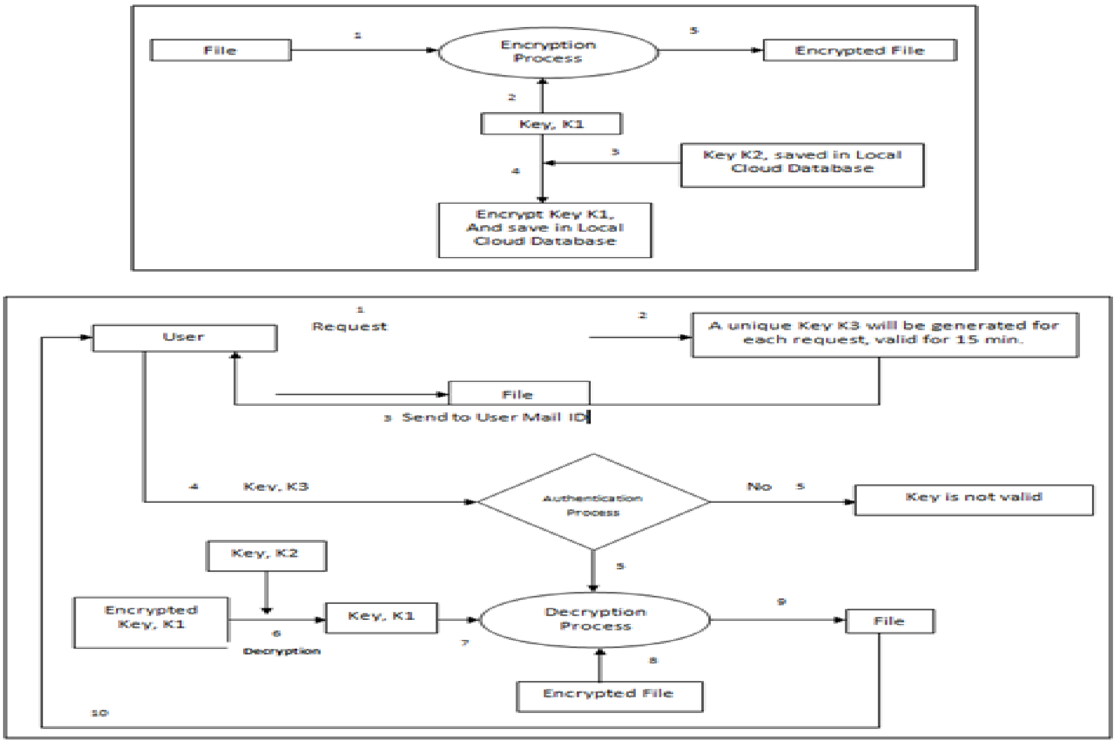


Fig. 1 Two- way authentication algorithm for Encryption and Decryption

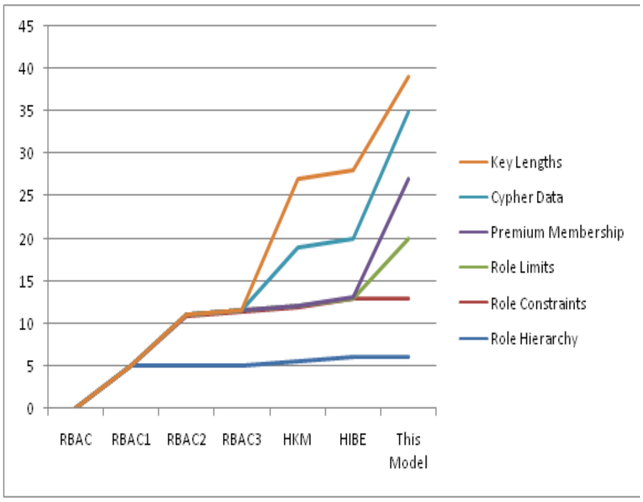
IV. IMPLEMENTATION

The authors have implemented the hybrid architecture for data storage with extended RBAC. The system is implemented in MVC Framework. Later this implemented web service is hosted on Microsoft's Azure cloud platform where the cloud use SQL database for its main storage of table contents which is to be stored on private cloud within an organization. Next the authors uploaded the data on this third party Public Cloud via implemented interface for hybrid cloud architecture for whose storage the authors created a storage account on Microsoft Azure Platform. Finally the authors allowed users to make access of this already stored data on Microsoft Azure cloud via this for hybrid cloud architecture.

The authors have performed experiments on a machine with Pentium (R) dual core t4400 @ 2.20 GHz processor, 4 GB of RAM and Microsoft Windows 7 Home Premium 32 bit Operating System. Once the administrator of this hybrid cloud architecture makes successful login, then s/he will be redirected to the main interface of this hybrid architecture where s/he can now go for the creation of roles and then impose permissions on these created roles. Here at this time the administrator can decide how many users can be allowed to use this particular role in future and also the download limit is defined for these users. After then s/he can create users who can be made members for already created roles based on their accessing attributes. While creating the users, the administrator will decide that particular role to which this user is made a member and also the nature of accessing data is decided over here i.e. whether the permissions and downloading limit constraints are to be imposed on this user or not which will be decided on the premium membership to be purchased by this user. Here the administrator will generate the passwords for users as well by virtue of which users can make their login in future for accessing this architecture. Next the administrator will upload the data content which is to be stored in storage account already created on Windows Azure Cloud. Now authentic users can make login to this architecture to access the stored data on Microsoft Azure Cloud Storage account. Here if any unknown user will try to access this web interface and validation fails, then s/he can be warned in several attempts to go for authentic details and then in next attempt s/he can be blocked for some time specific time interval to be decided by the administrator. This is the added security mechanism in this architecture which will enhance the security mechanism for accessing the implemented architecture. Once making successful login the users can access and download the stored content on Cloud based on their permissions and restrictions imposed on them which were initially decided in admin interfaces of the architecture and moreover for downloading every data file on cloud, s/he needs to provide secret key for decrypting the data which will be already provided to that user in mailbox.

V. RESULTS

The experimental study of this running system proved this architecture to be better in terms of constraints and the performance comparison of every activity to be shown as well in terms of the following line chart given in Fig 2.



VI. CONCLUSION

This implemented model has outlined a sketch for new system which addresses the security features for any multi-centric application. Then the authors implemented a secure model based hybrid cloud storage architecture which allowed 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 implemented 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 implemented and applied the Extended RBAC for authentication on this hybrid architecture.

REFERENCES

[1]. I. Foster, Y. Zhao, I. Raicu, and S. Lu, “Cloud computing and grid computing 360-degree compared”, Grid Computing Environments Workshop, GCE’08, pp. 1-10, 2009.

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

[3]. Blog service hosted by google crashes review.http://hostwisely.com/blog/blog-service-hosted-by-googlecrashes.

[4]. Keir Thomas,“Microsoft cloud data breach heralds things to come”, Tech world, 29 December, 2010.

[5]. Summary of the amazon ec2 and amazon rds service disruption in the US East region. http://aws.amazon.com/message/65648.

[6]. Darlene Storm, “Epsilon breach: hack of the century”, 2011. http://blogs.computerworld.com/18079/epsilon_breach_hack_of_the_century.

[7]. Siani Pearson, “Taking Account of Privacy when Designing Cloud Computing Services”, CLOUD’09, Vancouver, Canada, pp. 44-52, May 23, 2009.

[8]. European Network and Information Security Agency (ENISA)“Benefits, risks and recommendations for information security”, Accessed: 28, December 2013.

[9]. F. R. Institute. (2010). Personal Data in the Cloud: A Global Survey of Consumer Attitudes [Online].

[10]. *From* Hype to Future: KPMG’s 2010 Cloud Computing Survey [Online].

[11]. 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.

[12]. M. J. Atallah, K. B. Frikken, and M. Blanton, “Dynamic and efficient key management for access hierarchies”, in Proc. ACM Conference Comput. Commun. Sec., pp. 905-914.Nov, 2005.

[13]. 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.

[14]. 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, pp. 123–134, Sep. 2007.

[15]. 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.

[16]. P. Samarati and S. D. C. di Vimercati, “Data protection in outsourcing scenarios: Issues and directions”, in *Proc. ASIACCS*, pp. 1–14, Apr. 2010.

[17]. C. Gentry and A. Silverberg, “Hierarchical ID-based cryptography,” in ASIACRYPT, vol. 2501. New York, NY, USA: Springer-Verlag, , pp. 548–566, 2002.

[18]. 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.