ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

AUTHENTICATED RELIABLE INFORMATION SHARING IN CLOUD ENVIRONMENT

Magesh Kumar S*, Sathish Kumar P.J*, Parthipan V#
*Research Scholars, Bharath Institute of Higher Education and Research
Bharath University, Chennai, TamilNadu, India.
#Assistant Professor, IT Dept, Lord Venkateshwaraa Engineering College, Kanchipuram, TamilNadu, India
Email: mageshkumars@yahoo.com

Received on: 15.10.2016 *Accepted on: 22.11.2016*

Abstract

Hybrid cloud is the combination of public cloud and private cloud as per the security of information in the private cloud is very essential. Proposed scheme of security is to provide two different set of keys to the private and public cloud users, with that keys private cloud users are given privilege to access public cloud too. The keys will be changed whenever the change in user occurs. Initially public cloud users and private cloud users are segregated in a tree structure for easy and secure key transaction and information transaction. A lattice cluster model structure is developed for transacting secure keys between users before transacting data by this effective and secure transfer of data takes place between the users.

Keywords: Multicast key; Hybrid cloud; lattice model.

Introduction

Hybrid is the cloud which is very popular nowadays the hybrid cloud comprises of both public and private cloud .The cloud is the is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet).

The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing is broadly classified into Public Cloud, Private Cloud, and Hybrid Cloud.[4]

Public Cloud Computing - It is the IT infrastructure that is used by many companies and services at the same time. Data users of the clouds are not able to manage and maintain this cloud; the entire responsibility for these matters rests with the owner of the cloud. Subscriber services can be offered by any company and individual user. They offer an easy and affordable way to deploy Web sites and business systems, with high scalability, which in other solutions would be available.

Private Cloud Computing – A secure IT infrastructure is controlled and operated for the benefit of a single organization. The organization can manage its own private cloud or outsource this task from an external contractor. Infrastructure can be placed either on the premises of the customer, or in a data center. Ideal private cloud is the cloud that is deployed in the organization premises, served and controlled by its employees.

Hybrid cloud Computing –This type of cloud is used when an organization has seasonal periods of activity, in other words, once the internal IT infrastructure cannot cope with current challenges, some facilities are transferred to a public cloud (e.g. large amounts of statistical information, which is in its raw form or something that does not represent value for the enterprise), as well as to provide user access to enterprise resources (for private cloud) via a public cloud. Trend Micro, a cloud security company, recently conducted a survey which indicated that public cloud services fail to meet IT and business requirements of some of the business organizations. A hybrid cloud environment can help meet their needs. In some ways, hybrid clouds can be considered an intermediate stage as enterprises prepare to move most of their workloads to public clouds.[4]

Trend Micro Survey Results

A recent survey conducted by Trend Micro offers some insights into the expectations and concerns businesses have about cloud technologies. The survey was conducted in six different countries with 1200 respondents from companies with at least 500 employees. Some of the key results are:

- 38% of the survey respondents say that their IT requirements are not being met by the cloud providers. Similarly, 38% claimed that their current cloud service providers are not meeting their business needs.
- For companies that have public cloud or hybrid applications currently in production, 45% of the existing applications are already deployed in the cloud and an average of 53% of new applications will be deployed in the cloud.
- 49% of the survey respondents indicated that if they knew how to secure their data in the cloud, it would increase their consideration for cloud adoption.

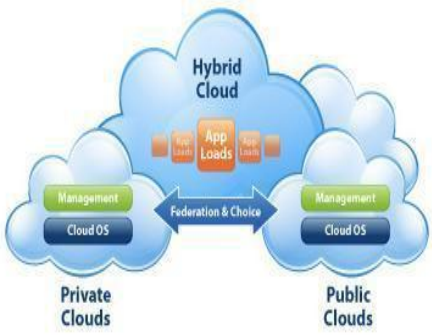

Fig:1. Hybrid Cloud Structure.

Increasingly, companies are realizing that the use of a hybrid cloud expands the number of applications they deploy into the cloud. However, almost half (49%) feel they need to improve their knowledge of cloud security to further increase cloud adoption. Using hybrid clouds will help them understand the security implications of the public clouds better before they move all their workloads there. Even though the need of cloud is more and essential as per the security issues it faces security threats that should be overcome to provide better services. Security Best Practices Many organizations will consider moving to public clouds if they understand how they can secure their data in the cloud. Hybrid clouds can serve as a transitional approach and help businesses fine tune their strategies for future public cloud adoption. Hybrid clouds offer businesses a safe shell from which they can try out public cloud services, while still maintaining sensitive data in a more controlled private cloud. There are some best practices that will help mitigate the risks associated with hybrid cloud deployments. In this section, we will highlight some of them.

● **VM-level security**: The perimeter of the hybrid cloud environment is not only elastic but also spans multiple clouds including on-premise private clouds. This calls for self defending security at the virtual machine level that travels through the on-premise data center, in the cloud and between multiple cloud providers.

● **Multi-layered defense**: Using tools like firewall, IDS/IPS, log inspection, etc. geared towards virtual machines is important. More importantly, the traffic between the virtual machines should be continuously monitored by setting policies appropriately.

● **Traffic control**: An on-premise gateway should be used to control incoming traffic to the public cloud rather than provide direct access.

● **Data and encryption**: Data in the cloud should be encrypted. An encryption solution should have well-designed encryption key management policies to ensure data integrity. Also, the business should retain encryption-key ownership to maintain separation of duties between the business and the public cloud service provider. This also allows the business to apply their encryption across its private and public clouds and prevents vendor lock in, allowing the organization to move between cloud vendors.

● **Security control**: Cloud security should be controlled by the business and not the cloud vendor. Whether it is by using single sign-on or by using a third-party tool to securely extend the perimeter to the public cloud, the control over security should be with the business organization deploying the hybrid environment.

● **Regulatory compliance**: Businesses should understand the impact of regulations and assess which policies and procedures change with respect to the hybrid cloud deployment. Companies should realize the nature of this change

and associated impact; develop processes to collect evidence, such as audit logs; and store this evidence securely. It is absolutely critical to collect the necessary evidence from the cloud provider and store it outside the public cloud environment. Also, businesses will benefit from selecting an auditor who understands the changed dynamics and challenges of using public cloud services.

Though the hybrid cloud posses these security, while transacting data the security is needed in various aspects like user authentication ,denial of service to the user who possess the authenticated key so on. There are some irregularities can be noticed while transacting the keys to the authenticated users, to avoid this a novel method is introduced based on multicast key management for disseminating keys between users and maintaining security while transacting the data from datacenter.

B. Multicast Operation

Multicast algorithms for clusters can achieve high performance by using an expensive algorithm that requires monitoring data to construct a high-throughput spanning tree, but they cannot adapt well to dynamic and unstable changes in network throughput. Multicast algorithms for P2P systems are scalable and can adapt well to network performance changes. However, It is difficult to use P2P algorithms to achieve high performance because they overly assume that not only the network but also the availability of the data and the nodes is unstable, resulting in significant overhead.

Our proposed algorithm achieves both high performance and scalability by combining the advantages of multicast algorithms for clusters and P2P systems. The multicast algorithm proposed by Van de is a well known algorithm for clusters and multiclusters environments. It achieves high performance multicast operations, the data stored in cloud is divided to be multicast into blocks of equal sizes based upon the number of nodes, these blocks are then send to the respective nodes, after all the nodes receives the blocks, they exchange the missing blocks with the neighboring nodes.

Both the concerns about security can be address using the lattice model during the processing of data from its storage to the applications nodes for computation. Next section will brief out the lattice model for secure information flow in cloud scenario.

Secure Multicasting Management

Group key: In using secure multicast, the key server must updated GKs of whole system whenever user joins or leaves. If new user (assume as an attacker) tries to join the service, he already collected all data in history. If the

system user the same key in the past, the eavesdropper may discover all data in history. In the other case, the trusted user want to leave the service, then the eavesdropper can attack that user and discover the GK. These are the reason why the system must updated key when user joins or leaves.

However, if secure multicast applies only one method such GK, number of updated keys is very large whenever joining/leaving. For this reason, we apply the theoretical model for secure multicast method as to improve this issue.

Theoretical Model for Secure Multicast

This model will provide us with multilevel security by using the structure of lattice for processing of data from the cloud storage to various clusters of computational nodes.Figure1.Shows the architecture of lattice based secure multicast algorithm on clouds, this architecture has three components: Hybrid Cloud Storage, Lattice Model and Cluster of Nodes.

i)**Hybrid Cloud Storage**

which is required to storing huge amount of data. It provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web. It gives developer access to the same highly scalable, reliable, fast, inexpensive data storage.

ii) **Lattice Model for secure information flow**

Here we make use of lattice structure for secured information flow. Information flow is controlled by assigning security class to every object. When information flow is between objects „Pc" and „PUc", indicates that the information flow is between the security class „Pc" and security class „PUc".

According to Denning the concept of lattice in information flow policies are as follows:

1.The set of security classes SC is finite.

2.The can-flow relation → is a partial order on SC. 3.SC has a lower bound with respect to→.

4. The join operator ⊕ is totally defined least upper operator.

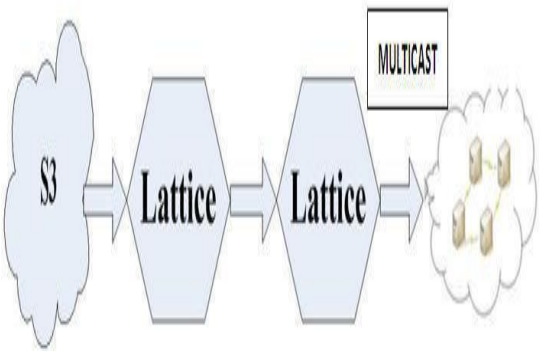

Fig 2: Lattice Based Secure Multicast algorithm on clouds

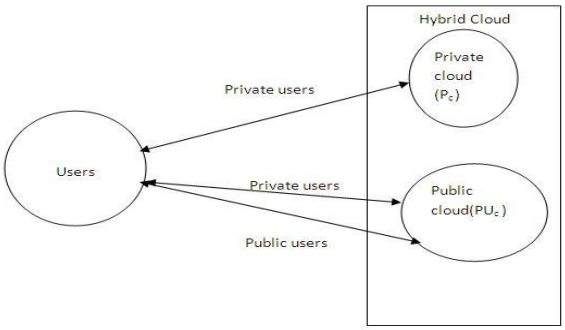

Fig 3: Lattice of 2 users Set {Pc, PUc}

With reference to figure.3, Access control and multilevel security is very much possible using Lattice structure [3]. Consider the scenario, if set „Pc‟ of users has set of permissions, and set „PUc‟ of users has set Γ of permissions, then Pc ∪ PUc has permissions ∩ Γ and Pc ∩ PUc has permissions ∪Γ.

Both access groups and permissions have lattice structure based on set inclusion. S is a finite set of security classes arranged on a lattice and → ⊆S ×S is a flow relation, which specifies permitted information flow between pairs of security classifications. Objects „Pc‟ and ‟PUc‟ in a system are assigned security classes „Pc‟ and „PUc‟ respectively and information is permitted to flow from „Pc‟ to „PUc‟ if and only if. (Pc, PUc)∈ → (written as Pc, PUc)

Algorithm: Secure Multicast

Step 1.Consider the Hybrid Cloud Storage from which data has to be multicast to multiple computational nodes through lattice structure. Step 2.Encrypt, Decrypt, Join, Compose.

Use lattice Cluster structure to perform the following set of operations

- Sampling a lattice L according to Gaussian mixture model distribution for parameters.
- Input a basis h of L such that ||h|| is a little bit less than S. For any lattice basis h Є $Z^{n \times k}$ any real S ≥ ||h|| .ω(√log n) whose output distribution is within negligible distance of $D_{£(h),S,C}$. The running time is expressed in terms of polynomial in n and the size of its input (h,s, c).
- Lattice1 performs encryption, join endomorphism with lattice2. (Refer appendix- Join and Compose using fitting Lemma) Distance preserving lemma i.e. Isometry (refer appendix) is used to ensure message integrity.
- After decryption, Composition is done at the lattice 2 using Fitting Lemma and then message is sent to the cluster.

Mixture models are a type of density models which that comprise a number of component functions, usually Gaussian[3]. A mixture of *K* Gaussians is:

$$\sum_{k=1}^{K} \alpha_k \, \mathrm{G}(x; \mu_k, \sigma_k)$$

$$\mathrm{P}(\omega|\mathrm{x}) = = \sum_{k=1}^{K} \alpha_k \cdot \frac{1}{(2\pi)^{d/2} |\boldsymbol{\Sigma}_k|^{\frac{1}{2}}} \exp\left\{ -\frac{1}{2} (\mathbf{x} - \boldsymbol{\mu}_k)^T \boldsymbol{\Sigma}_k \sum_{k=1}^{K} \alpha_k = 1_{,k}) \right\},$$

The parameters of a Gaussian mixture model are estimated by the above mentioned methods. For each user hybrid cloud , the probability of being relevant is calculated.

Conclusion

The hybrid cloud computing provides various internet based, on demand service like software ,hardware ,Server ,Infrastructure and data storage. In this paper, we have highlighted various security concerns such confidentiality and integrity of data and summarized few implications. We have focused on secure multicast algorithm by using multilevel security provided by lattice model to help us for secure follow of information by Gaussian mixture model distribution. The lattice model is boots trappable and runs in polynomial time and our secure scheme shows that it is multicast in hybrid cloud environment.

References

1. Y. Zhu, J. Wang, and C. Wang, "Ripple: A publish/subscribe service for multidata item updates propagation in the cloud," *Journal of Network and Computer Applications*, vol. In Press, Corrected Proof, pp.320, 2010. Available:http://www.sciencedirect.com/science/article/B6WKB-508X3MK-1/2/764c9645e3ce1bc875e021d9853d1370.
2. M. Srivatsa, A. Iyengar, J. Yin, and L. Liu, "Scalable key management algorithms for locationbased services," *IEEE/ACM Trans. Netw.*, vol. 17,pp. 1399–1412, October 2009. [Online]. Available: http://dx.doi.org/10.1109/TNET.2008.2010222.
3. *Fang Qian1, Mingjing Li2, Lei Zhang2, Hong-Jiang Zhang2, Bo Zhang1* Gaussian Mixture Model For Relevance Feedback In Image Retrieval **,** China.
4. Krishnan Subramanian "Hybrid Clouds", by Trend Micro Inc,2011
5. Tien-Dung Nguyen, Eui-Nam Huh "An efficient key management for secure multicast in Sensor-Cloud" International Conference on Computers, Networks, Systems, and Industrial Engineering 2011.
6. Parthipan V, Sriprasadh K, Magesh Kumar S, "Secure Information Transaction in Hybrid Cloud Computing, "IEEE Explore ISBN NO 978-1-4673-5786-9.