ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Scalable Media in Cloud Assisted Content Sharing Network Based on Attribute Access

Fahad Ayad Khaleel
Master of Science (Information System),
Nizam College (Autonomous), O.U,
Basheer Bagh, Hyderabad.

ABSTRACT:

With rapid development of cloud computing, more and more enterprises will outsource their sensitive data for sharing in a cloud. To keep the shared data confidential against untrusted cloud service providers (CSPs), a natural way is to store only the encrypted data in a cloud. The key problems of this approach include establishing access control for the encrypted data, and revoking the access rights from users when they are no longer authorized to access the encrypted data. This paper aims to solve both problems. First, we propose a hierarchical attribute-based encryption scheme (HABE) by combining a hierarchical identity-based encryption (HIBE) system and a ciphertext-policy attribute-based encryption (CP-ABE) system, so as to provide not only fine-grained access control, but also full delegation and high performance. Then, we propose a scalable revocation scheme by applying proxy re-encryption (PRE) and lazy re-encryption (LRE) to the HABE scheme, so as to efficiently revoke access rights from users.

Key words:

hierarchical identity-based encryption, proxy re-encryption, cloud service providers, sensitive data, untrusted cloud.

INTRODUCTION:
Cloud Computing:

Cloud computing promises new career opportunities for IT professionals. In many cases, existing core skill sets transfer directly to cloud technologies. In other instances, IT pros need to develop new skill sets that meet the demand of emerging cloud job roles.

Companies that consider moving to cloud computing will want to educate their IT professionals about the potential opportunities ahead so that they can build staff capabilities and skills ahead of the change. Chief Information Officers (CIO) who want to generate more business value from IT by necessity have to be in the front line of cloud skills education — both for themselves and to build training capacity for their IT staff. The emerging cloud world offers those with the capability to build and grow their portfolio of skills. This paper explores the advantages of moving to the cloud and outlines the delta skill sets IT pros will want to acquire. It describes what the cloud offers and how it applies to and impacts existing infrastructure, including such issues as cost, security, data control, and integrity.

The bulk of an IT professional's skills remain relevant in a cloud environment. System configuration tasks such as creating routing rules, configuring archiving, and managing policies are still necessary. The change is moving from building and supporting local IT infrastructure to managing IT services in the cloud, which requires an extension of skills and capabilities. For example, many IT professionals have the capability to manage virtual storage and the virtualization of servers, but will need to adjust their skill sets to function within a private or public cloud. IT professionals with the flexibility to adapt their technical skills while retaining and growing their business skills will be the highest in demand.

One way IT professionals become more essential in the cloud era has to do with their ability to implement public cloud services like Microsoft® Office 365 and Windows Azure®. Office 365 offers enterprises the capability to move key collaboration products and services such as Microsoft®

SharePoint®, Microsoft® Exchange Server, and Microsoft® Lync™ Server from an on-premise deployment model to a public cloud model. Windows Azure facilitates either moving existing customer applications to or building new applications in the public cloud. While managing and configuring these various services remains in the IT professional's hands, the majority of the infrastructure tasks are eliminated. Tasks that remain include monitoring, configuration, and integration with existing on-premise services such as Active Directory, while activities such as purchasing hardware, installing operating systems and managing patches are no longer needed since they are handled by the cloud provider.

Skills Impacts in Cloud Computing:

The move to cloud solutions opens up new opportunities for IT professionals. Key technical skill sets become more critical to career success, including custom application development and deep technical knowledge of the various collaboration products such as Exchange Server. These skill sets can be used to complement and enable customization of the provider cloud offerings. IT should look for opportunities to reduce tactical day-to-day support and spend more time developing and delivering services and applications that demonstrate value to the business.

"I think new marketing efforts will change and help IT administrators in their understanding of what the cloud portends," said Kay Sellenrode, Senior Technical Consultant for Platani. "IT professionals and developers face quite some challenges. But they represent good challenges. IT professionals need to see the new version of cloud as a product they would deal with in-house. They know the basics already. What's important is not what they're doing, but where they're doing it."The need for design skills will remain. The principal difference is that the infrastructure may be hosted outside the company. Additionally this will include more care of service agreements and less maintaining the service running Windows Server."They can give themselves new names; a network administrator can become a cloud administrator," he explained. "Once they learn more about the cloud and they see there's a big change that will help them in the future, it will become clear to them that they will have a job that is more challenging than just being an administrator."

In general, IT professionals should prepare for the multitude of cloud environments in which they might work. New paths are presenting themselves and options abound. Administrators may choose to shift to consulting, which entails enhancing their soft skills and beginning to focus on serving business needs. They may end up serving as a liaison between business divisions and IT within an enterprise. Contrastingly, they may also choose to deepen their technical skill sets and specialize in building and configuring the stack itself.

Considerations for Developers:

Developers will have to focus on innovation, integration, and rapid delivery on business requirements. They also will find more design opportunities beyond what they currently manage. Developers will need to work effectively with a much broader group of IT professionals for solutions they are developing. IT will also need to work more closely with business units to find out what they can do to help improve the productivity in departments such as marketing, human resources, and finance. Since enterprises can adopt more varied solutions in the cloud, it becomes vital to ensure that the selected solutions address any required service agreements between the business and IT.

Security Implications:

Cloud solutions have new security implications for consideration. Organizations in different industries have divergent requirements regarding privacy and data retention. This means that the solution selected by an organization or an enterprise must be carefully evaluated to ensure that the selected services allow the organization to remain in compliance. International companies may need to comply with regulations that vary by country or economic region. These must also be taken into consideration by the IT professional when selecting a cloud-based service.Managing security and compliance involves translating enterprise compliance requirements into a technology implementation. This requires practical skills and an understanding of implementing compliance within the deployed solutions. IT professionals will benefit from sharpening their security skills, including knowledge around data protection, privacy standards, and secure message integrity. Secure messaging may include topics such as encryption, digital signing, and malware protection. Additional skill sets of value include identity management, authentication methods, and auditing.

Understanding IT as a Service:

To understand IT as a service it is best to start with an understanding of the cloud models implemented today. Cloud services can be delivered in one of multiple formats. Often, an IT department will start with a private cloud environment and perhaps focus on deploying virtual servers. This is commonly referred to as infrastructure as a service and represents one of the flavors of IT as a service that is available within the world of cloud computing. Since this is only a single example of the possible cloud models, IT professionals must become familiar with a variety of cloud standards so that they can select appropriately based on the needs of the enterprise. It is common to divide cloud computing into three categories:

- Infrastructure as a service (IaaS), which provides flexible ways to create, use and manage virtual machines (VMs).

- Platform as a service (PaaS), focused on providing the higher-level capabilities — more than just VMs — required to support applications.

- Software as a service (SaaS), the applications that provide business value for users.

Deployment Models:

For each cloud computing category there are additional decisions regarding the type of cloud chosen. The type of cloud that is selected determines the placement and usage model of the physical infrastructure that is being removed from the customer's datacenter world. Essentially, the cloud computing deployment model describes where the software runs and includes the following options:

- A private cloud is a set of standardized computing resources that is dedicated to an organization, usually on-premises in the organization's datacenter. It works with the current capital investment and delivers the new functions as a service.

- A hosted private cloud has a dedicated infrastructure hosted by a third party, inaccessible to other organizations.

- A public cloud consists of computing resources hosted externally but shared with other organizations and dynamically provisioned and billed on a utility basis — the customer will pay for what is used as they use it.

PROBLEM STATEMENT :

In Existing System, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. Letting each user obtain keys from every owner who's records she wants to read would limit the accessibility since patients are not always online. An alternative is to employ a central authority (CA) to do the key management on behalf of all record owners, but this requires too much trust on a single authority (i.e., cause the key escrow problem). Key escrow (also known as a "fair" cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

PROBLEM DEFINITION:

An information management architecture using CP-ABE and optimized security enforcement efficiency . Furthermore, they employed the architecture and optimization method on two example applications:

An HIPAA (Health Insurance Portability and Accountability Act) compliant distributed file system and a content delivery network.

An approach to access control in content sharing services is to empower users to enforce access controls on their data directly, rather than through a central administrator. However, this requires flexible and scalable cryptographic key management to support complex access control policies. A native access control solution is to assign one key for each user attribute, distribute the appropriate keys to users who have the corresponding attributes, and encrypt the media with the attribute keys repeatedly.

IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Registration:

In this module normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files – leaf nodes is atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader has access to.

- PUD - public domains

- PSD - personal domains

- AA - attribute authority

- MA-ABE - multi-authority ABE

- KP-ABE - Key Policy Attribute based Encryption

- MCP-ABE - Multi-message Cipher-text Policy Attribute-Based Encryption

Attribute oriented access control:

In this Module, supports fine-grained access control policies and dynamic group membership6 by using CP-ABE scheme. In addition, is able to revoke a user without issuing new keys to other users or re-encrypting existing cipher-texts by using a proxy. KP-ABE (Key Policy Attribute based Encryption) to enforce access policies based on data attributes. Their scheme allows data owners to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents by combining techniques of attribute-based encryption, proxy re-encryption, and lazy re-encryption an information management architecture using CP-ABE and optimized security.

One-way hash function:

In this Module, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string. A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.

Cipher-text policy attribute-based encryption:

In this Module, every user's personal secret key is associated with a set of attributes while every cipher text is associated with an access policy. A user successfully decrypts a cipher text only if her set of attributes satisfies the access policy specified in the cipher text. We briefly describe the CP-ABE. We will extend this CP-ABE scheme to MCP-ABE scheme and use the latter in our access control scheme.

- AB-Setup

It is an initialization algorithm run by an Attribute Authority (AA). It takes as input a security and outputs a public key PK and a master secret key.

- AB-Keygen

It is run by AA to issue a personal secret key to a user. It takes as input MK and the set of attributes A of the user, and outputs the personal secret key SK associated with Specifically, for each user.

- AB-Encrypt

Data owner to encrypt a message according to an access tree.

- AB-Decrypt

Data consumer in possession of a set of attributes A and the secret key SK in order to decrypt the ciphertext CT with an access policy.

CONCLUSION:

In order to share media content in a controllable manner, a suitable access control mechanism should be deployed.

CP-ABE based access control allows a data owner to enforce access control based on attributes of data consumers without explicitly naming the specific data consumers. However, CP-ABE supports only one privilege level and hence is not suitable for access control to scalable media. In this paper we extended CP-ABE to a novel MCP-ABE and proposed a scheme to support multi-privilege access control to scalable media.

As cloud computing is increasingly being adopted and mobile devices are becoming pervasive, the present access control scheme allows a mobile user to offload computational intensive MCP-ABE operations to cloud servers while without compromising user's security. The experimental results indicated that the proposed access control scheme is efficient for securely and flexibly managing media content in large, loosely-coupled, distributed systems. With the assistance of the cloud server, the decryption operation is accelerated significantly at the consumer side. However, the decryption may be still slow for low-end devices because a modular exponentiation operation is required. Thus, one future work is how to speed-up the decryption operation at low-end devices.

BIBLOGRAPHY:

Good Teachers are worth more than thousand books, we have them in Our Department.

References Made From:

1.User Interfaces in C#: Windows Forms and Custom Controls by Matthew MacDonald.

2.Applied Microsoft® .NET Framework Programming (Pro-Developer) by Jeffrey Richter.

3.Practical .Net2 and C#2: Harness the Platform, the Language, and the Framework by Patrick Smacchia.

4.Data Communications and Networking, by Behrouz A Forouzan.

5.Computer Networking: A Top-Down Approach, by James F. Kurose.

6.Operating System Concepts, by Abraham Silberschatz.

7.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," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.

8."The apache cassandra project," http://cassandra.apache.org/.

9. L. Lamport, "The part-time parliament," ACM Transactions on Computer Systems, vol. 16, pp. 133–169, 1998.

10. N. Bonvin, T. G. Papaioannou, and K. Aberer, "Cost-efficient and differentiated data availability guarantees in data clouds," in Proc. of the ICDE, Long Beach, CA, USA, 2010.

SITES REFERRED:

» http://www.sourcefordgde.com

» htt]p://www.networkcomputing.com/

» http://www.ieee.org

» http://www.emule-project.net/

AUTHORS BIOGRAPHY:

fahad ayad khaleel, pursuing his Master of Science in Information System, from Nizam College (Autonomous),O.U,Basheer Bagh, Hyderabad,India.