ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 2 February, 2014 Page No. 3978-3981

Cloud Computing Security using Federated Key Management

Dr. Atulbhai Patel, Kalpit Soni

1. Principal, C.M.P.I.C.A., Charotar University of Science and Technology, Changa, Gujarat, India.
2. Ph.D. Research Scholar, Charotar University of Science and Technology, Changa, Gujarat, India

Abstract: Cloud Computing is solution in which resources such as hardware, software, network and storage requirement are provided to the user as per the demand. Basically Cloud Computing is the combination of private cloud and public cloud. This paper focus the overview of security issued which may arise during file sharing while adopting the hybrid clouds. It also focuses to use Federated Key Management in the cloud such that each user and each server will have its own unique identity, and the identity is allocated by the system hierarchy.

Keywords: Cloud Computing, Cryptography, Digital Identity,Encryption, Federated Key Management, Hybrid Cloud

1. Introduction: Cloud Computing is a relatively new business model in the computing world. In an October 2009 presentation titled "Effectively and Securely Using the Cloud Computing Paradigm,"[i] by Peter Mell and Time Grance of the National Institute of Standards and Technology (NIST) Information Technology Laboratory, Cloud Computing is defined as Follows: "Cloud Computing is a model for enabling ubiquitous, 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."[ii] The idea of Cloud Computing is based on a very fundamental principal of "Reusability of IT capabilities".[iii] With Internet access, Internet access are able to acquire computing resources, storage space and other kinds of software services according to their needs. In Cloud Computing, with a large number of various computing resources, users can easily solve their problems with the resources provided by a cloud. Using cloud computing service, users can store their critical data in servers and can access their data anywhere they can with the Internet. Also, different users in one system can share their information and work.

2. **Security in Cloud Computing:** Cloud computing have many advantages in cost reduction, resource sharing, and time saving for new service deployment. While in a cloud computing system, most data and software that users use reside on the Internet, which bring some new challenges for the system, especially security and privacy. Since each application may use resource from multiple servers. The servers are potentially based at multiple locations and the services provided by the cloud may use different infrastructures across organizations. All these characteristics of cloud computing make it complicated to provide security in cloud computing. To ensure adequate security in cloud computing, various security issues, such as authentication, data confidentiality and integrity, and non-repudiation, all need to be taken into account.

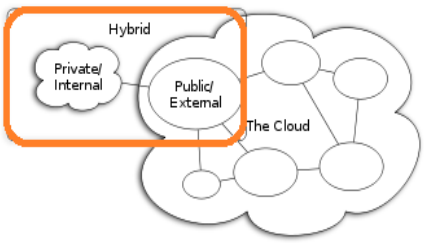

Figure 1: Cloud Type

Currently, as shown in Figure 1, there are three types of clouds in general: private cloud, public cloud and hybrid cloud.[iv] In a public cloud, resources are dynamically provisioned on a fine-

grained, self-service basis over the Internet. Services in the cloud are provided by an off-site third-party provider who shares resources and bills on a fine-grained utility computing basis. While in most private clouds, with limited computing resources, it is difficult for a private cloud to provide all services for their users, as some services may more resources than internal cloud can provide. Hybrid cloud is a potential solution for this issue since they can get the computing resources from external cloud computing providers. Private clouds have their advantages in corporation governance and offer reliable services, as well as they allow more control than public clouds do.

For the security concerns, in the public cloud, when a cloud environment is created inside a firewall, it can provide its users with less exposure to Internet security risks. Also in the private cloud, all the services can be accessed through internal connections rather than public Internet connections, which make it easier to use existing security measures and standards. This can make private clouds more appropriate for services with sensitive data that must be protected. While in a hybrid cloud, it includes more than one domain, which will increase the difficulty of security provision, especially key management and mutual authentication. The domains in a hybrid cloud can be heterogeneous networks; hence there may be gaps between these networks and between the different services providers. Even security can be well guaranteed in each of private/public cloud, while in a hybrid cloud with more than one kind of clouds that have different kinds of network conditions and different security policies, how to provide efficient security protection is much more difficult. For a hybrid cloud with a large number of domains, this will bring a problem for scalability. If different networks in a hybrid cloud using different authentication protocols, this problem can be more complex. In a cloud, the cloud computing system needs to provide a strong and user-friendly way for users to access all kinds of services in the system. When a user wants to run an application in the cloud, the user is required to provide a digital identity. Normally, this identity is a set of bytes that related to the user. Based on the digital identity, a cloud system can know what right this user has and what the user is allowed to do in the system. Most of cloud platforms include an identity service since identity information is required for most distributed applications.[v] These cloud computing systems will provide a digital identity for every user. For example, user with a Windows Live ID can use cloud computing services provided by Microsoft and user who wants to access cloud computing services from Amazon and Google also needs an Amazon defined identity and Google account. Here, each of these companies is a public cloud. The problem here is this digital identity can only be used in one private cloud or one public cloud. Users want to access services in the cloud that provided by different clouds will need to have multiple identities, each for one of the cloud. This is obviously not user friendly. To solve these problems in the cloud, we propose to use federated key (identity) management in clouds with HIBC. The proposed scheme does not only allow users from a cloud to access services from other clouds with a single digital identity, it also simplifies the key distribution and mutual authentication in a hybrid cloud. Let's look at exactly what this means and how it will probably work.

3. **Key Management:** A cryptographic key is much like the combination to a safe: if we have the right combination, it's easy to open a safe, but it's hard to open one without the right combination. Similarly, if we have the right key, decrypting encrypted data is easy, but decrypting it is impractical without this key. If we are careless with the combination to our safe, someone else can easily use it to open our safe, and the protection provided by the safe is compromised. Similarly, the cryptographic keys that we use to encrypt data need to be handled carefully. If we are careless with them then the protection provided by encryption can be essentially eliminated. Key management covers all the details of how to handle keys carefully enough to ensure this does not happen. Encryption only involves complicated mathematics that's incomprehensible to most people. Key management involves technology, people and processes, so it's even more difficult. Encryption provides an extremely high level of protection. Even with the world's most powerful supercomputers, hackers would need billions of years to beat modern encryption. Key management is nowhere near as robust. It's usually the weak link that limits how much protection data really gets, so it's important to get it right if we're serious about protecting sensitive data.

4. **Federation:** Federation describes how different computer systems can work together. In the context of key management, federation includes how different applications can get keys from the same key server. This is an important aspect of key management that needs to be addressed before encryption can be used to protect sensitive data in the cloud, and the lack of the ability to do federation dramatically limits the usefulness of many encryption and key management products today. Encrypting a backup tape in a data centre and decrypting it in an off-site disaster recovery site is a very simple example of federation. In this case, two different tape drives need to work with the same key server to get the key that's needed to encrypt or decrypt the backed-up data. But even extremely simple cases of federated key management can create problems that are hard to solve in practice. The *2009 Encryption and Key Management Industry Benchmark Report* from industry analyst firm Trust Catalyst estimates that

only 41 percent of businesses encrypt backup tapes, and that issues relating to key management are the most common reason for not doing so. If the simple cases are that hard, it's not hard to understand why there's no solution for the harder cases yet, but that's what we need to protect data in the cloud.

5. **Cloud Computing needs fully Federated Key Management:** In cloud computing, we have sensitive data that could be anywhere, and we need the ability for any application that needs access to this data to be able to decrypt it. To do this, we need a way for any application to be able to get the keys that it needs to decrypt data that it gets from the cloud and to use these keys in a careful way that keeps the data protected. More concisely, that's fully federated key management.

6. **Using Federated Key Management in Cloud:** If today's systems can't implement fully federated key management, what are the missing pieces? If we look more closely at how cryptographic keys are handled today, we can probably get a good idea of what's needed in the more general case. A cryptographic key always has additional information associated with it that uniquely identifies it. When a tape drive gets a key to use to encrypt stored data, for example, it also gets a unique key identifier which it stores with the encrypted data. To decrypt the encrypted data, the tape drive requests the key that corresponds to the key identifier that it finds with the encrypted data. It's possible to extend the idea of a key identifier to include information about the key server where the right key can be obtained. Instead of having a key identifier like this:

Key Identifier: 35624252655a6a75266c6f6753

We might have one like this:

Key Identifier: 35624252655a6a75266c6f6753
serverURL: https://data.test.com/

Where the additional information indicates the URL of the key server where the key can be obtained. If all applications understand how to handle such information when it's included in a key identifier, then they can easily use this information as the basis for federated key management.

7. **Key Generation in the Cloud:** This approach has already been used with great success in existing key management technologies. Systems that use Identity-Based Encryption (IBE), for example, already use more general key identifiers. In these systems, the identity of a user plus other policy information functions as the key identifier. In the case of using IBE to encrypt an email message, such an identifier might look like this:

Email = euser@test.com
Time=2014-02-23T08:00+05:30//+01:00
serverURL=https://data.example.com/

Which indicates the email address of the recipient of the encrypted message, the time after which the private key can be downloaded from the key server and the URL where the recipient can get the private key that he needs to decrypt the message? Any recipient that can interpret this type of key identifier can then contact the key server and request the IBE key needed to decrypt this message. This approach hasn't quite made it to other encryption technologies yet, although it probably will soon. The most recent draft of the IEEE P1619.3 *Standard for Key Management Infrastructure for Cryptographic Protection of Stored Data* uses this approach to define unique identifiers for keys from which it's easy to find the URL of the key server where the key can be obtained. Once that standard is implemented, key management for encrypting backup tapes will certainly get much easier. Once this idea is extended to other technologies, we'll have the fully federated key management that we need to protect sensitive data in the cloud. This sounds simple enough, but actually writing a standard that will be the basis for doing this in an interoperable way isn't easy. Using technologies like IBE may be as close as we can come to fully federated key management until the necessary standards are completed.

8. **Conclusions:** The quick development of cloud computing bring some security problems as well as many benefits to Internet users. Current solutions have some disadvantages in key management and authentication especially in a hybrid cloud with several public/private clouds. In this paper, we depicted the principles of identity-based cryptography and hierarchical identity-based cryptography and find the properties of HIBC fit well with the security demands of cloud. We proposed to use federated identity management and HIBC in the cloud and depicted how can the system generate and distribute the public and private keys to users and servers. Compared with the current Ws-Security approach, we can see our approach has its advantages in simplifying public key distribution and reducing SOAP header size. Also we showed how the users and servers in the cloud can generate secret session key without message exchange and authenticate each other with a simple way using identity-based cryptography.

References:

[1] Csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v25.ppt
[2] (http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc)
[3] Information Technology for Management: By BEHL
[4] http://en.wikipedia.org/wiki/Cloud_computing#cite_note-61

[5] Chappell, D.: A Short Introduction to Cloud Platforms, http://www.davidchappell.com/CloudPlatforms–Chappell.pdf