ID: IPHV1I20007X

International Journal Of Advanced Research and Innovations Vol.1, Issue .2

ISSN Online: *2319 – 9253*

Print: *2319 – 9245*

Enhanced Data Security and Access Control Approaches in Cloud Environment

Suresh B [1] **Sangeetha Guptha**[2]

1. **[M.Tech] , B.V.Raju Institute of Technology**
2. **Asst.Prof. , B.V.Raju Institute of Technology**

ABSTRACT

Cloud Computing is an environment has already proven in the market of data and services domains. Most of the industries are outsource their local data to remote cloud servers. Cloud Computing is recognized as future IT infrastructure provides elastic unlimited real world storage. In this paper we mainly shows my attention on security in cloud systems with well proven methods and focused on enhanced systems with proposed schemes. We shown the architectural methods(proxy encryption, re-encryption) to improve the security in cloud should definitely useful to the society of cloud and the people who utilize the cloud already….

Key words: cloud security, attributes , encryption, scalable methods, re-encryption

I. INTRODUCTION

Data to be secure in the cloud? Then consider encrypting the stored data. And don't store your encryption keys on the same server! It is unclear whether a cloud computing provider could be *compelled* by law enforcement agencies to decrypt data that

(1) it has encrypted or that

(2) users have encrypted, but if the provider has the keys, decryption is at least possible

Most cloud computing providers (1) *authenticate* (e.g. transfer usernames and password) via secure connections and (2) *transfer* (e.g. via HTTPS) data securely to/from their servers (so-called "data on the wire"), but, as far as I can tell, none (3) *encrypts stored data* (so-called "data at rest") automatically

II. DATA ENCRYPTION FOR THE CLOUD

The CipherCloud Gateway incorporates a number of military-grade, AES-based format and operations preserving encryption schemes that can be used to secure cloud-bound data before it leaves the enterprise network, without impacting the usability or functionality of cloud applications.

Organizations are able to reap all the benefits of migrating to the cloud without having to manage the overhead of storing sensitive data in local databases. Furthermore, the ability to select from various encryption schemes on a field-by-field basis provides customers the granularity needed to comply with their organizational data classification and regulatory requirements.

CipherCloud has implemented strong software-based cryptographic key management based on the NIST SP 800-21 standard that includes key rotation, split custodians, key encrypting keys and many other capabilities. Additionally, customers have the option to integrate with FIPS 140-2 compliant network attached Hardware Security Modules (HSM). Since the encryption keys are stored locally in CipherCloud and managed by customers themselves, the risk of an external party gaining unauthorized access to data is completely eliminated.

Identifying cloud encryption use cases and architectures

Cloud encryption can be complicated, but when implemented properly, it has advantages

International Journal Of Advanced Research and Innovations Vol.1, Issue .2

ISSN Online: 2319 – 9253

Print: 2319 – 9245

– both in private and public clouds -- by allowing enterprises to protect data that in a shared repository containing data with different levels of sensitivity.

In this tip, security professionals will learn three main use cases for cloud encryption and how the three major components for encryption -- the data, the encryption engine and the key management -- are handled in common cloud computing architectures.

Ensuring data security in the cloud with cloudEncryption

Every data protection strategy should consider both data in transit as well as data at rest. And, unfortunately, while most cloud service providers support encryption for data in transit, few offer support for data at rest. Consequently, in order to ensure data security in a cloud computing environment, organizations need to understand cloud encryption alternatives.

III. RELATED STUDY

The Infrastructure as a Service cloud computing has emerged as a viable alternative to the acquisition and management of physical resources. With IaaS, users can lease storage and computation time from large datacenters. Leasing of computation time is accomplished by has complete control over the configuration of the VMs using on-demand deployments, IaaS leasing is equivalent to purchasing dedicated hardware but without the long-term commitment and cost. The on-demand nature of IaaS is critical to making such leases attractive, since it enables users to expand or shrink their resources according to their computational needs, by using external resources to complement their local resource base.

This problem is particularly acute for VM images used in scientific computing where image sizes are large. A typical deployment consists of hundreds or even thousands of such images. Conventional deployment techniques broadcast the images to the nodes before starting the VM instances, a process that can take tens of minutes to hours, not counting the time to boot the operating system itself.

The huge computational potential offered by large distributed systems is hindered by poor data sharing scalability.

We addressed several major requirements related to these challenges. One such requirement is the need to efficiently cope with massive unstructured data (organized as huge sequences of bytes - BLOBs that can grow to TB) in very large-scale distributed systems while maintaining a very high data throughput for highly concurrent, fine-grain data accesses.

The role of virtualization in Clouds is also emphasized by identifying it as a key component. Moreover, Clouds have been defined just as virtualized hardware and software plus the previous monitoring and provisioning technologies.

Cloud Computing is a “buzz word” around a wide variety of aspects such as deployment, load balancing, provisioning, and data and processing outsourcing.

DISADVANTAGE

To give an less performance and storage space. Network traffic consumption also very high due to non concentrating on application status.

It is not possible to build a scalable, high-performance distributed data-storage service that facilitates data sharing at large scale.

IV. EXISTING APPROACH

Our existing solution applies cryptographic methods by disclosing data decryption keys only to authorized users. These solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine grained data access control is desired, and thus do not scale well.

International Journal Of Advanced Research and Innovations Vol.1, Issue .2

ISSN Online: 2319 – 9253

Print: 2319 – 9245

Data security in the cloud:

Weighing SaaS encryption options For some enterprises, embracing cloud services can be scary. Relinquishing control and having to rely on security providers isn't easy, and that especially holds true with Software as a Service (SaaS), which offers the least amount of control.

Considering this, companies should always work with cloud computing providers they trust for SaaS security, but there are also several SaaS encryption techniques companies can use for protecting sensitive data stored in a SaaS application. Here, gain a better understanding of SaaS security as well as SaaS encryption options.

Cloud computing encryption and Infrastructure as a Service

There are many obvious security reasons to encrypt data, but when you are dealing with a cloud computing provider, some of the reasons for implementing encryption maybe not be as obvious.

Cloud computing and data protection: Using DLP tools in the cloud

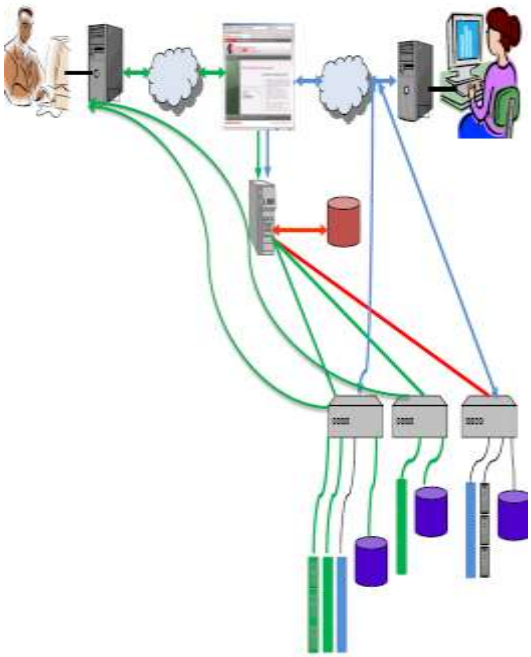
Making a move into the cloud can raise many enterprise security concerns, especially concerning data protection. Consequently, a thorough examination into and understanding of cloud computing and data protection options is essential for every enterprise. Data loss prevention (DLP) tools can help control migration of data to the cloud and also find sensitive data leaked to the cloud.

Cloud computing data security: Managing unauthorized use of cloud computing While you may think you are aware of any enterprise cloud computing activity, such as deployment of data or applications to the cloud, that is not always the case. Developers or sales executives may be moving data to the cloud without your knowledge.

V. PROPOSED APPROACHES

In order to achieve secure, scalable and fine-grained access control on outsourced data in the cloud, we utilize and uniquely combine the following three advanced cryptographic techniques:

- Key Policy Attribute-Based Encryption (KP-ABE).
- Proxy Re-Encryption (PRE)
- Lazy re-encryption



1) Key Policy Attribute-Based Encryption (KP-ABE):

KP-ABE is a public key cryptography primitive for one-to-many communications. In KP-ABE, data are associated with attributes for each of which a public key component is defined. User secret key is defined to reflect the access structure so that the user is able to decrypt a cipher text if

International Journal Of Advanced Research and Innovations Vol.1, Issue .2

ISSN Online: 2319 – 9253

Print: 2319 – 9245

and only if the data attributes satisfy his access structure. A KP-ABE scheme is composed of four algorithms which can be defined as follows:

- Setup Attributes
- Encryption
- Secret key generation
- Decryption

Setup Attributes:

This algorithm is used to set attributes for users. From these attributes public key and master key for each user can be determined. The attributes, public key and master key are denoted as

Attributes- $U = \{1, 2. . . N\}$

Public key- $PK = (Y, T1, T2, ... , TN)$

Master key- $MK = (y, t1, t2, ... , tN)$

Encryption:

This algorithm takes a message *M*, the public key *PK*, and a set of attributes *I* as input. It outputs the cipher text *E* with the following format:

$$E = (I, \tilde{} E, \{Ei\}i)$$

where $\tilde{}E = MY$, $Ei = Ti$.

Secret key generation:

This algorithm takes as input an access tree *T*, the master key *MK*, and the public key *PK*. It outputs a user secret key *SK* as follows.

$$SK = \{ski\}$$

Decryption:

This algorithm takes as input the cipher text ***E*** encrypted under the attribute set **U**, the user's secret key ***SK*** for access tree ***T***, and the public key ***PK***.

Finally it output the message ***M*** if and only if **U satisfies T**.

2) Proxy Re-Encryption (PRE):

Proxy Re-Encryption (PRE) is a cryptographic primitive in which a semi-trusted proxy is able to convert a cipher text encrypted under Alice's public key into another cipher text that can be opened by Bob's private key without seeing the underlying plaintext. A PRE scheme allows the proxy, given the proxy re-encryption key

$$rka \leftrightarrow b,$$

to translate cipher texts under public key ***pk1*** into cipher texts under public key ***pk2*** and vise versa.

3) Lazy re-encryption:

The lazy re-encryption technique and allow Cloud Servers to aggregate computation tasks of multiple operations. The operations such as

- Update secret keys
- Update user attributes.

CONCLUSITION

Finally we conclude that the enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine grained data access control to untrusted cloud servers without disclosing the underlying data contents.

Our proposed scheme enables the data owner to delegate tasks of data file re-encryption and user secret key update to cloud servers without disclosing data contents or user access privilege information. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

In my future will focuses on trust worthy system with cloud environment, will use this work as resources to my future enhancements.

International Journal Of Advanced Research and Innovations Vol.1, Issue .2

ISSN Online: 2319 – 9253

Print: 2319 – 9245

REFERENCES

[1] Amazon Web Services (AWS), Online at http://aws. amazon.com.

[2] Google App Engine, Online at http://code.google.com/appengine/.

[3] Microsoft Azure, http://www.microsoft.com/azure/.

[4] 104th United States Congress, "Health Insurance Portability and AccountabilityAct of 1996 (HIPPA)," Online http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996.

[5] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy insecure groups," in *Proc. of NDSS'01*, 2001.

[6] P. D. McDaniel and A. Prakash, "Methods and limitations of securitypolicy reconciliation," in *Proc. of SP'02*, 2002.

[7] T. Yu and M. Winslett, "A unified scheme for resource protection inautomated trust negotiation," in *Proc. of SP'03*, 2003.

[8] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in *Proc. of CCS'05*, 2005.

[9] J. Anderson, "Computer Security Technology Planning Study," Air Force Electronic Systems Division, Report ESD-TR-73-51, 1972, http://seclab.cs.ucdavis.edu/projects/history/.

[10] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu,"Scalable secure file sharing on untrusted storage," in *Proc. of FAST'03*,2003.

[11] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securingremote untrusted storage," in *Proc. of NDSS'03*, 2003.

[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxyre-encryption schemes with applications to secure distributed storage,"in *Proc. of NDSS'05*, 2005.

[13] 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. of VLDB'07*, 2007.

[14] Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryptionfor fine-grained access control of encrypted data," in *Proc. ofCCS'06*, 2006.

Author's profile

SURESH B
[M.TECH] ,
B.V.Raju Institute of Technology

Sangeeta Gupta
M.Tech in CSE
Asst.Professor
B.V.Raju Institute of Technolgy