IJCAT International Journal of Computing and Technology, Volume 1, Issue 4, May 2014
ISSN : 2348 - 6090
www.IJCAT.org

Reliability of Cloud Using Encryption Techniques: A Review

[1] N.S. Shambharkar, [2] Milind Tote

[1] Department of CSE,Nuva College of Engg.Nagpur University,Nagpur.
Nagpur,India

[2] Department of CSE, GNIET, Nagpur University,Nagpur.
Nagpur,India

Abstract- A key approach to secure cloud computing is for the information owner to store encrypted data within the cloud, and issue decipherment keys to authorized users. Then, only one time a user is revoked, the information owner can issue re-encryption commands to the cloud to re-encrypt the information, to prevent the revoked user from decrypting the information, and to get new decryption keys to valid users, so they'll still access the information. However, since a cloud computing environment is comprised of the many cloud servers, such commands may not be received and executed by all of the cloud servers due to unreliable network communications .Here, we have a tendency to solve this drawback by proposing a time based re-encryption theme, that allows the cloud servers to mechanically re-encrypt information supported their internal clocks. Our answer is made on high of a replacement encoding theme, attribute based encoding, to permit fine-grain access management, and doesn't need excellent clock synchronization for correctness.

Keywords- **Cloud, Encryption**

1. Introduction

The use of cloud computing is increasingly widespread as a result of the potential price savings from outsourcing information to the cloud service provider (CSP). One technique to guard information the into the information from a attainable un trusted CSP is for the information owner to encrypt the outsourced data. Flexible encoding schemes like attribute based mostly encoding (ABE) is adopted to supply fine grained access management. ABE permits information to be encrypted exploitation AN access structure comprised of various attributes. Rather than specific decryption keys for specific files, users area unit issued attribute keys. Users should have the necessary attributes that satisfy the access structure so as to decipher a file. for instance, a file encrypted victimisation the access structure implies that either a user with attributes α1 and α2, or a user with attribute α3, will decipher the file.

However, command-driven re-encryption schemes don't take into account the underlying system design of the cloud environment. A cloud is actually a large scale distributed system where {a information a knowledge an information} owner's data is replicated over multiple servers for top availableness. As a distributed system, the cloud can expertise failures common to such systems, like server crashes and network outages. As a result, re-encryption commands sent by the information owner might not propagate to any or all of the servers during a timely fashion, therefore making security risks.

A better answer is to permit every cloud server to independently re-encrypt information while not receiving any command from the information owner. In this paper, we tend to propose a reliable re-encryption theme in unreliable clouds (R3 theme for short). R3 may be a time-based re-encryption theme, that permits every cloud server to automatically re-encrypt information supported its internal clock. the basic plan of the R3 theme is to associate the information with AN access management and an interval. every user is issued keys related to attributes and attribute effective times. the information is decrypted by the users control the keys with attributes satisfying the access control, and attribute effective times satisfying the access time.

2. Literature Survey

We have to analysis the information and data Engineering: Data & information Engineering (DKE) may be a journal in information systems and knowledgebase systems. it's revealed by Elsevier. it had been supported in 1985, and is command in over 250 tutorial libraries. The editor-in-chief is P.P. Chen (Dept. of engineering, American state State University, USA) This explicit journal publishes twelve problems a year. All articles from the information & information Engineering journal is viewed on categorization services like Scopus and Science Citation Index.Knowledge engineering (KE) was outlined in 1983

by Edward Feigenbaum, and Pamela McCorduck as follows: KE is an engineering discipline that involves group action information into laptop systems so as to unravel advanced issues usually requiring a high level of human experience. At present, it refers to the building, maintaining and development of knowledge-based systems. it's a great deal in common with software engineering, and is employed in several engineering domains like computing, including databases, data mining, knowledgeable systems, call support systems and geographic info systems. information engineering is additionally associated with mathematical logic, similarly as powerfully concerned in science and socio-cognitive engineering wherever the information is made by socio-cognitive aggregates (mainly humans) and is structured in line with our understanding of however human reasoning and logic works.

Various activities of KE specific for the development of a knowledge-based system:

- Assessment of the problem
- Development of a knowledge-based system shell/structure
- Acquisition and structuring of the related information, knowledge and specific preferences (IPK model)
- Implementation of the structured knowledge into knowledge bases
- Testing and validation of the inserted knowledge
- Integration and maintenance of the system
- Revision and evaluation of the system.
-

Knowledge engineering principles
Since the mid-1980s, knowledge engineers have developed a number of principles, methods and tools to improve the knowledge acquisition and ordering. Some of the key principles are:

- There are different:
    - Types of knowledge each requiring its own approach and technique.
    - Types of experts and expertise, such that methods should be chosen appropriately.
    - Ways of representing knowledge, which can aid the acquisition, validation and re-use of knowledge.
    - Ways of using knowledge, so that the acquisition process can be guided by the project aims (goal-oriented).
- Structured methods increase the efficiency of the acquisition process.
- Knowledge Engineering is the process of eliciting Knowledge for any purpose be it Expert system or AI development

Introduction to information Mining: data mining (also called Knowledge Discovery in Databases - KDD) has been outlined as "The nontrivial extraction of implicit, antecedently unknown, and probably helpful info from data" It uses machine learning, applied mathematics and visualization techniques to get and gift information in a kind that is well comprehensible to humans.

3. Proposed System

We propose a reliable re-encryption theme in unreliable clouds (R3 theme for short). R3 may be a time-based re-encryption theme, that permits every cloud server to mechanically re-encrypt information supported its internal clock. the fundamental plan of the R3 theme is to associate the information with an access management And an interval. Every user is issued keys related to attributes and attribute effective times. The information is decrypted by the users victimization the keys with attributes satisfying the access management, and attribute effective times satisfying the interval. Not like the command-driven re-encryption theme, the information owner and also the CSP share a secret key, with that every cloud server will encrypt information by change the information interval in line with its own internal clock. Even through the R3 theme depends on time, it doesn't need excellent clock synchronization among cloud servers. Classical clock synchronization techniques that guarantee loose clock synchronic within the cloud area unit spare.

The most contributions area unit as follows:

1) We propose an automatic, time-based, proxy re encryption theme appropriate for cloud environments with unpredictable server crashes and network outages.

2) We extend an ABE theme by incorporating timestamps to perform proxy re-encryption.

3) Our answer doesn't need excellent clock synchronization among all of the cloud servers to take care of correctness.

4. Conclusion

We planned the R3 theme, a brand new technique for managing access management supported the cloud server's internal clock. Our technique doesn\'t accept the cloud to faithfully propagate re-encryption commands to all or any servers to confirm access management correctness. we tend to showed that our solutions stay secure while not good clock synchronization ciao as we will sure the time distinction between the servers and also the knowledge owner.

References

[1] S. Kamara and K. Lauter, "Cryptographic cloud storage," monetary Cryptography and knowledge Security, 2010.

[2] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "A read of cloud computing," Communications of the ACM, 2010.

[3] A. Sahai and B. Waters, "Fuzzy identity-based coding," Advances in Cryptology–EUROCRYPT, 2005.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based coding for fine-grained access management of encrypted knowledge," in Proc. of ACM CCS, 2006.

.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased coding," in Proc. of IEEE conference on S&P, 2007.

[6] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," Advances in Cryptology–EUROCRYPT, 1998.

[7] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based coding with economical revocation," in Proc. of ACM CCS, 2008.

[8] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based coding for fine-grained access management in cloud storage services," in Proc. Of ACM CCS (Poster), 2010.