INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 1)
Available online at: www.ijariit.com

Authorization for secured cloud storage through SHA-256

M. R. Sundarakumar
sundar.infotech@gmail.com
AMC Engineering College, Bengaluru, Karnataka

Dr. G. Mahadevan
g_mahadevan@yahoo.com
AMC Engineering College, Bengaluru, Karnataka

ABSTRACT

Cloud computing has become one of the most influential paradigms in the IT industry in recent years. This emerging computing technology demands the user to believe their data is secure to cloud providers, there have been increasing security and privacy concerns on outsourced data. Many Schemes emphasis on Attribute-Based Encryption (ABE) have been made for access control of user's data in cloud computing; however, they lack from some major security issues. In order to realize flexible, reliable, and fine grained access control of available data in cloud computing, A Secured Hashing Algorithm is proposed which is a one-way cryptography technique with no decryption. This online storage mechanism is an integrated cloud backup suite that gives end-to-end visibility and full control of your data storage resources at corresponding rates. Cloud offers high scalability for all your storage needs your scalable data demands met from highly scalable archival to storage, equip your enterprises with the comprehensive storage suites needs. Cloud storage allows you to store unlimited data in an always available, highly durable and fully secure environment with Enterprises-Grade System Management for your commercial and budgetary needs. The key benefits are scalability, durability, support and predictable pricing. The proposed scheme not only achieves security due to its Secured Hashing Algorithm (SHA) but also inherits scalability and efficient access control in supporting compound attributes of ASBE (Attribute Set Based Encryption).

Keywords— *Access control, Cloud computing, Data security, Secured Hashing Algorithm*

1. INTRODUCTION

Cloud computing holds the promise of providing computing as the fifth utility after the other four utilities (water, gas, electricity, and telephone). The key benefits of cloud computing include increased operational efficiencies, scalability, reduced costs and capital expenditures, immediate time to market, flexibility and so on. Many cloud computing models offering different services have been proposed which includes Infrastructure As A Service (IAAS), Platform As A Service (PAAS), and Software As A Service (SAAS).

One of the most prominent security concerns is data privacy and security in cloud computing due to its distributed online storage and access scheme. People using cloud want to ensure that their data in the cloud remains secure and confidential to outside users, which emerges as the top priority requirement. However, Data security is not the only security requirement, Access policy and flexible access control are also strongly required in the service-oriented cloud computing model. A trending access control scheme emphasis in attributed-based encryption is put forwarded by yu*et al.* which adapted to the key-policy of attribute-based encryption (kp-abe) to enforce fine-grained and secured access control. However, his proposal falls short of flexibility issues in attribute management and lacks scalability when considering dealing with multiple attributes. In this paper, we propose a new kind of hashing based encryption scheme for effective access control in cloud computing. It also uses the cypher-text policy attribute-set-based encryption in an efficient way with a hierarchical structure of system users, this hashing based encryption scheme helps to achieve a flexible and fine-grained access control with better scalability. The online storage in the cloud is an integrated cloud backup suite that provides complete control and visibility of your data storage resources. It offers a large scale storage platform for all your needs. Your scalable data demands met from highly scalable archival to store, equip your enterprises with the comprehensive storage suites needs. Cloud storage allows you to store massive data that is of high availability of data in a completely protected environment with enterprise-grade system management for your budgetary needs. The key advantages of cloud storage are scalability, durability, support, predictable pricing.

2. LITERATURE REVIEW

2.1 Existing System

Cloud storage enables distributed online storage where user's data is stored on different virtual servers, generally maintained by third parties, rather than storing on a single server. With a distributed storage, there arise security problems. So, In order to enforce security among data in the cloud, this proposed scheme consists of efficient methods that ensure on-demand data authentication and verification. Cloud System has the computation assigned in a great number of distributed computers, rather than a local computer or remote server. Though cloud services are entirely based on distributed computing, there are both internal and external security threats for data integrity still exist. Thus, the distributed scheme for storage correctness assurance will be of most importance in achieving robust and reliable cloud storage systems.

2.2 Limitations of the Existing System

- Aimed at data storage rather than data security.
- No effective data encryption algorithms that solve all demands
- No error correction algorithms are implemented in the existing system.

2.3 Proposed system

Here Secured Hash Algorithm (SHA-256) based encryption technique for access control in cloud computing is proposed. SHA-256redefines the cipher text-policy with a well-defined structure of system users, in order to obtain a flexible and secure access control. In this process, the text is encrypted with the access policy selected by an encryptor, while the corresponding decryption key is created with respect to a set of attributes. The attributes associated with the decrypting key satisfies the access policy associated with a given encrypted text, the key can be used to decrypt the text. With this SHA we have achieved a fine-grained access control and secured accessing of data in the cloud in a well-formed manner.

3. METHODOLOGY

3.1 Architecture of proposed system

The cloud computing system under consideration consists of five types of parties: a cloud service provider, data owners, data consumers, a number of domain authorities, and trusted authority. The cloud service provider manages a cloud to provide data storage service. Data holder always try to encrypt their data and store it in the cloud. To access them, they download the encrypted files and decrypt with their own private key and use them. Each data owner or consumer is administrated by specific domain authority. Domain authority is maintained and managed by another trusted authority. They are organized in a hierarchical manner. The most trusted authority is the head of all authorities and responsible for leading most of the domain authorities. Top level authorities correspond to major organizations such as a federated enterprise, while lower-level domain authority corresponds to middle and low-level organizations such as an affiliated company in an enterprise. Data owners/consumers may correspond to employees in an organization. Each domain authority has the responsibility to manage and maintain the next level or the data owners/consumers in its own domain. In my system, neither data owners nor the data consumer needs to be always online. They come online only when necessary. On the other hand, the cloud service providers, the trusted authorities, and the domain authorities are always online. The cloud has abundant massive storage and very large computational power. In addition, we assume that data consumers can access data files for reading only.

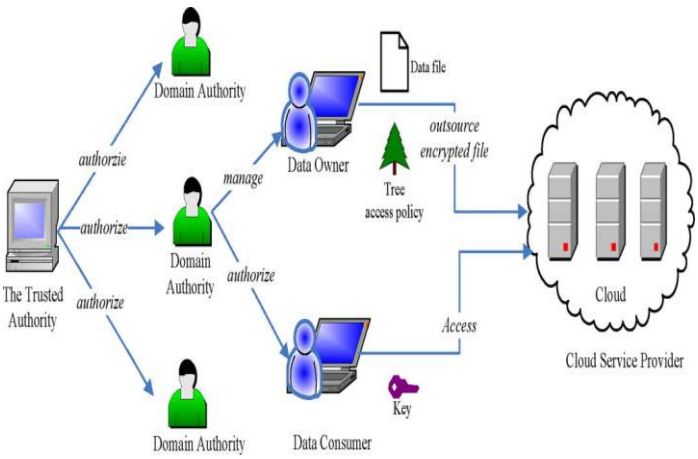


Fig. 1: Proposed system architecture

3.2 SHA-256Hash Technique

The proposed SHA-256 scheme seamlessly extends the ASBE scheme to handle the hierarchical structure of system users. Each user in the system is assigned a key structure which specifies the hashed value that cannot be decrypted. To achieve a scalable and well secured, flexible access control in cloud computing by using Secured Hashing Algorithm(SHA-256), we compare this proposed scheme with the one proposed by Yu *et al* on real-time security features in implementing access control for cloud computing.

3.3 Scalability

Cloud storage is a backup suite that provides storage, end-to-end visibility and complete control of your data storage resources. We extend ASBE with a hash structure to effectively improve the high-level authorities private key generation operation to lower-level domain authorities. By this practice, trusted authorities will find a reduced workload than low-level authorities, which can provide secured and fast flow of data for end users. Thus, this hierarchical structure achieves great scalability. Yu *et al.*'s scheme have only one authority to deal with key generation, which is not at all scalable for large-scale high-level cloud computing applications.

3.4 Flexibility

Compared with Yu *et al.*'s scheme, SHAeffectively organizes user attributes into a recursive structure which allows the user to emphasis dynamic constraints on to combine these attributes to satisfy a constrain policy. So SHA can support compound attributes as well as multiple numerical Assignments for a given attribute conveniently and effectively.

3.5 Fine-grained access control

Based on SHA, our scheme can easily achieve a well fine-grained access control with no latency. A data owner can define and enforce any kind of expressive and flexible access constrain policy for the data files

4. MODULES

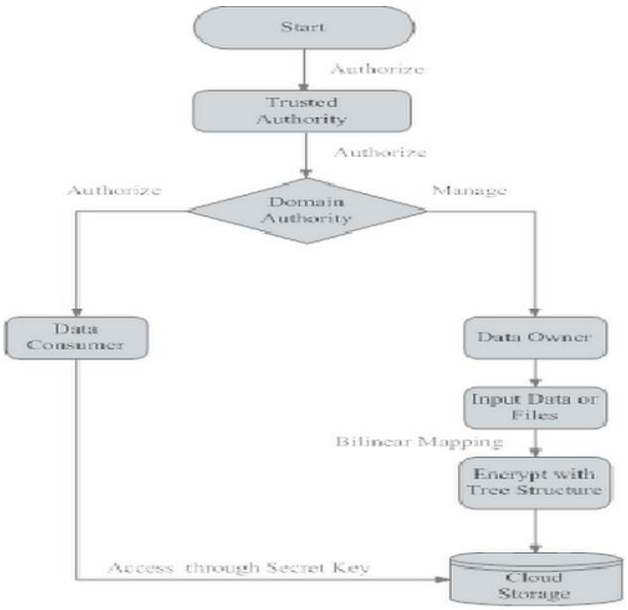


Fig. 2: Modules

4.1 Root and Domain Authority

The topmost prioritized authority for security is the root and domain authority. They administrate the domain authority. Domain authorities lay below the root authority and are responsible for managing its child authorities

4.2 Bilinear Mapping

Attribute-Based Encryption (ABE) is preceded by bilinear mapping technique of the specific attribute information of data owner and the data to be stored in the cloud. It can be achieved by multiplicative factors of both logical AND and XOR operations.

4.3 Master and secret key

The master key is generated by doing the logical AND operation and given attributes of the data owner. Using the master key public key is generated and the secret key is generated by logical XOR operation. The secured secret key is generated by ABE.

4.4 Secure cloud storage

The security is applied in the data owner's file and those files are stored in the cloud servers. For this crypto process, algorithms such as blowfish algorithm are used for both encryption and decryption.

4.5 Secure Data Retrieval

The data to be retrieved very secure and decryption is performed using a secret key.

5. PERFORMANCE ANALYSIS

First, analyze the theoretic computation complexity of the proposed scheme in each operation. We analyze the computation complexity for each system operation in our scheme as follows.

5.1 System setup

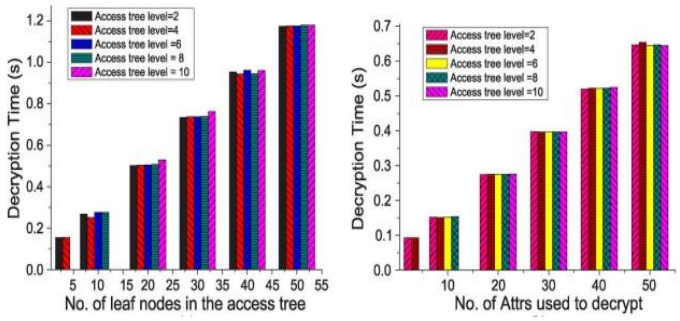
During the system setup, the top level trusted authority selects a bilinear group and some random numbers. When PK and MK_0 are generated, there exist several exponentiation operations. So the computation complexity of System Setup is O (1).

5.2 Top-Level Domain Authority Grant

This operation is performed by the trusted authority. The master key of domain authority is in the form of, MK_0=(A, D, $D_{i,j}$, $D'_{i,j}$for $a_{i,j}\epsilon$ A, $E_i$for AϵA_i), where A is the key structure associated with new domain authority, A is the set of A_i. Let N be the number of attributes in A, and M be the number of sets in A. The computation complexity of Top-Level Domain Authority Grant operation is O(2N + M).

5.3 New User/Domain Authority Grant

In this operation, a new user or new domain authority is associated with an attribute set, which is the set of that of the upper-level domain authority. The computation complexity is O(2N + M).



5.4 New File Creation

In this operation, Symmetric key is used by the data owner to encrypt the data file and then encrypt DEK using SHA. The complexity in this encryption technique with DEK depends on the volume of the data file and the usage of the encryption algorithm. Encrypting DEK in a hierarchical access structure consists of exponentiations per leaf node and one exponentiation per translating node. So the computation complexity of New File Creation is O(2|Y| + |X|), where Y denotes the leaf nodes of T and X denotes the translating nodes of T.

5.5 File Access

In this operation, we discuss the decrypting operation of encrypted data files. A user first obtains DEKS with the Decrypt algorithm and then decrypt data files using DEK_S. We will discuss the computation complexity of the Decrypt algorithm. Depending on the key and the way of the algorithm used for decryption, the cost for decrypting the key differs accordingly. Even for a given key, the way to satisfy the associated access tree may be various.

5.6 File Deletion

Deletion operations are done at the demand of a data owner to delete the data. If the cloud verifies the requestor as the legal owner of the file, the file is deleted from could immediately. So the computation complexity is O(1).

6. CONCLUSION AND FUTURE WORK

We introduced the SHA-256 scheme for fine-grained access control in cloud computing and to ensure scalability and flexibility in it. The SHA scheme seamlessly enforces a secured structure of system users by applying a delegation algorithm which redefines the methodologies ASBE. Finally, I implemented the proposed scheme and performed comprehensive performance analysis and evaluation, which showed its advantages and efficiency over existing schemes.

Usage of High-security cryptographic algorithms

Using Secured Hashing Algorithm, which is 256 bits key length results in higher security, rather than using traditional DES and AES algorithms are smaller in key sizes results in lesser security.

Reducing Storage Overhead

By means of the de-duplication concept, we can reduce the storage overhead problem that reduces the problem of redundant data of multiple users being stored in cloud storage.

7. REFERENCES

[1] Automated trust negotiation using cryptographic credentials, J. Li, N. Li, and W. H. Winsborough, in Proc. ACM Conf. Computer and Communications Security (CCS), Alexandria, VA, 2005.

[2] Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility, R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, Future Generation Computer. Syst., vol. 25, pp.599–616, 2009.

[3] HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing, Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, Ieee Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012.

[4] Like technology from an advanced alien culture: Google apps for education at ASU, K. Barlow and J. Lane, in Proc. ACM SIGUCCS User Services Conf., Orlando, FL, 2007.

[5] Salesforce.com: Raising the level of networking, Barbara, Inf. Today, vol. 27, pp. 45–45, 2010.

