International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Key-Aggregate Based Vulnerable Data Access Control in Cloud Computing

Sowmiya. S
PG Student, Department of CSE, Mailam Engineering College, Mailam, Tamil Nadu, India

Dr. T. Priyaradhikadevi
Head, Department of CSE, Mailam Engineering College, Mailam, Tamil Nadu, India

ABSTRACT

In the developing technologies in the computers the cloud computing is one the way to provide services through the internet to the users in the efficient manner. Cloud based services not only provide users with convenience, but also bring many security issues. The user can store his data in the cloud service. Although cloud computing brings great convenience to enterprises and users, the cloud computing security has always been a major hazard. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy. The system proposed a fine-grained two-factor authentication (2FA) access control system, 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both user secret key and a BBS+ Signatures. The mechanism implemented using CP-IBE(cipher text identity based encryption) and digit signature authority, compare to existing method which provide the paranoid security and achieving the secure data access in cloud computing.

Keywords: *access control; data sharing; privacy protection; cloud-based services*

I. INTRODUCTION

Data mining (the analysis step of the "Knowledge Discovery in Databases" process, or KDD), an interdisciplinary subfield of computer science is the computational process of discovering patterns in large data sets ("BIG DATA") involving methods at the intersection of artificial intelligence, machine learning, statistics, and database systems. The overall goal of the data mining process is to extract information from a data set and transform it into an understandable structure for further use.

The actual data mining task is the automatic or semi-automatic analysis of large quantities of data to extract previously unknown, interesting patterns such as groups of data records (cluster analysis), unusual records (anomaly detection), and dependencies (association rule mining).Data mining is a knowledge discovery technique to analyze data and encapsulate it into useful information.

In the developing technologies in the computers the cloud computing is one the way to provide services through the internet to the users in the efficient manner. Cloud based services not only provide users with convenience, but also bring many security issues**.** The user can store his data in the cloud service. Although cloud computing brings great convenience to enterprises and users, the cloud computing security has always been a major hazard. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy.

II. LITERATURE SURVEY

H.Shacham[1] This paper presents SiRiUS, a secure file system designed to be layered over insecure network and P2P file systems such as NFS, CIFS, Ocean Store, and Yahoo! Briefcase. SiRiUS assumes the network storage is untrusted and provides its own read-write cryptographic access control for file level sharing. Key management and revocation is simple

with minimal out-of-band communication. File system freshness guarantees are supported by SiRiUS using hash tree constructions. SiRiUS contains a novel method of performing file random access in a cryptographic file system without the use of a block server. Extensions to SiRiUS include large scale group sharing using the NNL key revocation construction. The implementation of SiRiUS performs well relative to the underlying file system despite using cryptographic operations.of adding access control to a secure file system. Performance measurements of our experimental file.

S.Hohenberger[2] Atomic proxy re-encryption, in which a semi-trusted proxy converts a cipher text for Alice into a cipher text for Bob without seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Present new re-encryption schemes that realize a stronger notion of security, and demonstrate the usefulness of proxy re-encryption as a method

V.Goyal[3] As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. One drawback of encrypting data, is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). It develops a new cryptosystem for fine-grained sharing of encrypted data that we call Key-Policy Attribute-Based Encryption (KP-ABE). The cryptosystem, cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt. It demonstrates the applicability of our construction to sharing of audit-log information and broadcast encryption.

Rui jiang [4] Cloud computing is an internet based computing which enables sharing of services. It is very challenging part to keep safely all required data that are needed in many applications for user in cloud. Storing our data in cloud may not be fully trustworthy. Since client doesn't have copy of all stored data, he has to depend on Cloud Service Provider. This work studies the problem of ensuring the integrity and security of data storage in Cloud Computing.This paper, proposes an effective and flexible Batch Audit scheme with dynamic data support to reduce the computation overheads. To ensure the correctness of users data the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the data stored in the cloud.We consider symmetric encryption for effective utilization of outsourced cloud data under the model, it achieve the storage security in multi cloud data storage. The new scheme further supports secure and efficient dynamic operations on data blocks, including data insertion, update, delete and replacement.

III. PROPOSED SYSTEM

The systemproposed a fine-grained two-factor authentication (2FA) access control system, 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both user secret key and a BBS+ Signatures.

The mechanism implemented using CP-IBE(cipher Text Identity Based Encryption) and digit signature authority, where a user cannot access the system if s/he does not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for cloud service.

Cryptography methods improving the privacy of the users, an authority of the users provide using the BBS+ signatures.

Cloud based services not only provide users with convenience, but also bring many security issues**.** The user can store his data in the cloud service. Although cloud computing brings great convenience to enterprises and users, the cloud computing security has always been a major hazard. For users, it is necessary to take full advantage of cloud storage service, and also to ensure data privacy.

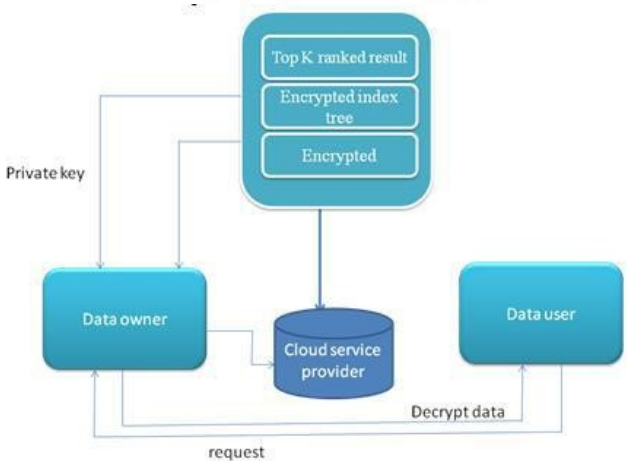

Fig. 1: Overall Architecture

A. GROUP COMMITTEE

Admin login the group and get the details of user and view the files. Select a user from cloud server and give request to the user to login into a group. A data distributor has given sensitive data to a set of supposedly trusted user.

B. SERVICE PROVIDER

The Cloud Service Selection Verification acts like a certificate authority .The service provider is associated with a pair of public and private keys, and its public key is made available to CSPs, cloud brokers and cloud clients .Each cloud broker handles a potentially large amount of online client's requests. For a service selection request from a client, the cloud broker will query the authenticated CSP profile database provided by the collector and recommend CSPs to the clients.

C. THIRD PARTY VERIFIER

Fake objects are objects generated by the distributor in order to increase the chances of detecting agents that leak data. The distributor may be able to add fake objects to the distributed data in order to improve his effectiveness in detecting guilty agents. Our use of fake objects is inspired by the use of "trace" records in mailing lists.

D. A third party verifier cannot get Any information about the client's data m from the protocol execution. Hence, the protocol is private against third party verifiers. If the server modifies any part of the client's data, the client should be able to detect it; furthermore, any third Party verifier should also be able to detect it. In case a third party verifier verifies the integrity of the client's data, the data should be kept private against the third party verifier.

E. COLLECTOR

The collector is responsible for collecting the files the properties and other information such as user ratings, etc of CSPs, and constructing an authenticated CSP profile data base that ensures the integrity of the CSPs' information. The collector sells the authenticated CSP profile database to multiple cloud brokers.

F. DATA CHUNK

Data chunk means after clients store their data at the remote server, they can dynamically update their data at later times. At the block level, the main operations are block insertion, block modification and block deletion.

G. PUBLIC VERIFIABILITY

Each and every time the secret key sent to the client's email and can perform the integrity checking operation.

In this definition, we have two entities:

Challenger: that stands for either the client or any third party verifier, **Adversary:** that stands for the un trusted server. Client doesn't ask any secret key from third party.

H. FINE GRAINED META DATA

Each of the Meta data from the data blocks mi is encrypted by using a suitable algorithm to give a new modified Meta data. The encryption method can be improvised to provide still stronger protection for Client's data. All the Meta data bit blocks that are generated using the procedure are to be concatenated together. This concatenated Meta data should be appended to the file F before storing it at the cloud server. The file F along with the appended Meta data is stored in the cloud. Let the verifier V wishes to the store the file F. Let this file F consist of n file blocks. We initially preprocess the file and create metadata to be appended to the file. Let each of the sn data blocks have m bits in them. A typical data file F which the client wishes to store in the cloud.

IV.SYSTEM IMPLEMENTATION

The system output is mainly based on privacy preserving method. It will be evaluated using attribute based encryption. Attribute-based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes .In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext.

V. CONCULSION

In this project, presented a new 2FA (including both user secret key and a lightweight security device) access control system for web-based cloud computing services. Based on the attribute-based access control mechanism, the proposed 2FA access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy. Detailed security analysis shows that the proposed 2FA access control system achieves the desired security for data sharing. Providing secure and efficient access to large scale outsourced data is an important component of

cloud computing. In this paper, I propose a mechanism to solve this problem in owner-write-users-read applications.

I have propose to encrypt every data block with a different key so that flexible cryptography-based access control can be achieved. Through the adoption of key derivation methods, the owner needs to maintain only a few secrets. Analysis shows that the key derivation procedure using hash functions will introduce very limited computation overhead. I propose to use over-encryption and/or lazy revocation to prevent revoked users from getting access to updated data blocks. An design mechanisms to handle both updates to outsourced data and changes in user access rights. I investigate the overhead and safety of the proposed approach, and study mechanisms to improve data access efficiency.

VI. REFERENCES

1) S. Yu, C. Wang, K. Ran, "Achieving secure, scalable, and fine-grained data access control in cloud computing," Proc. IEEE INFOCOM, pp.2010.
2) J. Bethe court, A. Shari, B. Waters, "Cipher text-policy attribute-based encryption," Proc. Security and Privacy, pp. 321-334, 2007.
3) J. Hurt, D.K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7 pp. 1214-1221, 2011.
4) A. Lawks, B. Waters, "Decentralizing attribute-Basedencryption,"Proc. Advances in Cryptology-EUROCRYPT, pp. 568-588, 2011.
5) M. Li, S. Yu, Y. Zhen, "Scalable and secure sharing of personal health records in cloud computing using attribute-Based Encrypt IEEE
6) Transactions on Parallel and Distributed System, vol. 24, no. 1, pp. 131-14
7) J. Li, K. Kim, "Hidden attribute-based signatures with révocation," Information Sciences, vol. 180, no. 9, pp. 1681-1689, 2010.
8) H.K. Magi, M. S. Yu, C. Wang, K. Reno, "Achieving secure, scalable, and fine-grained data access control in cloud computing," Proc. IEEEINFOCOsM,pp.1-9,2010.