ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Data Storage in Clouds by Using Decentralized Access Control

Ahmed Tameem Mohammed
Masters in Information System
Nizam College, Osmania University, T.S-500007, India.

Abstract

This survey proposes a brand new decentralized get admission to manage scheme for relaxed records garage in clouds which helps nameless authentication. The cloud verifies the authenticity of the collection without enormous expertise within the consumer's identification earlier than storing facts. This scheme additionally has the delivered function of get admission to manage. In get right of entry to manipulate scheme most effective legitimate customers are capable of decrypt the saved statistics/records. This scheme prevents replay assaults additionally helps introduction, change, and analyzing facts saved within the cloud. These schemes additionally cope with consumer revocation. Moreover, the authentication and get admission to manipulate scheme is decentralized and sturdy in nature in contrast todifferent get admission to manipulate schemes designed for clouds that are centralized. The computation, verbal exchange, and garage overheads are corresponding to centralized techniques.

1 Introduction

Research in cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet. This frees users from the hassles of maintaining resources on-site. Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures(e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g. Amazon's S3, Windows Azure).Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are, thus, very important issues in cloud computing[1]. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement[2].

Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents (as in Google Docs or Drop box) or even personal information (as in social networking)[3].

There are broadly three types of access control: user-based access control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC).
1. In UBAC, the access control list contains the list of users who are authorized to access data. This is not feasible in clouds where there are many users.
2. In RBAC (introduced by Ferraiolo and Kuhn [10]),

Cite this article as: Ahmed Tameem Mohammed, "Secure Data Storage in Clouds by Using Decentralized Access Control", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 5 Issue 11, 2018, Page 55-58.

users are classified based on their individual roles. Data can be accessed by users who have matching roles. The roles are defined by the system. For example, only faculty members and senior secretaries might have access to data but not the junior secretaries.
3. ABAC is more extended in scope, in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes, satisfying the access policy, can access the data.

2- Literature survey

Literature survey is the maximum critical step in software program improvement system. Before growing the device it's miles vital to decide the time component, economic system in employer electricity. Once this stuff is glad, then subsequent steps is to decide which working gadget and language may be used for growing the device. Once the programmers begin constructing the device the programmers want lot of outside guide. This help may be acquired from senior programmers, from e book or from web sites. Before constructing the machine the above attention are taken into consideration for growing the proposed gadget [4].

In 2006 A. Sahai and B. Waters, labored on “Fuzzy Identity-Based Encryption” In Identity Based Encryption scheme, A person has a fixed of attributes further to its specific ID. A Fuzzy IBE scheme may be implemented to permit encryption .In Fuzzy scheme biometric enter used as identification [5].

Advantages:-
- Mistakes-tolerant
- Secure towards collusion assaults.

In 2006 V. Goyal, O. Pandey, A. Sahai, and B. Waters, labored on “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data “.This paper, the sender has an authorization to encrypt records. A revoked attributes and keys of customers cannot write once more to stale facts. The characteristic authority getsattributes and mystery keys from the receiver and he/she is capable of decrypt statistics if it has matching attributes [6].

Advantages:-
Distribution of audit-log statistics and display screen out encryption.

In 2007 J. Bethencourt, A. Sahai, and B. Waters, labored on “Cipher textual content-Policy Attribute-Based Encryption”. By the use of this technique the receiver has the get right of entry to coverage inside the shape of a tree. The tree include attributes as leaves and monotonic get admission to shape with AND, OR and different threshold gates[7].

Advantages:-
- Encrypted facts may be saved private although the garage server is untrusted.
- Secure towards collusion assaults.

In 2007 M. Chase, labored “Multi-Authority Attribute Based Encryption”. This scheme describes numerous Key Distribution Authorities (coordinated via a depended on authority) which distribute attributes and mystery keys to customers. Multi authority Attribute Based Encryption protocol which calls for no relied onauthority which calls for each person to have attributes from at all of the KDCs [8].

Implementation

2.1 Modules

1. Key Generation
2. Data Storage in Clouds
3. Reading from the Cloud
4. Writing to the Cloud

2.1.1 Key Generation

There are three users, a creator, a reader, and writer. Creator Alice receives a token from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token. There are multiple KDCs (here 2), which can be scattered. For example, these can be servers in different parts of the world.

A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. In the Fig. 1, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encrypted under the access policy X. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim [9].

2.1.2 Data Storage in Clouds

A consumer Uu first registers itself with one or greater trustees. For simplicity we anticipate there may be one trustee. The trustee offers it a token y=(u,Kbase,K0,p) in which p is the signature on u|| Kbase signed with the trustees personal key TSig (through (6)). The KDCs are given keys PK[i]; SK[i] for encryption/decryption and ASK[i]; APK[i] for signing/verifying [10].

The consumer on offering this token obtains attributes and mystery keys from one or extra KDCs. A key for an characteristic x belonging to KDC Ai is calculated as Kx= Kbase 1/(a+bx), wherein (a , b) ASK[i]. The person additionally getsmystery keys skx; u for encrypting messages. The consumer then creates an get admission to coverage X that is a monotone Boolean characteristic [11]. The message is then encrypted underneath the get right of entry to coverage as C = ABE. Encrypt (MSG, X) the person additionally constructs a declare coverage Y to allow the cloud to authenticate the person. The writer does now not ship the message MSG as is, however makes use of the time stamp T and creates H(C)||T. This is finished to save you replay assaults. If the time stamp isn't always despatched, then the consumer can write preceding stale message returned to the cloud with a legitimatesignature, even if its declare coverage and attributes had been revoked [12].

Reading from the Cloud:

When a person requests records from the cloud, the cloud sends the ciphertext C the usage of SSH protocol. Decryption proceeds the usage of set of rules ABE. Decrypt (C,{sKi,u}) and the message MSG is calculated as the subsequent:
The ciphertext C with signature is c, and is despatched to the cloud. The cloud verifies the signature and shops the ciphertext C. When a reader desires to study, the cloud sends C. If the consumer has attributes matching with get admission to coverage, it may decrypt and get again authentic message [13].

3-Bibliography

[1] S. Ruj, M. Stojmenovic, and A. Nayak, “Privacy Preserving Access Control with Authentication for Securing Data in Clouds,” Proc. IEEE/ACM Int’l Symp.Cluster, Cloud and Grid Computing, pp. 556-563, 2012.

[2] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, “Toward Secure and Dependable Storage Services in Cloud Computing,” IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.- June 2012.

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy Keyword Search Over Encrypted Data in Cloud Computing,” Proc. IEEE INFOCOM, pp. 441-445, 2010.

[4] S. Kamara and K. Lauter, “Cryptographic Cloud Storage,” Proc. 14th Int’l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, “Identity-Based Authentication for Cloud Computing,” Proc. First Int’l Conf. Cloud Computing (CloudCom), pp. 157-166, 2009.

[6] C. Gentry, “A Fully Homomorphic Encryption Scheme,” PhD dissertation, Stanford Univ., http://www.crypto.stanford.edu/craig, 2009.

[7] A.-R. Sadeghi, T. Schneider, and M. Winandy, “Token-BasedCloud Computing,” Proc. Third Int’l Conf. Trust and TrustworthyComputing (TRUST), pp. 417-429, 2010.

[8] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M.Kirchberg, Q. Liang, and B.S. Lee, “Trustcloud: A Frameworkfor Accountability and Trust in Cloud Computing,” HP TechnicalReport HPL-2011-38, http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,” Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[10] D.F. Ferraiolo and D.R. Kuhn, “Role-Based Access Controls,” Proc. 15th Nat’l Computer Security Conf., 1992.

[11] D.R. Kuhn, E.J. Coyne, and T.R. Weil, “Adding Attributes to Role-Based Access Control,” IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.

[12] M. Li, S. Yu, K. Ren, and W. Lou, “Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings,” Proc. Sixth Int’l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.

[13] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute Based Data Sharing with Attribute Revocation,” Proc. ACM Symp.Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.