International Journal of Science and Engineering Applications
Volume 5 Issue 2, March-April 2016

A Survey on Different Techniques Used in Decentralized Cloud Computing

Mohini Tanaji Patil
B.V.D.U.C.O.E.P.
Katraj,Pune,India
Mohini.patil1@gmail.com

Abstract: This paper proposes various methods for anonymous authentication for data stored in cloud. Cloud verifies the authenticity of the series without knowing the user's identity before storing data. This paper also has the added feature of access control in which only valid users are able to decrypt the stored information**.** These schemes also prevents replay attacks and supports creation, modification, and reading data stored in the cloud. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches .The aim of this paper is to cover many security issues arises in cloud computing and different schemes to prevent security risks in cloud. Storage-as-a-service (Saas) offered by cloud service providers (CSPs) is a paid facility that enables organizations to outsource their sensitive data to be stored on remote servers. In this paper, we propose a cloud-based storage schemes that allows the data owner to benefit from the facilities offered by the CSP and enables indirect mutual **trust** between them. This Paper provides different authentication techniques and algorithms for cloud security.
Keywords: cloud security**,** auditing,security,ciphertext.

1. INTRODUCTION

In the current era of digital world, various organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data. The local management of such huge amount of data is problematic and costly due to the requirements of high storage capacity and qualified personnel. Therefore, storage-as-a-service(Saas) offered by cloud service providers (CSPs) emerged as a solution to mitigate the burden of large local data storage and reduce the maintenance cost by means of outsourcing data storage. Since the data owner physically releases sensitive data to a remote CSP, there are some concerns regarding confidentiality, integrity, and access control of the data. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote servers. For verifying data integrity over cloud servers, researchers have proposed provable data possession technique to validate the intactness of data stored on remote sites. A number of PDP protocols have been presented to efficiently validate the integrity of data. Proof of retrieve ability was introduced as a stronger technique than PDP in the sense that the entire data file can be reconstructed from portions of the data that are reliably stored on the servers. Commonly, traditional access control techniques assume the existence of the data owner and the storage servers in the same trust domain. This assumption, however, no longer holds when the data are outsourced to a remote CSP, which takes the full charge of the outsourced data management, and resides outside the trust domain of the data owner. A feasible solution can be presented to enable the owner to enforce access control of the data stored on a remote untrusted CSP. Through this solution, the data are encrypted under a certain key, which is shared only with the authorized users. The unauthorized users**,** including the CSP, are unable to access the data because they do not have the decryption key. This general solution has been widely incorporated into existing schemes, which aim at providing data storage security on untrusted remote servers. Another class of solutions utilizes attribute-based encryption to achieve fine-grained access control.

Different approaches have been investigated that encourage the owner to outsource the data, and offer some sort of guarantee related to the confidentiality, integrity, and access control of the outsourced data. These approaches can prevent and detect malicious actions from the CSP side. On the other hand, the CSP needs to be safeguarded from a dishonest owner, who attempts to get illegal compensations by falsely claiming data corruption over cloud servers. This concern, if not properly handled, can cause the CSP to go out of business.

2. CLOUD SECURITY ISSUES AND CHALLENGES

Cloud computing is a emerging technology with shared resources, lower cost and rely on pay per use according to the user demand. Due to many characteristics it has effect on IT budget and also impact on security, privacy and security issues. All those CSPs who wish to enjoy this new trend should take care of these problems. Customer not know where the data are stored, who manage data and other vulnerabilities that can occur. Following are some issues that can be faced by CSP while implementing cloud services.

2.1 Privacy Issues

It is the human right to secure his private and sensitive information from others. In cloud context privacy occur according to the cloud deployment model. In Public cloud (accessed through the Internet and shared amongst different consumers) is one of the dominant architecture when cost reduction is concerned, but relying on a CSP to manage and hold customer information raises many privacy concerns and are discussed under:

2.2 Lack of user control

In SAAS environment service provider is responsible to control data. Now how customer can retain its control on data when information is processed or stored. It is legal requirement of him and also to make trust between customer and vendor.

2.3 Unauthorized Secondary Usage

One of the threats can occur if information is placed for illegal uses. Cloud computing standard business model tells that the service provider can achieve profits from authorized

Secondary uses of users' data, mostly the targeting of commercials. Now days there are no technological barriers for secondary uses

2.4 Audit

To implement internal monitoring control CSP need external audit mechanism .But still cloud fails to provide auditing of the transaction without effecting integrity.

3. DIFFERENT TECHNIQUES USED FOR DECENTRALIZED ACCESS CONTROL

3.1 Flexible distributed storage integrity auditing mechanism [1] ensures strong cloud storage. Assurance of cloud data integrity availability achieved by enforcing quality of cloud storage service. To achieve data integrity and availability data may store across multiple physical servers. They support dynamic data support including block update, delete and append. Since data do not resides at users' local site but at cloud service provider's address domain. This system is useful for achieving integration of storage correctness insurance and data error localization i.e. It is useful for detecting servers that not working properly. It is highly efficient to malicious data modification attacks and support third party auditing. It mainly useful for SaaS cloud platform.

3.2 Identity based authentication [2] is a new identity based authentication protocol for cloud computing and services. Identity based encryption (IBE) and identity based signature (IBS) schemes are useful to achieve security in communication. Based on IBE and IBS, identity based authentication for cloud computing (IBACC) is proposed. This protocol is more effective and lightweight than SAP (SSL Authentication Protocol).It is more lightweight on user side.

3.3 The act of trust in clouds [3] focuses on cloud accountability & auditability and gives preventive approaches to increase accountability. There are many components of trust in cloud.i.e.security, privacy, accountability, availability. Further they classified trust component into 2 categories as preventive control and detective control. They introduces Cloud Accountability Life Cycle (CALC) CALC consists of 7 phases. These are policy planning, sense and Trace, Logging, Safe keeping, reporting and Replaying, Auditing, Optimizing and Rectifying. According to CALC's phases, it introduces abstraction layers of accountability in cloud computing i.e. workflow layer, Data layer, and System layer .This technique is useful to investigate external risks and risks within CSP

3.4 Mandatory Access Control(MAC)[4] which is used in secure military applications whereas Discretionary Access Control(DAC) is used in security processing of industrial and civilian of government. In many organizations, end user does not own information for which they allow access so DAC is not useful. In these case, role based access control is appropriate which promotes central administration of an organizational specific security policy. This method gives secure processing needs of much civilian government organization and more suitable than DAC (Discretionary Access Control).

3.5 Role based access control with attribute support [5] dynamic attributes. A pure RBAC solution may provide inadequate support for dynamic attributes. To support dynamic attributes, proposed attribute based access control suggests that attribute and rule either replace RABC or make it more simple and flexible. They support dynamic attributes.

3.6 Hierarchical Attribute Based Encryption for Fine Grained Access Control [6] is useful for organizations to efficiently share confidential data on cloud servers. It supports fine grained access control and also provides high performance to obtain data. This scheme achieved goal by combining hierarchical identity based encryption and ciphertext policy attribute base encryption. There is 3 levels HABE model. Root Master (RM) is root level model corresponds to Trusted Third Party (TTP). Multiple Domain Masters (DMs) that is responsible for multiple enterprise users and numerous users that correspond to all personnel in enterprise. This scheme gives high performance and scalability and support fine grained access control.

3.7 Attribute Based Signature (ABS) [7] not attests to identity of individual but instead to a claim regarding attributes. ABS is mainly useful for Attribute Based Messaging as well as in security and authentication. This ABS scheme supports multiple authorities and multiple signature trustees who need not trust each other. This is also centralized approach. This scheme significantly saves decryption time and provides strong privacy.

3.8 Attribute Based Signature [8] proposes application of ABS like ABS, ABA. In ABS signature, signature hides attributes used to satisfy predicate and any identifying information about signature. This method takes decentralized approach and provides authentication without disclosing identify of users. This method is Secure against malicious attribute authority.

3.9 Authorization to encrypt information using ABS for fine grained access control [9] introduces new cryptosystem called Key-policy Attribute Based Encryption (KP-ABE). In KP-ABE, cipher text are labeled With sets of attributes and private keys are associated with access structures then control which cipher text to use is able to decrypt. This method distributes audit log information.

3.10 For realizing complex access control on encrypted data ciphertext-Policy Attribute Based Encryption [10] is used. By using this technique encrypted data can be kept confidential even if storage secure against collusion attacks. In previous systems, attributes are used to describe encrypted data and built policies in user's credentials. This system allows policies to be expressed as any free access structure and is resistant to collusion attacks. Encrypted information can be kept confidential even if storage server is untrusted and also secure against collusion attacks.

3.11 There are several key Distribution Authorities co-ordinated by a trusted authority, which distribute attributes and secret keys to users. They propose multiple attribute [11] authorities monitor different sets of attribute which does not require no trusted authority. This method allows more numbers of attributes.

4. DISCUSSION

The different access control approaches in this survey support both centralized and decentralized approach. In this paper we compare different access control schemes according to their access control criteria. For Example, access control mechanism based on used identity or role, also done through their attributes. Each of these scheme having their own advantages and disadvantages, as result can be used to guide selection of an appropriate approach according to their needs and also find out key areas for future enhancement. Performance of access control schemes varies from one mechanism to different. RBAC,ABAC

having high performance than traditional DAC,MAC whereas performance of MAC depends on security level. All access control mechanisms are user convenient

5. CONCLUSION

This survey presented a decentralized access control technique with anonymous authentication. This decentralized scheme provides user revocation and prevents replay attacks. It provides the load balancing as well as request broker services which will able to handle multiple cloud storage providers (CSP). So it will actually improve the performance of the system because load is shared across the storage service provider very efficient manner. It will prevent from the many attack. Even though the cloud does not know the identity of the user who stores information, but it verifies the user's credentials. The main purpose of this paper is to introduce different access control techniques used in cloud with their benefits.

6. REFERENCES.

[1] 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.Junen2012**.**

[2] 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.

[3] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M.Kirchberg, Q. Liang, and B.S. Lee, "Trustcloud: A Framework for Accountability and Trust in Cloud Computing," HP Technical ReportHPL201138,http://www.hpl.hp.com/techreports/

[4] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc.15th Nat'l Computer Security Conf., 1992

[5] 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.

[6] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.

[7] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance,"IACR Cryptology ePrint Archive, 2008.

[8] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392,2011.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[11] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf.Computer and Comm. Security, pp. 121-130, 2009.

[12] Sushmita Ruj,Milos Stojmenvovic and Amiya Nayak "Decentralized Access Control Anonymous Authentication Of Data Stored in Clouds "IEEE TRANSACTIONS 2014