Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 8, August 2016, pg.85 – 91

Survey on Decentralized Access Control with Anonymous Authentication of Data Stored in Cloud

Stalin
M.Phil. Scholar,
Department of Computer Science,
Bishop Heber College (Autonomous),
Trichirappalli, Tamilnadu, India

R.Thamarai Selvi
Asst. Professor & Head,
Department of computer Applications,
Bishop Heber College (Autonomous),
Trichirappalli, Tamilnadu, India

ABSTRACT: This Paper new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the scheme the cloud verifies the authenticity of the series without knowing the user's identity before storing data. In this study scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. It's prevents replay attacks and supports creation, modification, and reading data stored in the cloud. In this paper address user revocation. Moreover, our authentication and access control scheme is decentralized and robust, different other access control schemes designed for clouds which are centralized. In this Paper used technique algorithms digital signature key, attribute-based encryption, cloud storage.

Keywords: Cloud computing, Access control, authentication, digital signatures key, attribute-based encryption, cloud storage

1. INTRODUCTION

In cloud computing is getting a lot of attention from both academic and industrial worlds. In cloud computing, users should be outsource their computation and storage to servers (also called clouds) using Internet. This frees users from the hassles of preserving resources on-site. Clouds can provide several types of services like requests (e.g., Google Apps, Microsoft online), organizations (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write requests (e.g., Amazon's S3, Windows Azure). Much of the data stored in clouds is highly sensitive, for example, medical archives and social systems. Security and privacy are, thus, very important issues in cloud computing. In one hand, the user should authenticate itself earlier creating any transaction, and on the other hand, it must be ensured that the cloud does not damage with the data that is out sourced. User

privacy is also required so that the cloud or other users do not know the uniqueness of the user. The cloud can hold the user accountable for the data it outsources, and similarly, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also proved.

Apart from the technical results to ensure security and privacy, there is also a need for law enforcement. Just now, Wang et al. addressed secure and dependable cloud storage. Cloud servers prone to Byzantine disaster, where a storage server can fail in random ways. The cloud is also prone to data modification and server colluding attacks. In server plotting attack, the adversary can compromise storage servers, so that it can modify data files as long as they are with in constant. To provide secure data storage, the data needs to be encrypted. However, the data is often altered and this dynamic property needs to be taken into account while designing efficient secure storage techniques. Effective search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to store the files that satisfy the query. This is achieved by means of searchable encryption. The keywords are lead to the cloud encrypted, and the cloud returns the result without knowing the actual keyword for the search. The difficult here is that the data records should have keywords associated with them to enable the search.

2. RELATED WORK

S. Ruj, A. Nayak, and I. Stojmenovic,(2011), says about "Privacy Preserving Access Control with Authentication for Securing Data in Clouds" Current methodologies to impose fine-grained access control on confidential data hosted in the cloud remain based on fine-grained encryption of the data. Under such approaches, data owners are in charge of encrypting the data earlier uploading them on the cloud and re-encrypting the data whenever user credentials change. Data owners can be emphasizethe high communication and computation costs. A better approach should delegate the execution offline-grained access control to the cloud, so to diminish the overhead at the data owners, while assuring data confidentiality from the cloud. We suggest an approach, based on two layers of encryption that addresses such requirement. **Algorithm** Attribute based access control (ABAC),

C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing" Cloud storage supports users to remotely store their data and enjoy the on-demand high quality cloud requests without the burden of local hardware and software management. Though the benefits are clear, such a service is also leaving user's physical possession of their outsourced data, which inevitably poses new security hazards toward the correctness of the data in cloud. In order to address this new problem and further achieve a secure and reliable cloud storage service, we propose in this paper a flexible distributed storage integrity inspecting mechanism, developing the homo-morphed token and distributed erasure-coded data.

M. Li, S. Yu, K. Ren, and W. Lou, says about "**Securing Personal Health Records in Cloud Computing",** Personal health record (PHR) is an emergent patient-centric distinctive of healthiness factual interchange, which is frequently outsourced to be stored at a third party, such as cloud providers. We impact the Attribute Based Encryption (ABE) techniques to encrypt each patient's PHR file. Different from above works in secure data outsourcing, we focus on the various data owner scenario, and divide the users in the PHR system into several security domains that significantly shrinks the key management complexity for owners and users. Our scheme also enables dynamic consistency of access policies or file attributes, supports efficient on-demand user/attribute reverse and break-glass access under emergency situations. Extensive analytical and experimental results are presented which presence the security, scalability and efficiency of our future scheme. **Algorithms ABE,KeyEswro**

S. Ruj, A. Nayak, and I. Stojmenovic,(2011), says about "Distributed Access Control in Clouds" In proposed a data storage and access in which many encrypted copies of data can be dodged. The main novelty of this paper is producing the key distribution centers wherever one or more KDCs distribute keys to data owners and users. KDC provide access to particular fields in all records. Solitary keys separates the data and the data owners, using this technique the user own the data by having the attribute it had, and this can be rescued only if the attribute matches the data. The Author apply the Attribute Based Encryption (ABE)scheduled elliptic curves. This scheme is collusion secure in which two users cannot composed decode any data, that no one has individual right to access.

S. Jahid, P. Mittal, and N. Borisov,(2011), "Easier: Encryption-Based Access Control In Social Networks With Efficient Revocation This thesis an approach of privacy risk in the Online Social Network (OSN's) , in which it shifts OSN provider to User by Encryption. This make a key management and the dynamic groups, to address this problem the author proposed the Easier an architectural sustenance in Fine grained access control and the dynamic group by the Attribute based Encryption. It is possible to eliminate access from a user without issuing new keys to other users or re-encrypting existing ciphertexts, this is achieved by creating the proxies and using this proxy can minimally trusted and cannot decrypt ciphertexts or provide access to previously revoked users. This type of technique is used in FACEBOOK

D. Chaum and E.V. Heyst,(2012)"Attribute-Based Signatures: Achieving Attribute-Privacy Collusion resistance" In proposed an Attribute based Signature in which the signature demonstrates not to identify the individual of the message by a user instead it claim regarding the attribute that created by the user. The signature was shaped by a single party whose attributes satisfy the claim being made i.e. it is not plotting the all individuals instead it just make the attribute together who pooled it. The author explains the security of ABS as a cryptographic primitive, and then tells that efficient ABS construction based on groups with bilinear pairings. Thus by verifying the construction is secure in the generic group model, ABS fills a critical security requisite in attribute-based messaging(ABM) systems.

A. Beimel,(1996)"Secured Scheme For Secret Sharing And Key Distribution" In proposed the sharing of data, now a day's take place in Computer Networks, and the data which can be communicated privileged network may affected through the bad users, to overcome this user users two Cryptographic tools such as Isolated Secret Sharing scheme and Key distribution scheme. These make it probable to store only the secret information in the network such that good users can be access the information. the secret sharing scheme generally established through the verge secret sharing schemes, only through the certain threshold the information can accessed and can used by the user.

A. Sahai and B. Waters,(2005) "Fuzzy Identity-Based Encryption" A new Identity Based Encryption (IBE) scheme, another one is called as Fuzzy Identity-Based Encryption. A Fuzzy IBE private key was identity by ω while the ciphertext encrypted is identified by ω. It selves ω and ω' are can be measured by the "set overlap" reserve metrics. It used to put on the Encryption by obtaining the biometric input as identifier which essentially has some noise each time they are tested. Thus it is used for a type of application that we term "attribute-based encryption". In this paper two construction of Fuzzy, IBE scheme are elaborate where the Identity-Based Encryption of a message below some attributes that combine a (fuzzy) identity. Hence in this scheme both are error-tolerant and secure alongside collusion attacks.

3. PERFORMANCE ANALYSIS

In this section, we propose our privacy conserving authenticated access control scheme. According to our scheme a user can make a file and store it securely in the cloud. This scheme consists of use of the two protocols ABE and ABS, respectively. We will first deliberate our scheme in details and then provide a concrete example to demonstrate how it works. There are three users, a creator, a reader, a writer. Creator Alice receives a token from the trustee, who is assumed to be honest. A trustee can be somebody like the federal government who manages social insurance numbers etc.

A creator on presenting the token to one or more KDCs takes keys for encryption/decryption and signing. In the Fig. 1, SKs are secret keys given for decryption, Kxoe are keys for passing. The message MSG is encrypted under the access policy X. The creator agrees on a claim policy Y, to prove her authenticity and signs the message under this claim. The cloud validates the signature and stores the ciphertext C. While a reader wants to read, the cloud sends C. If the user has attributes can be matching with access policy, it can decrypt and get back unique message.

Cloud computing

Cloud computing is the use of computing properties (hardware and software) that are delivered as a service over a network (typically the Internet). The name derives from the common use of a cloud-shaped symbol as an abstraction for the complex structure it comprises in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation.

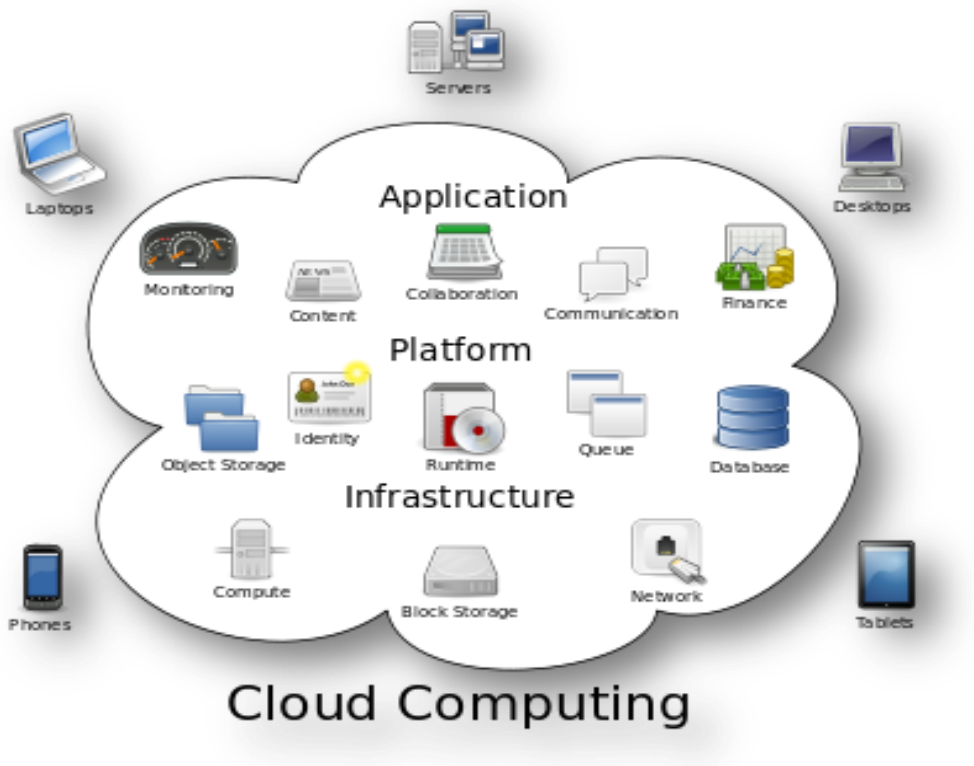
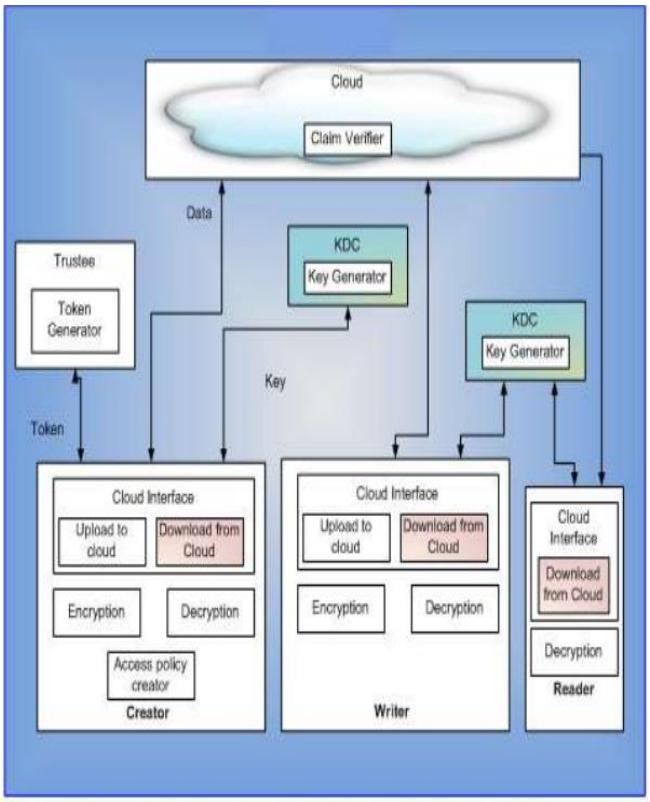


Figure : 1 Cloud Computing

SYSTEM MODULES



Comparison of Our Scheme with Existing Access Control Schemes

Fine Grained Access Control	Centralized /Decentralized	Write/Read Access	Type of access control	Privacy Authentication	User Revocation
Yes	Centralized	1-W-M-R	ABE	No Authentication	No
Yes	Centralized	1-W-M-R	ABE	No Authentication	No
Yes	Centralized	1-W-M-R	ABE	No Authentication	No
Yes	DeCentralized	1-W-M-R	ABE	No Authentication	No
Yes	Centralized	1-W-M-R	ABE	No Authentication	No
Yes	DeCentralized	1-W-M-R	ABE	Not Privacy	No
Yes	Centrailzed	M-W-M-R	ABE	Authentication	No
Yes	DeCentralized	M-W-M-R	ABE	Authentication	Yes

Scheme	Read/write Access
Secure and efficient access to outsoursed data	1-W-M-R
Securing Personal Health Records in Cloud Computing	1-W-M-R
DACC: Distributed Access Control in Clouds	1-W-M-R
Outsourcing the Decryption of ABE Ciphertexts	1-W-M-R
Decentralizing Attribute-Based Encryption	1-W-M-R
Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems	M-W-M-R
Proposed System	M-W-M-R

Table 1: Comparison between the access policy between the schemes

File Size	Upload (Sec)	Download (Sec)
10 Bytes	15	0
1 KB	17	3
10 KB	19	0
100KB	20	7
1 MB	22	7

Table 2 :Analysis of time required for transaction on cloud

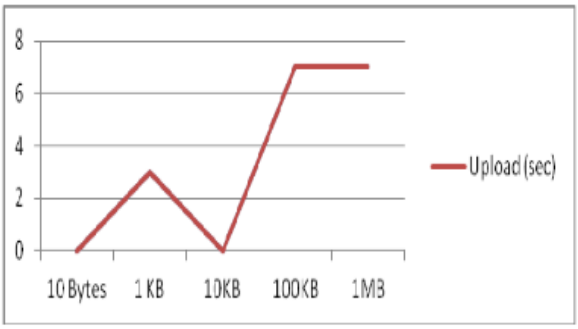


Figure 2: Graph showing time required for uploading the file on cloud

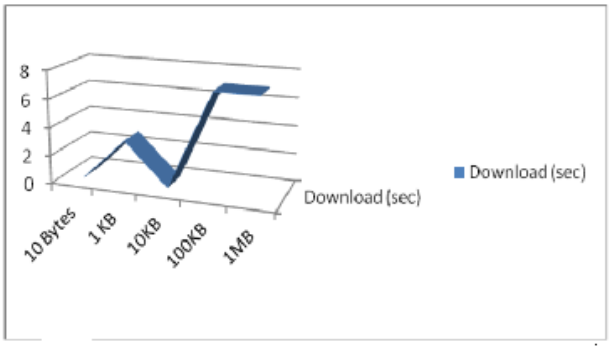


Figure 3: Graph showing time required for downloading the file on cloud

4. CONCLUSION

This Paper has presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents repetition attacks. The cloud does not know the identity of the user who stores information, but only the user's identifications. Key dispersal is done in a decentralized way. One limitation is that the cloud knows the access procedure for each record stored in the cloud. Paper dealt about various methods prevailing in works of unidentified authentication mechanisms for data stored in clouds. It is a Decentralized access of system in which

each system have the access control of data. This Scheme prevents Replay attack which mean Eaves Dropping can be avoided, sustenance creation of data inside storage, Modifying the data by unknown users, and Reading data stored in Cloud. Users can revocate the data only by talking over the cloud. The authentication and accessing the Cloud is Robust, Hence general communication storage has developed by comparing to the Centralized approaches. This paper would encourage a lot of research in the area of Anonymous Authentication.

REFERENCES

[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-Based Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (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 Framework for Accountability and Trust in Cloud Computing," HP Technical Report HPL-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.
[14] 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.
[15] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.

