INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

A REVIEW ON DECENTRALIZED ACCESS CONTROL WITH ANONYMOUS AUTHENTICATION OF DATA STORAGE IN CLOUDS

PROF. MAHIP BARTERE[1], BHARATI DALVI[2]

1. Guide, Dept. of Computer Sci. & Engg., G. H. Raisoni College of Engg. &Management, Amravati.
2. Guide, Dept. of Computer Sci. & Engg., G. H. Raisoni College of Engg. &Management, Amravati.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* In this paper we propose a new decentralized access control scheme for secure data storage in clouds which supports anonymous authentication. The cloud verifies the authenticity of the series without significant knowledge in the user's identity before storing information. This scheme also has the added feature of access control. In access control scheme only valid users are able to decrypt the stored data/information. This scheme prevents replay attacks also supports creation, modification, and reading information stored in the cloud. These schemes also address user revocation. Moreover, the authentication and access control scheme is decentralized and robust in nature unlike other access control schemes designed for clouds which are centralized. The computation, communication, and storage overheads are comparable to centralized approaches.

Keywords: Access control, anonymous authentication, decryption/ encryption, data storage, cloud.

PAPER-QR CODE

Corresponding Author: PROF. MAHIP BARTERE

Access Online On:

www.ijpret.com

How to Cite This Article:

Mahip Bartere, IJPRET, 2016; Volume 4 (9): 552-559

INTRODUCTION

In cloud computing, users can catch out their computation and storage to servers (also called clouds) using Internet. This frees users form the stability of maintaining resources on-site. Several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms (e.g., Amazon's S3, Windows Azure) can be provided by cloud to help developers to maintain secure connections.

Information which is stored in clouds is very sensitive. For example, medical records and social network, we can consider these as a sensitive data. In cloud computing, security and privacy are considered as a big issue. At first step the user should authenticate itself before initiating any transaction, and on the second step, it must be ensured that the cloud does not alter with the data that is outsourced.

User privacy is also required in cloud. By using privacy the cloud or other users do not know the identity of the other user. The cloud can hold the user accounts for the data in cloud, and likewise, to provide services the cloud itself is accountable. The validity of the user who stores the data is also verified. There is also a need for law enforcement apart from the technical solutions to ensure security and privacy.

The cloud is also prone to data modification and server colluding attacks. The adversary can compromise storage servers in server colluding attack, so that server can modify data files even though the servers are internally consistent. The data needs to be encrypted to provide secure data storage. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques [1].

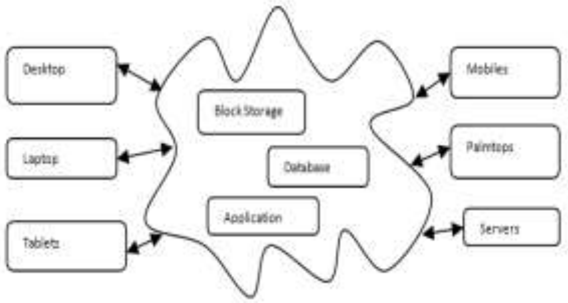

Fig1: Example diagram for data sharing with cloud storage.

Efficient search on encrypted data is also an important fear in clouds. The clouds should not know the query but it can be able to return the records that satisfy the query. Searchable encryption used to achieve this scheme.

Users authentication scheme using public key cryptographic technique is used in cloud computing. Many homomorphic encryption techniques have been optional to ensure that the cloud is not able to read the data while performing computations on the data. By using this encryption scheme, the cloud receives cipher text of the data and performs computations on the cipher text and returns the encoded value of the result to user then the user is able to decode the result, even though the cloud does not know what data it has operated on. In such circumstances, it must be probable for the user to verify that the cloud returns correct results.

Neither the clouds nor users should deny any operations performed or requested. It is important to have log of the transactions performed;

II. RELATED WORK &LITERATURE SURVEY

In 2006, A. Sahai and B. Waters worked on “Fuzzy Identity-Based Encryption” In Identity Based Encryption scheme, user has a set of attributes in addition to its unique ID. A Fuzzy IBE scheme can be applied to enable encryption .In Fuzzy scheme biometric input used as identity. This proposed method was error-tolerant and also secure the data against collusion attacks [2].

In 2006, V. Goyal, O. Pandey, A. Sahai, and B. Waters, proposed another technique for encryption of data i.e.; “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data”. In this scheme, the sender has an authorization to encrypt information. A revoked attributes and keys of users cannot write again to steal information. The attribute authority receives attributes and secret keys from the receiver and the user will be able to decrypt information if he/she has matching attributes [3].

In 2007, J. Bethencourt, A. Sahai, and B. Waters worked on “Cipher text-Policy Attribute-Based Encryption”. By using this approach the receiver has the access policy in the form of a tree. The tree contain attributes as leaves and monotonic access structure with AND, OR and other threshold gates The advantage of using this technique is that the encrypted information can be kept confidential even if the storage server is not trusted; and it is also secured against collusion attacks [4].

In 2007, M. Chase, worked on “Multi- Authority Attribute Based Encryption”. This scheme describes several Key Distribution Authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users. Multi-authority Attribute Based Encryption protocol does not require a trusted authority, which means every user must have attributes from at all the KDCs. The benefit of using this technique is that it allows more number of attributes [5].

In 2008, H.K. Maji, M. Prabhakaran, and M. Rosulek worked on “Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance”. In this paper, ABCs were introduced to ensure anonymous user authentication. This was also a centralized approach. The basic advantage of using this technique is that the user significantly saves decryption time, without raising the number of transmissions [6].

In 2010, M. Li, S. Yu, K. Ren, and W. Lou worked on “Securing health records in cloud computing: Patient-centric and fine-grained data access control in multi owner settings”. A colossal measure of data is constantly archived in the cloud, and much of this is sensitive data. Utilizing Attribute Based Encryption (ABE), the records are encrypted under a few access strategy furthermore saved in the cloud. Clients are given sets of traits and corresponding keys. Just when the clients have matching set of attributes, would they be able to decrypt the data saved in the cloud [7].

In 2011, A.B. Lewko and B. Waters worked on “Decentralizing Attribute-Based Encryption,” In this proposed work users could have zero or more number of attributes from each authority and did not require a trusted server. This proposed technique is collision resistant [8].

In 2011, M. Green, S. Hohenberger and B. Waters proposed another work based on “Outsourcing the Decryption of ABE Ciphertexts,” .This proposed scheme subcontract the decryption task to a proxy Server, so that the user made computation on minimum resources like hand held devices. The advantage of using this is that the user significantly saves bandwidth, without raising the number of transmission [9].

In 2011, S. Jahid, P. Mittal, and N. Borisov proposed EASIER ie; “EASiER: Encryption-based access control in social networks with efficient revocation”. Access control is likewise gaining imperativeness in online social networking where users store their personal data, pictures, films and shares them with selected group of users they belong. Access control in online social networking has been studied in [10].

In 2011, the work done by F. Zhao, T. Nishide, and K. Sakurai in ““Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems,” gives privacy preserving authenticated access control in cloud. Nonetheless, the researchers take a centralized methodology where a single key distribution center (KDC) disperses secret keys and attributes to all clients. Unfortunately, a single KDC is not just a single point of failure however troublesome to uphold due to the vast number of clients that are upheld in a nature's domain. This scheme] uses a symmetric key approach and does not support authentication [11].

In 2011, S. Ruj, A. Nayak, and I. Stojmenovic proposed "DACC: Distributed access control module in clouds". On the other hand, the approach did not provide client verification. The other weakness was that a client can make and store a record and different clients can just read the record. write access was not allowed to clients other than the originator [12].

In 2012, Kan Yang, Xiaohua Jia and Kui Ren proposed a decentralized approach in "DAC-MACS: Effective Data Access Control for Multi- Authority Cloud Storage Systems", their strategy does not confirm clients, who need to remain anonymous while accessing the cloud [13].

III.PROPOSED SYSTEM

We propose our privacy preserving authenticated access control scheme now. The scheme consists of use of the two protocols ABE and ABS.

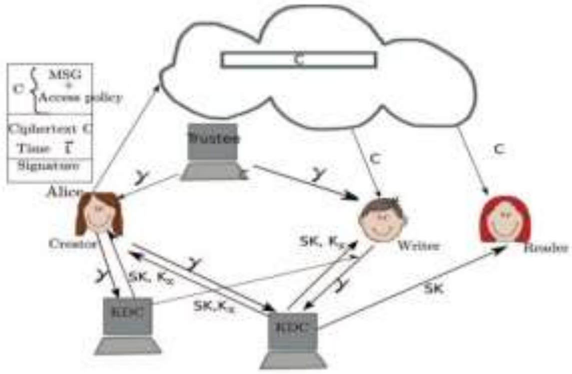

Fig. 2. Cloud secure storage model.

There are three following users, a creator, a writer, and a reader. Creator Alice receives a token γ from the trustee, now it is assumed to be who is honest. 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 defines a claim policy Y to prove the authenticity and signs of the message under this claim.

The cipher text C with a signature c is sent to the cloud. The cloud verifies the signature and stores the cipher text C. When a reader wants to read the message in the cloud sends C. That the user has attributes matching with the access policy, it can be decrypted and get back the original message.

Write also proceeds in the similar way as file creation. By designating the verification of the data to the cloud, it relieves the individual users from time consuming verifications.

When a reader wants to read some data stored in the cloud, it tries to decrypting and using the secret keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.

A. *Data Storage in Clouds*

A user can have one or more trustees. This is used to prevent the replay attacks. In this time, data is not sent, then the user can write previous stale message back to the cloud with a valuable signature, even when its claim policy and attributes have been revoked.

B. *Data Storage in Clouds*

The user requests data from the cloud, the cloud sends the cipher text using SSH protocol. Decryption proceeds using ABE algorithm.

C. *Data Storage in Clouds*

The user must send its message with the claim policy as done during file creation. The cloud verifies the claim policy, and only if the user is authentic, he/she is allowed to write on the file.

D. *User Revocation*

It should be ensured that users must not have the ability to access data, even if they possess matching set of attributes.

E. *Advantages*

1) Our access control scheme is secure which means no outsider or cloud can decrypt cipher texts.

2) Collusion resistant.

3) Can be accessed by authorized users only.

4) Resistant to replay attacks

5) Protects privacy of the user.

6) The cloud is honest-but-curious, such that the cloud administrators can be able to view user's content, but cannot modify data.

7) Honest-but-curious model of adversary do not tamper with data so that they can keep the system functioning normally and remain undetected.

8) Users have rights like either read or write or both accesses to a file stored in the cloud.

9) The communications between users/clouds are secured by secure shell protocol, SSH.

CONCLUSION

This review paper presented a decentralized access control technique with anonymous authentication. This decentralized scheme provides user revocation and prevents replay attacks. Even though the cloud does not know the identity of the user who stores information, but it verifies the user's credentials. This paper made key distribution is done in a decentralized way. In our next paper we will present the working of our proposed work.

ACKNOWLEDGMENT

I would be grateful to my guide for his cooperation in studying various security techniques used for data stored in cloud.

REFERENCES

1. R.Ranjith, D.Kayathri Devi, "Secure Cloud Storage using Decentralized Access Control with Anonymous Authentication", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013.
A. Sahai and B. Waters, "Fuzzy Identity- Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.
2. 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.
3. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

4. M. Chase, “Multi-Authority Attribute Based Encryption,” Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515- 534, 2007.

5. H.K. Maji, M. Prabhakaran, and M. Rosulek, “Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion- Resistance,” IACR Cryptology ePrint Archive, 2008.

6. M. Li, S. Yu, K. Ren, and W. Lou, “Securing health records in cloud computing: Patient-centric and fine-grained data access control in multi owner settings,” in SecureComm, pp. 89–106, 2010.

7. A.B. Lewko and B. Waters, “Decentralizing Attribute-Based Encryption,” Proc. Ann. Int’l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.

8. M. Green, S. Hohenberger, and B. Waters, “Outsourcing the Decryption of ABECiphertexts,” Proc. USENIX Security Symp., 2011.

9. S. Jahid, P. Mittal, and N. Borisov, “EASiER: Encryption-based access control in social networks with efficient revocation,” in ACM ASIACCS, 2011.

F. Zhao, T. Nishide, and K. Sakurai, “Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems,” in ISPEC, ser. Lecture Notes in Computer Science, vol. 6672. Springer, pp. 83–97, 2011.

10. S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed access control in clouds,” in IEEE TrustCom, 2011.

11. Kan Yang, Xiaohua Jia and Kui Ren, “ DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems”, IACR Cryptology ePrint Archive, 419, 2012.