Secure Data Storage in Cloud by using Assymetric Key Management based Encryption

C. Vinoth[1], Prof. G. R. Anantha Raman[2]
Department of Computer Science and Engineering, Adhiyamaan College of Engineering, Hosur, India

ABSTRACT

Cloud computing is a recently evolved computing terminology in which benefits of the computing framework that given as a service over the Internet. We progress a new methodology for fine grained sharing of re-encrypted data that we call Key-Policy Attribute Based Encryption (KP-ABE). This technique presents a real processing overhead on data possessing for key distribution and the data administration. When fine-grained access control of data is in demand, and subsequently does not scale well. The issue of the same time managing fine-grained, scalability and the data confidentiality of access control is still remain uncertain. We accomplish this goal by using decentralized key policy Attribute Based Encryption (KP-ABE). Extensive study shows that the proposed scheme is highly efficient and secure.

Keywords: Access Control, Cloud Computing, Key-Policy Attribute Based Encryption (KP-ABE)

I. INTRODUCTION

Cloud computing is a propitious computing model which currently has drawn far reaching analysis from both the educational community and industry. A set of existing and new method from the research areas like Service-Oriented Architectures (SOA) and virtualization method, cloud computing is has all things considered a computing model in which benefits in the computing infrastructure are given as services over the Internet. It is one of the new business solutions for remote reinforcement outsourcing, then it offers a reflection of helpful storage space for customers to have data reinforcements in a pay-as-you- go way. It helps associations and government offices fundamentally decrease their financial overhead of data administration, since they can now able to store their data reinforcements remotely to third-party cloud storage suppliers as opposed to keep up data centers on their own. Numerous services like Net banking, email and so forth are given on the Internet such that the customers can utilize them from anyplace at any time. The cloud storage is exactly more adaptable and then the security and protection are accessible for outsourced data turns into a genuine concern. The three main issues are availability, integrity and confidentiality.

To accomplish secure data agreement in cloud, suitable cryptography method is used. The data possessor must encrypt these records and then store the records to the cloud. Assuming that, the third party downloads the record, and they may see records only if they had the key that will be used to decrypt the encrypted record. This may lead to failure because of the improvement of technology and the programmers. To solve this issue there is lot of procedures and techniques to make secure transaction and storage.

Recently the Anonymous authentication is considered for data archiving to clouds. Anonymous authentication is the method of accepting the client without knowing the details of the client. So, the cloud server does not know the details of the client, which gives more security to the clients to conceal their details from the other clients of that cloud.

Privacy and security assurance in clouds are analyzed and tested by many researchers. The paper gives storage security uses the Reed-Solomon eradication correcting the codes. By using homomorphic encryption, the cloud obtains cipher text and furnishes an encoded value of the result. The client has the capacity to convert the result; however the cloud does not understand what data it has worked on.

In this paper Key-Policy Attribute Based Encryption scheme has been used to control unauthorized access of data. In addition revocation plan is used for the time based file assured deletion.

IJSRSET151166 | Received: 18 Feb 2015 | Accepted: 24 Feb 2015 | January-February 2015 [(1)1: 303-305]

II. METHODS AND MATERIAL

RELATED WORK

Access control in clouds is obtaining consideration on the grounds that it is essential that only authorized clients have been able to access the services. A massive measure of data is always archived in the cloud, and much of the data are more sensitive. Using Attribute Based Encryption (ABE), the data are encrypted under a few access strategy moreover saved in the cloud. Clients are the sets of traits and corresponding keys. Just the clients have matching set of attributes, would they will be able to decrypt the data that saved in the cloud. Junbeom et al. studied the access control schemes in health care.

Access control is also gaining essential data in online social networking where users store their personal films, data and pictures and shares them with the selected group of users. Access control scheme in online social networking has been studied. The work done by allows privacy preserving authenticated access control to secure data stored in cloud. The researchers take a centralized procedure then a single key distribution center (KDC) distributes the attributes and secret keys to all the clients. A single key distribution center (KDC) is not just a single point of failure but troublesome to confirm due to the vast number of clients that are upheld in a nature's domain.

This scheme uses a symmetric key approach that does not support authentication. Multi-authority ABE scheme was concentrated on in which required no trusted power which needs each client to have the characteristics from all the KDCs.

In spite of the reality that Jingwei et al. prefer a decentralized approach, their policy does not confirm clients, who required to remain anonymous while obtain the cloud. Sushmita Ruj et al. proposed a distributed access control module in clouds. On the other hand, the proposal did not give client verification. One of the other problems is that a client can make and cache a record and different clients can only read the record. The access to write on the data is not allowed to clients other than the creator.

Time-based file assured deletion that is initially presented and understood that records could be securely erased and survive forever difficult to reach after some predefined time. The primary idea is a record that is encrypted with information key by the possessor of the data and this information key has been further encrypted with a control key by a different key Manager.

III. PROPOSED METHODOLOGY

A. Distributed Key Policy Attribute Based Encryption

KP-ABE is a public key cryptography technique for one-to-many correspondences. In KP-ABE, information is related with attributes for all of which a public key part is identified. The encryption links the set of attributes to message by scrambling it with the comparing public key parts. Each client is assigned an access structure that normally characterized as access tree over the information attributes, i.e., inside center of the access tree are limit doors and the leaf hubs are joined with attributes. The client secret key is characterized to return the access structure so the client has the capacity to decode a cipher-text if and only if the information attributes fulfill the access structure. The proposed system consists of four algorithms which defined as follows.

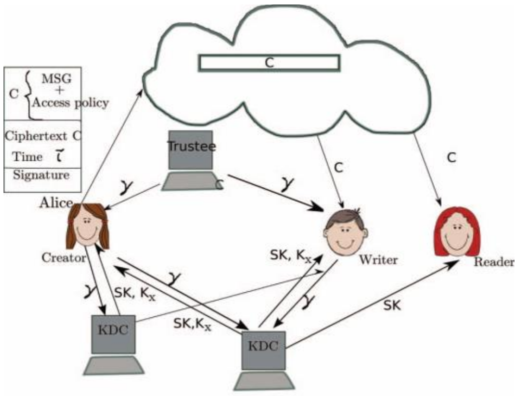

Figure 1: Cloud Architecture

Setup:
This algorithm takes as the input security parameters and attribute universe of the cardinality N. Then it defines a bilinear group of the prime number. It will return a public key and the master key which will keep secret by the authorized party.

Encryption: It takes the messages, public key and set of attributes. It will output a cipher text.

Key Generation: It takes input as an access tree, master key and public key. It will outputs user secret key.

Decryption: It takes input as a cipher text, user's secret key and public key. It first computes the key for each leaf node. Then it will aggregate the results using a polynomial interpolation technique and that returns the message.

B. File Assured Deletion

The policies of a file may be denied under some request by the customer, when conclude the time of the agreement or completely move the files starting with the cloud onto the next cloud nature's domain. The point at any of the above basis exists the policy will be renounce and the key director will totally clears the public key of an associated file. So, no person can able to recover the control key of a repudiated file in future. For this reason only the file is certainly removed.

To recover the data, the user must ask for key supervisor to make the public key. For that, the user should be verified. The key-policy attribute based encryption scheme is used for access the files that has been verified by means of an attribute attached with the files. With the file access control, the files are downloaded from the cloud server will be in the arrangement of read only or write underpinned. Every client has been connected with approaches for every file. So the right client can able to access the right file. For creating file access the key policy attribute based encryption is used.

C. Security Analysis

Security architecture satisfies the security requirements for authentication, integrity and confidentiality, which follows from the employment of the standard cryptographic primitives, namely message authentication code, digital signature and encryption in our system. The fraud can be repudiated only if the client can provide a different representation will knows of from the trusted authority (TA).

III. RESULTS AND DISCUSSION

Its key generation procedure is modified for our purpose of removing escrow. Then the proposed scheme is then built on the new CP-ABE variation by further integrating it into the proxy re-encryption protocol for the user revocation. To hold the fine-grained user revocation, the data storage center should obtain the user access (or revocation) list for each attribute group which is related to TPA permission generated code, since the revocation cannot take effect after all. This setting has the data-storing center knows the revocation list does not violate the security requirements. It is only one allowed to re-encrypt the cipher texts with authentication and can by no means obtain any information about the attribute keys of users only accessed by valid users.

This section gives the details and specification of the hardware on which the system is expected to work. The CloudSim is an advanced tool to simulate the integration of Java coding. The processor will be Dual core 2 GHz with 2 GB RAM and 120 GB hard disk. The Windows XP Operating System used. Java coding are easy to implement and CloudSim is an open source.

IV. CONCLUSION

We have introduced a decentralized access control to secure data stored in cloud, which will gives client renouncement that prevents replay attacks. The cloud server does not know the identity of the any client; however just check the client's certification. It is more secure and fine grained data access control scheme. In this, the key distribution will be carried out in a decentralized manner. One of the limitations is that the cloud knows the access policy for each record stored in the cloud server.

V. REFERENCES

[1] S. Ruj, M. Stojmenovic, and A. Nayak," Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE transactions on Parallel and Distributed Systems, Vol. 25, No. 2, February 2014.

[2] 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.

[3] A.B. Lewko and B. Waters, "Decentralizing Attribute-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.

[4] Mohamed Nabeel, Member, IEEE, Ning Shang, and Elisa Bertino, Fellow, IEEE," Privacy Preserving Policy-Based Content Sharing in Public Clouds" IEEE Transactions on Knowledge and Data Engineering, Vol. 25, No. 11, November 2013.

[5] Changji Wang and Jianfa Luo," An Efficient Key-Policy Attribute-Based Encryption Scheme withConstant Ciphertext Length", Hindawi Publishing Corporation Mathematical Problems in Engineering, Volume 2013, Article ID 810969, 7 pages.

[6] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc.14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

[7] Junbeom Hur and Dong Kun Noh," Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems", IEEE Transactions on Parallel and Distributed Systems, Vol. 22, No. 7, July 2011.

[8] Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng," Attribute-Based Encryption With Verifiable Outsourced Decryption", IEEE Transactions on Information Forensics and Security, Vol. 8, No. 8, August 2013.

[9] Fuchun Guo, Yi Mu,Willy Susilo,Duncan S. Wong, and Vijay dharajan,"CP-ABE With Constant-Size Keys for Lightweight Devices", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 5, May 2014.

[10] Piotr K. Tysowski and M. Anwarul Hasan," Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds," IEEE Transactions on Cloud Computing, Vol. 1, No. 2, July-December 2013.

[11] Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang," Securely Outsourcing Attribute-Based Encryption with Checkability", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 8, August 2014.

[12] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou," Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 1, January 2013. [13]. John Bethencourt , Amit Sahai and Brent Waters," Ciphertext-Policy Attribute-Based Encryption".