ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. IV, Issue IV, April 2018

Secure Data Sharing in Cloud Computing Environment

R.Logesh1, K.Ajithkumar2,V.Maiyurinathan3,V.Vignesh4
1,2,3 UG Scholar, 4Assistant Professor(Sl.Gr)
Department of Information Technology, Sri Ramakrishna Engineering College, Coimbatore

Abstract–Cloud storage is an application of clouds that liberates organizations from establishing in-house data storage systems. However, cloud storage gives rise to security concerns. In case of group-shared data, the data face both cloud-specific and conventional insider threats. Secure data sharing among a group that counters insider threats of legitimate yet malicious users is an important research issue. In this paper, we propose the Secure Data Sharing in Clouds methodology that provides: 1) data confidentiality and integrity; 2) access control; 3) data sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) forward and backward access control. The SeDaSC methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server.

We formally verify the working of SeDaSC by using high-level Petri nets, the Satisfiability Modulo Theories Library, and a Z3 solver. The results proved to be encouraging and show that SeDaSC has the potential to be effectively used for secure data sharing in the cloud.

I. INTRODUCTION

Cloud computing is rapidly emerging due to the provisioning of elastic, flexible, and on-demand storage and computing services for customers [1]. Organizations with a low budget can now utilize high computing and storage services without heavily investing in infrastructure and maintenance. According to Google’s Kevin Marks, the term “cloud computing” comes “from [the] early days in the Internet where we drew the network as a cloud. We didn’t care where the message went… the cloud hid it from us” [2]. The National Institute of Standards and Technology (NIST) has defined cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, e.g. networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction [3]. Cloud computing can provide elastic resources with dynamic provisioning and scaling based on user demands. This approach is intended to deal with both resource over-provisioning, i.e., more resources than needed are allocated, and resource under-provisioning, i.e., fewer resources than required are allocated. The elastic management yields better overall system resource usage and hence increases system efficiency. The cloud model simplifies installation, operation and maintenance of information systems, and reduces costs while increasing system reliability and efficiency. A cloud system is also user friendly, in the respect that it requires less expertise to use. One can draw the analogy with current electricity and running-water systems, where end-users can use services from providers with ease, without being concerned with the technical complexity behind those systems.

ENCRYPTION TECHNIQUES

Some of the encryption techniques used in the existingsystem are discussed and summarized as follows.

A. Attribute Based Encryption (ABE)

Attribute-based encryption is a type of public-keyencryption. In this technique, the secret key of a user andthe ciphertext are dependent upon attributes. Thedecryption of a ciphertext is possible only if the set of attributes of the user key matches the ciphertext attributes.It provides a secure way that allows data owner to share outsource data on untrusted server.

B. Identity-Based Encryption (IBE)

Identity-based systems allow any party to create apublic key from a known identity value such as an ASCIIstring (e.g email id).an Identity based Encryption scenario. A trusted third party called asPrivate Key Generator, which generates the corresponding private keys. To operate, the Private Key Generator first distributes a master public key, and retains the equivalent master private key. Given the master publickey, any party can compute a public key related to theidentity by combining the master public key with the identity value. To achieve a corresponding private key, the party authorized to use the identity ID contacts Private Key Generator, which uses the master private key to create the private key for identity ID. As a result, parties may encrypt messages without prior distribution of keys between individual participants.

C. Proxy Re-encryption

Proxy Re-encryption is another technique that

enables secure data sharing and confidential data sharing in the Cloud. Proxy Re-encryption allows a semi-trusted proxy with a re-encryption key to convert a cipher-text under the data owner fs public key into another cipher-text that can be decrypted by other user fs secret key. A user, Alice, encrypts her data using her public key. Alice sends the encrypted data to a proxy, when she wants to share her data with another user, say Bob. The proxy then converts the data encrypted under Alice fs public key into data that is encrypted under Bob fs public key and sends this to Bob. Bob is able to use his private key to decrypt the cipher-text and reveal the data.

D. Ciphertext-Policy Attribute Based Encryption

In cipher text - policy attribute-based encryption (CP-ABE) a user private-key is related with a set of attributes and a ciphertext define an access policy over a set of defined attributes within the system. A user will be able to decrypt a ciphertext, only if his attributes suit the policy of the respective ciphertext. Policies may be determined over attributes using disjunctions, conjunctions and (k, n)-threshold gates, i.e., k out of n attributes have to be given. For instance, let us assume that the attributes is defined to be {A, B, C, D} and user 1 receives a key to attributes {A, B} and user 2 receives a key to attribute {D}. If a ciphertext is encrypted with respect to the policy (A ÈC) ÉD, then user 1 will not be able to decrypt, while user 2 will be able to decrypt. An advantage of CP-ABE is that the users can get their private keys only after the data has been encrypted with respect to policies.

II.LITERATURE SURVEY

Xinyi Huang et.al [10] (2015) introduced a Identity-based (ID-based) ring signature, which eliminates the process of certificate verification. By providing forward secure ID-based ring signature method security level of ring signature is increased. In this method, if the secret key of any user has been compromised, previous generated signatures of all is included and the user still remains valid. If a secret key of single user has been compromised it is impossible to ask all data owners to reauthenticate their data. It is especially important to any large scale data sharing system and it is very efficient and does not require any pairing operations. The user secret key is one integer, while the key update process requires an exponentiation. This scheme is useful; especially to those require authentication and user privacy. Huang Qinlong et.al [6] (2015) suggested an attribute-based secure data sharing scheme with Efficient revocation (EABDS) in cloud computing. To guarantee the data confidentiality and to achieve fine-grained access control this proposed scheme encrypts data with Data encryption key (DEK) using symmetric encryption method and then encrypts DEK based on Ciphertext policy attribute-based encryption (CP-ABE). The homomorphic encryption technique is used to solve key escrow problem in order to generate attribute secret keys of users by attribute authority in support with key server. This homomorphic encryption technique is used to prevent the attribute authority from accessing the data by generating the attribute secret keys alone. EABDS scheme achieves immediate attribute revocation which guarantees forward and backward security, and less computation cost on users. Advantages of this method are more secure and efficient.

Hong Liu et.al [2] (2015) proposed a shared authority based privacy preserving authentication protocol (SAPA) to address the privacy issues for a cloud storage. Their protocol is attractive for multi-user collaborative cloud applications. The existing security solutions mainly focus on authentication. In SAPA, the shared access authority is achieved by anonymous access request matching mechanism, provides Ciphertext-policy attribute based access control to enable users to reliably access its own data fields and proxy re-encryption is applied to provide data sharing among multiple users. Universal Composability (UC) model is established to prove the SAPA has design correctness. When a user challenges the cloud server to request other users for data sharing, this access request itself may reveal user's privacy. This scheme addresses user's sensitive access related privacy during data sharing in cloud environment and achieves data access control, access authority sharing and privacy preservation. Through the SAPA protocol, authentication and authorization is preserved without compromising user's private information. Xin dong et.al [3] (2014), proposed an effective, scalable and flexible privacy-preserving data policy with semantic security. They used two techniques Ciphertext policy attribute-based encryption (CP-ABE) and Identity based Encryption (IBE) that provided a dependable and secure cloud data sharing service that allows dynamic data access to users. Their scheme ensures robust data sharing, preserves privacy of cloud users and supports efficient and secure dynamic operations which includes file creation, user revocation and modification of user attributes. This scheme also enforces fine-grained access control, full collusion resistance and backward secrecy. Although cloud computing is economically attractive to customers and enterprises, it does not guarantee users privacy and data security. The proposed scheme provides semantic security for data sharing in cloud computing through the generic bilinear group model and also imposes backward secrecy and access privilege confidentiality. The performance analysis of this scheme incurs a small overhead compared to existing schemes. Qiang Tang et.al [9] (2014) suggested a searchable encryption namely multi-party searchable encryption (MPSE). It enables users to selectively permit each other to search in their encrypted data. For worst-case and average-case collusion due to the user status dynamics a security model is considered. He proposed a new scheme with provable security. A security model for MPSE provides stronger security guarantee than that from [11]. In the formulation of MPSE, authorization is approved on index level, for each of her indexes example Alice can make a decision whether Bob can search or not i.e. if all keywords try by authorized Bob then Alice supports authorize Bob to look for a subset of keywords in her indexes as well as the cloud server colluded with Bob can recover the keyword in all Alice's search queries. In this MPSE formulation, expected to be that Alice can find out a problem of single trapdoor search for all indexes that have been authorized by her. Disadvantages of this formulation are If Alice have many key pairs in the index and use them with various peers then it leaks some unnecessary information. In contrast, inverted index structure may not face this kinds of problem, as shown in [12].

Junbeom Hur et.al [7] (2013) stated that, the most challenging issues in data sharing systems is the implementation of access policies and support of policies updates. Ciphertext policy attribute-based encryption method enables data owners to define their own access policies over user attributes and implement the policies on the data to be distributed. Disadvantages of this method are key escrow problem. Junbeom Hur[7] proposed a attribute based data sharing scheme to implement a fine-grained data access control by the characteristic of the data sharing system. In this scheme, Junbeom Hur[7] proposed a escrow-free key issuing protocol which solves the problem of key escrow problem. The escrow-free key issuing protocol is constructed using the secure two-party computation between the data-storing centre and the key generation centre. This scheme improves confidentiality and data privacy in the data sharing system. In this scheme, user revocation on each attribute set can do an immediate, which takes the advantage of the scalable access control given by the cipher text policy attribute-based encryption. Advantages of this method are more secure, fine-grained data access control in the data sharing system, efficient and scalable to securely manage user data in the data sharing system. Ming Li et.al [8] (2012) proposed a novel patient-centric framework and a mechanisms for data access control to Personal Health Records (PHRs), which is stored in semi-trusted servers. The attribute based encryption (ABE) techniques is to encrypt each patient's PHR file to achieve fine-grained and scalable data access control for PHRs. In this scheme, it divides the users in the PHR system into multiple security domains which greatly reduces the key management difficulty for owners and users. By using multi-authority attribute based encryption patient privacy is guaranteed. It's also enables dynamic modification of file attributes or access policies, which supports efficient on-demand user or attribute revocation and prove its security. Advantages of this scheme are both scalable and efficient.

III. DYNAMIC SECURE GROUP SHARING

Zhongma Zhu and Rui Jiang [1] (2016), proposed a secure anticollision data sharing scheme for dynamic groups. The group manager takes charge of user registration and user revocation. Group members are a set of registered users. They will store their own data into the cloud and share them with others. They proposed a secure way of key distribution without any secure channels. The users can obtain their private keys from group manager without any Certificate Authorities, due to the verification for the public key of the user. Since there are no secure communication channels between communication entities, the information can be protected from passive eavesdroppers. The proposed scheme achieved fine-grained access control. This allowed any user in the group to use the source in the cloud and the revoked users cannot access the cloud again after they are revoked. This scheme protects from collusion attack and provides a secured user revocation, so the revoked users cannot get the original data file. It supports dynamic groups efficiently. So, previous users need not update their private keys when a new user joins the group or when a user is revoked from the group. The design goals of this scheme include key distribution, data confidentiality, access control and efficiency. Kaiping Xue [5] (2014) proposed a dynamic secure group sharing framework in public cloud computing environment. This framework combines proxy re-encryption, enhanced Treebased Group Diffie-Hellman (TGDH) and proxy signature together into a protocol. By applying the proxy signature technique, the group leader can give rights to group management to choose one or more groups members, all the session key are protected in the digital envelopes and all the data sharing files are safely stored in Cloud Servers. The improved TGDH scheme is to dynamically modify a group key pair when they are in group ,leaving the group or joining the group as well as its does not require all of the group members been online all the time. Based on proxy re-encryption, most data processing operations can be assigned to Cloud Servers without reveal any private information. Advantages of this proposed scheme is highly efficient and satisfies the security requirements for public cloud based secure group sharing. Xuefeng Liu [4] (2013) proposed a secure data sharing design for dynamic groups in an untrusted cloud. In this design, a user can share data with others in the group without revealing identity privacy to the cloud. Its supports efficient user revocation, which can be achieved through a public revocation list without modifying the private keys of the remaining users, and new users join can directly decrypt files stored in the cloud before their participation. This scheme guarantees efficiency as well as encryption computation costs are constant

IV. CONCLUSION

Data sharing in the Cloud is available in the future as demands for data sharing continue to grow rapidly. In this paper, we presented a review on secure data sharing in cloud computing environment. To reduce the cost data owner outsource the data. Data owner is unable to control over their data, because cloud service provider is a third party provider. The problem with data sharing in the cloud is the privacy and security issues. Various techniques are discussed in this paper to support privacy and secure data sharing such as Data sharing with forward security, secure data sharing for dynamic groups, Attribute based data sharing, encrypted data sharing, Shared Authority Based Privacy-Preserving Authentication Protocol for access control of outsourced data. The study concludes that secure anti collision data sharing scheme for dynamic groups provides more efficiency, supports access control mechanism and data confidentiality to implement privacy and security in dynamic group sharing. There is more scope for future research in the field of secure data sharing for dynamic groups.

In future the proposed methodology can be extended by limiting the trust level in the CS.

This will further enhance the system to cope with insider threats .Moreover the response of the methodology with varying key sizes can be evaluated .

References

[1]. Zhongma Zhu and Rui Jiang, " A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud," IEEE Transactions On Parallel And Distributed Systems, Vol. 27, No. 1, January 2016.

[2]. Hong Liu, Huansheng Ning, Qingxu Xiong and Laurence T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing,"
IEEE Transactions On Parallel And Distributed Systems, Vol. 26, No. 1, January 2015.

[3]. Xin Dong a, Jiadi Yu a, Yuan Luo , Yingying Chen, Guangtao Xue , Minglu Li, "Achieving an effective, scalable and privacy-preserving data sharing service in cloud computing," ScienceDirect journal

homepage: www.elsevier.com/locate/cose computers & security 42 (2014) 151 e1 6 4, Elsevier Ltd 2013.

[4]. Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 6, June 2013. [5]. Kaiping Xue and Peilin Hong, "A Dynamic Secure Group Sharing Framework in Public Cloud Computing," . Citation information: DOI 10.1109/TCC.2014.2366152,IEEE Transactions on Cloud Computing.

[6]. HUANG Qinlong, MA Zhaofeng, YANG Yixian, FU Jingyi and NIU Xinxin, "EABDS: Attribute-Based Secure Data Sharing with Efficient Revocation in Cloud Computing," Chinese Journal of Electronics Vol.24, No.4, Oct. 2015.

[7]. Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing," IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, October 2013.

[8]. Ming Li Member, 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 2012.

[9]. Qiang Tang, "Nothing is for Free: Security in Searching Shared and Encrypted Data," IEEE Transactions on Information Forensics and Security, Vol. 9, No. 11, November 2014.

[10]. Xinyi Huang, Joseph K. Liu, Shaohua Tang, IEEE, Yang Xiang, Kaitai Liang, Li Xu, and Jianying Zhou, "Cost-Effective Authentic and Anonymous Data Sharing with Forward Security," IEEE Transactions On Computers, Vol. 64, No. 4, April 2015.

[11]. R. A. Popa and N. Zeldovich, " Multi-Key Searchable Encryption,"

[12]. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 79–88. [13]. Tim, Mather, SubraKumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise perspective of Risks and Compliance," O'Reilly Media, Inc., 2009.

[14] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, Senior Member, IEEE, "HASBE: A Hierarchical Attribute-Base Solution for Flexible and Scalable Access Control in Cloud Computing" in Proc.IEEE Transactions on Information Forensics and Security, vol.7, No.2, April 2012.

[15] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, Matei Zaharia. A view of cloud computing. Communications of the ACM, Volume 53 Issue 4, pages 50-58. April 2010.

[16] S.Yu, C.Wang, K.Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. IEEE Infocom 2010, 2010, pp. 534– 542.