International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume 2, Issue 12 (December '2016)

PRIVACY RISKS AND SECURE ACCESS CONTROL IN USING CLOUD STORAGE

V.Matheswaran,
M.Phil Scholar,
Department of Computer Science and Applications,
Mahendra Arts and Science College,
Kallipatti,Namakkal.

N.Suresh,
Assistant Professor,
Department of Computer Science and Applications,
Mahendra Arts and Science College,
Kallipatti,Namakkal.

Abstract: In the process of storing data to the cloud, and retrieving data back from the cloud, there are mainly three elements that are involved, namely the client, the server and the communication between them. In order for the data to have the necessary security, all three elements must have a solid security. For the client, it is mostly every user's responsibility to make sure that no unauthorized party can access his machine. When talking about security for cloud storage, it is the security for the two remaining elements that is our main concern. On the server side, data must have confidentiality, integrity and availability. Confidentiality and integrity of data can be ensured both on the server side and on the client side. In this paper we have discussed security around cloud storage.

Keywords: Cloud computing, security, cryptography, resources, storages

I. INTRODUCTION

Cloud computing as a shared pool of configurable computing resources with the capability of storing data and perform the computation remotely was a long vision of computing. Growing data and increasing popularity of cloud computing is a motivation to use data storages or personal and institutional data backups in the cloud. By having the data storages in the cloud infrastructures, users can be relieved from limitation of local data storage. Beside storage functionality, the cloud data storages focus on file sharing and synchronization as well. Generally speaking, cloud data storages have significant benefits, they bring ubiquitous data access (anytime from anywhere with any device) and sharing capabilities without the need of self-managing replication and data backups. In spite of all the advantages delivered by cloud data storage, several challenges are arising for storing sensitive data without compromising user's privacy. The fact that users have no physical possession of their outsourced data and it is stored and processed remotely is hindering the adoption of cloud based data storages. Relying on a corporation to have access to all your personal data is a major concern for many end users. Thus, cloud data storages magnify an essential concern over data security and privacy. Several studies ranked security and privacy as a major area of attention for cloud adoption [1]. Due to privacy leakage and security exploit of major vendors, the end-users prefer local storage for sensitive data over cloud storage [2]. In addition to rising demand of personal data storage, the proliferation of online social networks is another issue to think about. Rapid growth of sharing and storing contents in online social networks become major points of concern for security and privacy issues. The centralized nature of online social networks and service provider ownership of data brings the limitations for users. Thus, it becomes a potential motivation for developing a decentralized network for online social networking. Decentralized social network is a distributed information management platform, such as a network of trusted servers or peer-to-peer systems for social networking. On the other hand, implementation of the personal data storage is one of the key enablers of moving from centralized to decentralized online social network [3].

II.LITERATURE SURVEY

R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M.Kirchberg, Q. Liang, and B.S. Lee,(2013) proposed Potential customer has a lack of trust in the Cloud, where the security and the privacy is been researched to developed in the cloud ,but still there is focuson the accountability and the audit ability. The sheer amount of data revealed from the virtualization and the data distribution is been researched in the cloud accountability. As it has the responsible of customers concern of server health and the utilization in integrity of data and the safety of end user's data. This paper tells the trusted cloud through the detective control and presents the Trust cloud framework which are approached through technical and policy based approach

D.R. Kuhn, E.J. Coyne, and T.R. Weil,(2010) proposed the Role Based Access Control(RBAC) which is a Information security helps to reduce the complexity of the Secure administration and it provides the permission to the user . It is been criticized for the difficulty of setting up an initial role structure and for inflexibility in rapidly changing domains. The Pure RBAC provide inadequate attribute for the user , to provide the dynamic attribute , particulary in large Organization the "Role Explosion" which results in thousands of roles been seprated to use for the different collection of the permission. Thus the attributes and the rules could either replace RBAC or make it simple and flexible

S. Jahid, P. Mittal, and N. Borisov,(2011) proposed it is an approach of privacy risk in the Online Social Network (OSN's) , in which it shifts OSN provider to User by Encryption. This creates a key management and the dynamic groups , to address this problem the author proposed the EASiER an architectural support in Fine grained access

control and the dynamic group by the Attribute based Encryption. It is possible to remove 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

M. Green, S. Hohenberger, and B. Waters,(2011) proposed ABE is only used in cloud storage and many Computing application.The main drawback of the Ciphertext is size of the text and the time required to complexity of the access formula. ABE ciphertexts are stored in the cloud. In which a user can provide the cloud with a single transformationkey that allows the cloud to translate any ABE ciphertext satisfied by that user's attributes into a (constant-size) El Gamalstyle ciphertext, without the cloud being able to read any part of the user's messages. This provide a new secured definitions for both CPA and replayable CCA security with outsourcing ,several new constructions, an implementation of our algorithms and detailed performance measurements. In a typical configuration, the user saves significantly on both bandwidth and decryption time, without increasing the number of transmissions.

III. PRIVACY RISKS IN USING CLOUD STORAGE

Due to the separation between cloud users and their data, there are a number of serious privacy risks with storing information in a cloud. This section examines key privacy risks which can appear due to storage in the cloud.

Jurisdiction: Data in a cloud can potentially be stored, processed, and used in other ways within multiple jurisdictions. However, data protection laws differ in the various jurisdictions. As a result cloud based storage might be a serious threat to sensitive corporate or private data. Moreover, some of the different data protection legislations require that the data have a distinct ownership. However, in some cases it is in practice hard to identify the owner of the data.

Creation of new data: The cloud model has the potential to create and retain a huge amount of new data related to the activities of the cloud user. The creation of such data may raise concerns about the ownership of this data. This secondary data is generated by interactions with a cloud-based infrastructure. Although this data is not the actual data which is stored in a cloud by the cloud user, the ownership of this new data is a subject for debate. For instance, Facebook is storing information about what the users like, who their friends are, what music they listen to, what movies they like, etc., and later related advertisements show up in their profiles. Some might say that data created by interacting with a cloud based infrastructure should be owned by the user who this data concerns and therefore be protected by data privacy legislation and hence not be resold to third parties without the user's explicit permission.

In the report "Reaching for the Cloud(s): Privacy Issues related to Cloud Computing" [4] the Office of the Privacy Commissioner of Canada states that "In the Pew Internet Study, users expressed great concern about the misuse of their data in the cloud 90% were concerned about their data being sold to another organization; 80% expressed concern about their photos or other data being used in marketing campaigns; and 68% said they would be concerned if their data were analysed and used to serve them with targeted advertising". This suggests that the users are becoming more concerned about their data privacy and in some countries there are those who believe that these users' rights should be protected by appropriate legislation. Finally, the secondary data created in the cloud may be personally identifiable information (according to the EU regulation 95/46/EC) and hence subject to restrictions. Additionally, individuals might be unaware of the existence of this data.

Securing the data: The Internet is not a safe place for sensitive private data to travel. Additionally the cloud model does not define what security measures should be taken in order to secure the data while it is inside the cloud. All security related decisions depend upon the specific policies and actions of each CSP. This raises security risks both in the protection of data and in the safeguards applied to this data. According to [20], recent studies show that CSPs have tended to provide their services without strong security solutions. However, Christopher Soghoian recommends that CSPs should use the kind of encryption which is currently used by on-line banks. Moreover, data protection should be applied to data at rest, in transition, and while processing it.

Lawful access: Cloud computing raises additional concerns when the private data in the cloud has to be accessed by the government, its agencies, etc. For instance a lawful access request can target a certain individual or a company whose data is stored in the cloud. However, if there is data which belongs to multiple data subjects, this data may also be exposed. This actually raises four privacy risks. First, the court order or other lawful access request may result in access to information above and beyond what was intended. Second, the CSP client who is not the target of the lawful access request might be unaware of the possible data intrusion and might never be informed of this intrusion. A third risk is that the target of the lawful access request might also never be aware of the intrusion. A fourth risk is that the government agency which receives this information might not securely handle the data or they may retain the data for longer than it should be retained.

Misuse of processing data: The CSP should be bound to the privacy requirements equal to those used within the organization whose data is going to stored or processed in the cloud. A CSP must ensure that access and modification procedures are possible and that deletion procedures are adequate and appropriate. These procedures and privacy requirements are important because there is a possibility that a CSP might access, manipulate, or mine data in an inappropriate way [5]. In that case, regulators may have to distinguish whether the data were processed for a specified purpose or purposes in order to know which regulations or laws are relevant.

Permanence of data: In the contract between an organization or a person and a CSP there should be a

statement of what measures will be taken to ensure that the data is protected while it is held in the cloud by the CSP. However, there is a security and privacy risk to the data when the contract expires. Methods should be introduced to securely remove the customer's data from the cloud infrastructure. A client should be acquainted with what will happen to his data after the end of the contract and within what time period these operations are guaranteed to be carried out. Moreover, in Megaupload's case [6] customers' data is no longer accessible to these customers since some of them violated copyright law. All 25 PB of data residing in the data center is seized by the law enforcement authorities and is not available even to those customers whom did not violate copyright law. From the perspective of the data center this case brought a huge financial loss since the government is not willing to pay for operational costs of data retention and it does not allow deleting that data.

IV.SECURE ACCESS CONTROL IN CLOUD

Cryptographic Basics: PRE and ABE are two important cryptographic techniques which are highly related to our work. In order to best understand the PRE and ABE, we will briefly introduce them below. We firstly introduce the bilinear map that is the basic of ABE. Notably, knowledge of basic mathematics, such as finite fields, groups and elliptic curves, are required to understand the cryptographic algorithms. However, an extensive introduction of these areas is beyond the scope of this thesis.

Bilinear map : Bilinear map, or bilinear pairing, is a basis of many cryptography paradigms. There are different definitions of bilinear map, depending on the type of group and elliptic curve. Generally speaking, a bilinear map is an operation that combines elements of two groups to yield an element of a third group. Here we outline two commonly used definitions of bilinear map that are proposed by Boneh, Franklin and Lynn [33].

Symmetric pairing:

Definition : Let , be cyclic groups of large prime order , and be a ring of integers modulo. Let be a generator of . A bilinear pairing or bilinear map is an efficiently computable function:

$$e:G \times G \rightarrow G_T$$

such that Non-degeneracy: e(g,g)<>1 The map does not send all pairs in GxG to the element in G_T If is a generator of G then is a generator of G_T

(i) Bilinearity: $e(g^a,g^b)= e(ga,gb)^{ab}$ for all . a,b ∑ Z_p The symmetric bilinear map is the original and simplest abstract definition of the pairing, and it is completely defined by the value it takes at $^{t\ e}$ (g,g) . The Diffie-Hellman problem [9] can be solved in the bilinear map, since given $g,g^x,g^y.g^z$, by Bilinearity and nondegenracy z=xy if and only $ifg(g,g^z)=e=g^x.g^y$. However, symmetric pairings can only be instantiated by using suitable super-singular elliptic curves.

Asymmetric pairing:

In order to allow a wider range of curves to be used, the asymmetric pairing looses the definition of symmetric pairing.

Definition: Let G^1,G^2,G^T be cyclic groups of large prime order . Assume the Diffie-Hellman problem is hard inG_1.Let ϕ: G_2-> G_1 . Let : be an efficiently computable group isomorphism. Let be a generator of G2. Set g_1= ϕ (g_2) (g_1 is the generator of G_1.) A bilinear pairing is an efficiently computable function: $e:G_1xG_2\text{-->}G_T$

such that

(i) Non-degeneracy: $e(g_1,g_2 \# 1..)$.

(ii) Bilinearity: $e(g_1^a, g_2^b) = e(g_1, g_2)_{ab}$foralla, b E Z_p

This modified definition allows a greater variety of pairings to be used on ordinary curves, and security proofs require only minimal changes because of the map Ø . However, there is a problem with hashing in this definition. It turns out that there is no known method to hash to an element of G_2 such that its discrete log to some fixed base is unknown. This issue can complicate the design of some cryptosystems, and make the system designers give up asymmetric pairing in some cases.

V.THE PROPOSED SCHEME

In this scheme, we proposed multi-dimensional control on cloud data access based on individual trust evaluated by the data owners, and/or public reputation evaluated by one or multiple RCs. To be more concretely, a data owner firstly encrypts its data with a symmetric key DEK, and then the data owner can divide the DEK into several segments K0, K1, K2… Kn, Kn+1 . K0, K1, K2… Kn are encrypted with public keys from different RCs which are employed to evaluate reputations and control data access Kn+1. can be encrypted with a public key PK_TL which is related to individual trust levels. After the data encryption, the data owner uploads the encrypted data and key segments to the CSP, and specifies the access policy to each of the RCs. In order to access data, a user needs to be authorized by all the RCs, and collect all key segments to recover the DEK for decryption.

The size of the key segments K0, K1, K2… Kn can be flexibly set by data owners, according to different application scenarios or security requirements. If a data owner would like to control data access only by itself, the symmetric key DEK will not be divided, and is encrypted with a public key PK_TL which is related to individual trust levels. If a data owner would like the RCs to the control data access, all the key segments are encrypted with the RCs' public keys. User revocation is achieved by applying a blacklist which contains the ID of non-trusted or non-eligible users. The blacklist is managed by the CSP, and can be updated according to RC or data owners' notification and feedback.

Scheme algorithms:

The scheme consists of four main algorithms: Key generation, Symmetric key DEK division and combination, PRE, modified CP-ABE which is proposed in [6].

Key generation: Key Generation contains three kinds of keys: Symmetric key DEK for data encryption, public key pairs for PRE, and key pairs for CP-ABE. The key generation for CP-ABE consists of system public key PK, master key MK, user public key pairs and Individual Trust public key and secret key. The key generation can be conducted by users or by a trustworthy user agent.

Symmetric key DEK division and combination: Key division is operated by the data owner based on its data access control policy. The symmetric encryption key DEK is divided into n+1 parts, where n is the number of RCs which are employed by the data owner to control its data access based on the access policy. Key combination is operated by the user who receives all pieces of the symmetric key DEK, and aggregates all partial keys together to get a complete key DEK for decryption.

PRE: The data owner encrypts n pieces of partial symmetric key DEK using corresponding RC's PRE public key, and stores the encrypted data and key files in the CSPs. The RCs control data access right by evaluating the access policy and users' reputation, and conduct re-encryption key generation if a user is eligible for accessing the data. The CSPs conduct the re-encryption and send the re-encrypted data to the user.

CP-ABE: CP-ABE is applied for the purpose of integrating the individual trust level (TL) into the data access control mechanism, and controlling access right by the data owner itself. One piece of symmetric key DEK is encrypted using the data owner's Individual Trust public key, and is stored in the CSPs. After verifying the individual trust level of a user who requires the data, the data owner will then issue the user an Individual TL secret key, and inform the CSPs to send the encrypted data to the user.

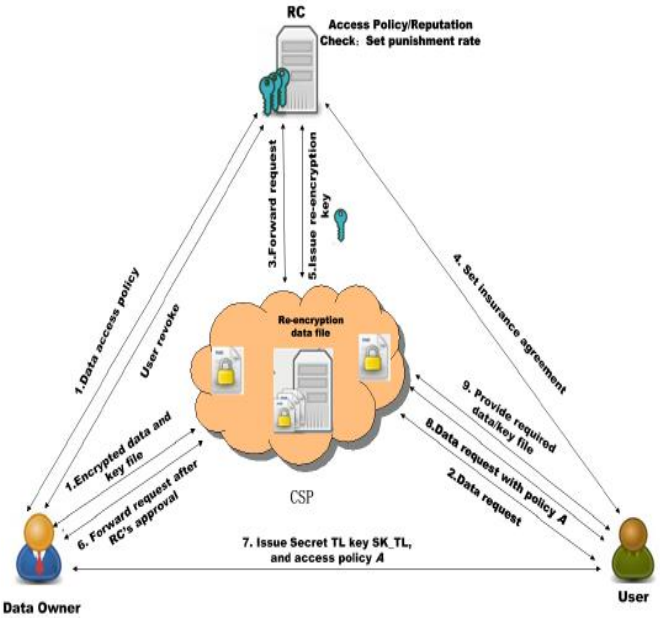

Figure 1 Procedure of cloud data access control based on heterogeneous scheme

Step 1: The data owner encrypts its data using a symmetric key DEK, and divides the DEK into two segments: K_O and K_1,K_o is encrypted with the RC's public key pk_RC, and $K_1$is encrypted with a public key PK_TL which is related to individual trust levels. The encrypted data is denoted as E(DEK, data), and the key segments are denoted as E(pk_EC,K_o) and E(PK_TL,K_1)Then the data owner uploads the encrypted data to the CSP, and specifies an access policy to both the CSP and RC.

Step 2: The user sends an access request to the CSP, and waits for responses.

Step 3: The CSP verifies the user's ID and checks the blacklist in order to decide whether to forward the access request to the RC. If the user's ID is valid and it is not in the blacklist, the CSP will forward the request to the RC. Otherwise, the request is rejected.

Step 4: The RC evaluates the user's reputation, and decides if the user meets the access policy. If the user is eligible, the RC will set an insurance agreement with the user in case of illegal data disclosure. Otherwise, the request is rejected.

Step 5: The RC issues the re-encryption key rk_RC->u=RG(sk_RC, pk_u), in which RG(sk_RC, pk_u) is the re-encryption key generation function, based on the RC's own private key sk_RC and user's public key pk_u.

Step 6: After receiving the re-encryption key rk_RC from the RC, the CSP forwards the access request to the data owner.

Step 7: The data owner evaluates the user's trust level TL based on previous behaviors and activities. If the user is trustworthy, the data owner issues a secret key SK_TL based on the user's trust level TL, and also sends corresponding access policy A . Otherwise, the request is rejected.

Step 8: After receiving the secret key SK_TL and access policy A from the data owner, the user again sends a data access request along with the access policy A to the CSP.

Step 9: The CSP checks if the access policy from the user is the same as that received from the data owner. If both of the policies match, the CSP conducts the ciphertext re-encryption R (rk_RC->u, E(pk_RC,K_o))= E(pk_u,K_o)and sends E(DEK, data), re-encrypted data E(pk_u, K_o) and E (PK_TL,K_1)to the user.

VI.CONCLUSIONS

In this chapter, we present the conclusions of this thesis, and propose several improvements for the future works. To protect the data and privacy from disclosure, a number of schemes have been proposed for data access control in cloud computing. Before applying an access control scheme in a practical system, it is indispensable to evaluate its performance in various aspects, such as efficiency and flexibility. Reputation and individual trust can be an effective method to control data access in cloud computing, and also for choosing CSPs with better performances. It can be applied in combination with cryptographic algorithms, and help to reduce the computational cost.

REFERENCES

[1] Dan Hubbard and Michael Sutton. Top Threats To Cloud Computing. Tech. rep.

[2] Iulia Ion et al. "Home is Safer Than the Cloud!: Privacy Concerns for Consumer Cloud Storage". In: Proceedings of the Seventh Symposium on Usable Privacy and Security. SOUPS '11. Pittsburgh, Pennsylvania: ACM, 2011, 13:1–13:20. ISBN: 978-1-4503-0911-0. DOI: 10.1145/2078827. 2078845. URL: http://doi.acm.org/10.1145/2078827.2078845.

[3] Anwitaman Datta et al. "Decentralized Online Social Networks". In: Handbook of Social Network Technologies and Applications. 2010, pp. 349–378. DOI: 10.1007/978- 1-4419- 7142- 5_17. URL: http://dx.doi.org/10.1007/978-1-4419-7142-5_17.

[4] M.Alhamad, T.Dillon, E.Chang, "SLA-Based Trust Model for Cloud Computing", 2010 13th International Conference on Network-Based Information Systems, Sept 2010, IEEE P.321, E-ISBN 978-0-7695-4167-9.

[5] W.J.Li, L.D.Ping, X.Z.Pan, "Use trust management module to achieve effective security mechnisms", 2010 International Conference on Electronics and Information Engineering, Aug 2010, IEEE P.v1-14, E-ISBN 978-1-4244-7681-7.

[6] H.Sato, A.Kanai, S.Tanimoto, "A Cloud Trust Model in a Security Aware Cloud", 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet, July 2010, IEEE P.121, E-ISBN 978-0-7695-4107-5.

[7] A.Sahai, B.Waters, "Fuzzy identity-based encryption", in Proceedings of the 24th annual international conference on Theory and Applications of Cryptographic Techniques, Berlin 2005, Springer P.457, ISBN 3-540-25910-4 978-3-540-25910-7.

[8] C.Wang, Q.Wang, K.Ren, W.J.Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", 2010 IEEE Proceedings of INFOCOM, San Diego March.2010, IEEE P.1, ISBN 978-1-4244-5836-3.

[9] C.Wang, N.Cao, K.Ren, W.J.Lou, "Enabling Secure and Efficient Ranked Keyword Search over Outsourced Cloud Data", IEEE Transaction on Parallel and Distributed Systems, Volume 23, Issue 8, Dec.2011, IEEE P.1467, ISSN 1045-9219.

[10] C.X.Leng, H.Q.Yu, J.M.Wang, J.H.Huang, "Securing personal health records in the cloud by enforcing sticky policies", TELKOMNIKA Indonesian Journal of Electrical Engineering, Volume 11, Number 4, 2013, P.2200, DOI 10.11591/telkomnika.v11i4.2406.

[11] S.Narayan, M.Gagne, R.Safavi-Naini, "Privacy preserving EHR system using attribute-based infrastructure", in Proceeding of 2010 ACM workshop on Cloud Computing Security, New York 2010, ACM P.47, ISBN 978-1-4503-0089-6.

