I J C T A, 9(11) 2016, pp. 5263-5270

PERSONAL DATA ACCESS CONTROL BASED ON TRUST AND REPUTATION IN CLOUD COMPUTING

Priyanka Thakur[*], Ravishanker[**] and Dr. Ashish Kr. Luhach [***]

Abstract: The technical limitation of a personal computers system e.g. hard disk failure forces enabled the user to stores their application data on cloud, along with images, videos or highly sensitive data. In the last decade cloud computing has been widely developed in context to provide security along with data access to user. The major security issue in cloud computing is that the semi-trusted cloud service providers also possess the data access control. Due to semi-trust, the user stores their personal data in encrypted form, but in critical condition such as personal healthcare records of a patient needs to be accessed by doctors immediately but it need the data owner to be online in order to give access to the data. In this paper data protection scheme is proposed which enable the confidentiality, integrity of data and authentication. The proposed scheme verifies the integrity of data and computes the trust level of the data requester. Later the trust value is computed using multi-factor authentication for data owner and the users also using the mobile social networking and social networking.

Key Words: Access control, Reputation, Trust, Auditing, Cloud Computing, Mobile social networking.

1. INTRODUCTION

Internet is a global information system network technology which provides a way to interact with people using social network, commit e-commerce transactions and exchange the information. Cloud is a combination of different resources (like computing, storage and various types of services) and provided the platform as per the requirement of the user. By providing services at lower cost, cloud computing attracts the people. The cloud platform provides the user promising services with properties such as fault tolerance elasticity, pay-per-use and scalability to users. If one cloud service provider (CSP) cannot provide the services required by the user than other CSP will collaborate together for fulfill the requirements [1].

Data privacy is the main concern in cloud computing as the user cannot trust the cloud completely due to semi-trust. To reduce the computing and storage burden from mobile devices, users store their personal and private information on the data center offered by the CSP. An example is user stores his personal health records on the data center provide by the CSP. The data owner must prefer to share his personal information only with trust worthy users, so any modification with personal information may risk the user. The data security issue due to semi-

[*] Department of Computer Science and Engineering, Lovely Professional University, Punjab, India
thakurpriyanka1994@gmail.com

[**] Department of Computer Science and Engineering, Lovely Professional University, Punjab, India
ravishanker20@gmail.com

[***] Department of Computer Science and Engineering, Lovely Professional University, Punjab, India
ashishluhach@acm.org

trusted CSP can be mitigated by providing a secure mechanism to control the access to personal data [2].

Various techniques are proposed for enhancing data security. The cloud cannot be trusted by the users completely because the users do not know the location of the stored data. As the cloud is known to be dynamic in nature, there are chances of data breaches, so the data security needs to be enhanced. The factors required to enhance the security requirements for cloud environment are as follows:

- Security from Service Provider: In order to keep the data safe at server side, the data is encrypted before storing it in the cloud.
- Access Control**:** A proper access control mechanism is required to control the access of user data by semi-trusted CSPs.
- User Identity Validation: Weak username and password cannot verify the valid user as they are easily estimated; even strong passwords don't provide the required security. Hence, a proper identification method is required to verify the validity of the user.
- Identify Honest Client: Identify the trust worthy clients who wants to access the data.
- Log based systems: To enhance the data security service providers are required to maintain proper logs.
- Trust: There should be a proper scheme to evaluate the trust on CSP and third party.
- Disaster Recovery: There should be a solution to protect the data from natural disaster.
- Fraud Control: For sharing the data with other users, there must be proper verification of users [3].

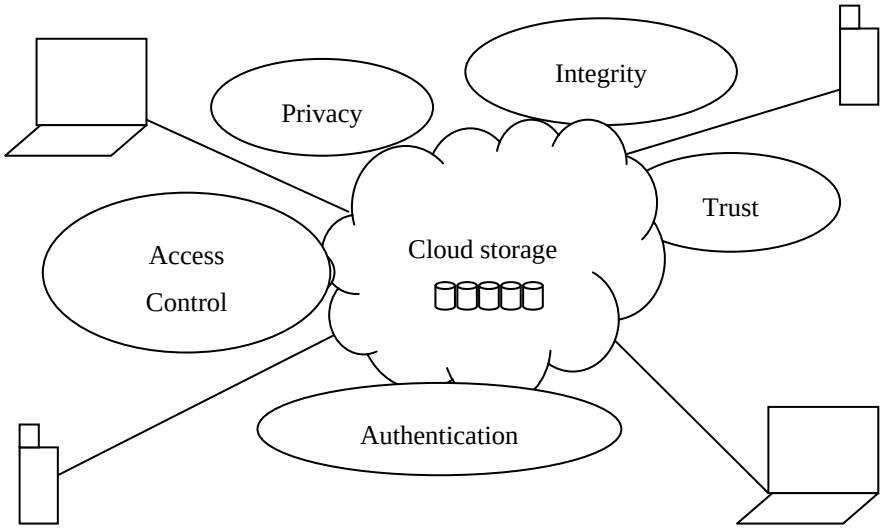

Figure: 1 Security issue in Cloud

This paper proposes a data protection scheme for checking data integrity, assessed the trust based on mobile social networking and provides secure access to data. It also checks for authentication of users. A reputation authenticator is introduced which verifies the integrity of outsourced data without retrieving the whole data. Reputation system helps in building a mutual trust relationship between cloud platform and users; required to implement enhanced data access mechanisms in cloud. Nowadays, a number of reputation management systems are available [4]. Yan et al.'s [5] proposed a work that is based on the trust number of services composed together

and the services are selected on the basis of reputation. Yan et al.'s [2] evaluate a social trust relationship level to access the personal data. On the basis of Quality of Service and feedback, the trust of an entity is evaluated by reputation centre in Yan et al.'s [6].

2. RELATED WORK

Personal data uploaded on cloud can be for individual or organization or for a particular group of users, allowing the cloud or reputation center to manage and maintain the data. Rather than fully trusting the cloud and reputation center. A timely check is performed on the data stored at the cloud for ensuring data integrity and privacy.

Ateniese et al.'s [7] proposed a PDP (Provable Data Possession) mechanism which utilizes the Homomorphic authenticator method based on RSA for protecting the data stored in cloud. A public auditing scheme which utilizes a trusted third party is introduced for checking data integrity without the retrieval of whole data. Dynamic operations performed by cloud on data are not considered in this scheme. Wang Q et al.'s [8] propose a scheme which supports fully dynamic data operations. It combines the homomorphic linear authenticator and Merkle hash tree and check the data in a distributed manner. However, this scheme cannot provide the data privacy against non-trusted CSP and third party. Nirmala et al.'s [3] proposes a User Authenticator scheme which utilizes an encrypting mechanism for checking data integrity without using any third party auditor. A scheme is proposed by Kim et al.'s [9] which use a Homomorphic hash function and a random value to provide data privacy from TPA and cloud. The scheme [12] provides fully dynamic auditing but increases the cost of computation.

A trust model is proposed by Shaikh et al.'s [10] which measure the security strength of cloud computing service. Cloud services security can be enhanced by using the model as a benchmark to improved the cloud infrastructure or find the limitation of the CSP. Trust model helps the user for selecting the services provided by cloud. Yan Z. et al.'s [2] proposed a method which evaluates the trust of user using the mobile social networking to provide the access to data. At CSP the personal data access is controlled by calculating an entity trust is on the basis of behaviors, experiences, and mobile social activities (weight age of calls between users or message, emailing). But it needs the data owner to be online while providing the access. Yan et al.'s [6] again introduced a scheme which utilizes a proxy re-encryption technique for reducing the access risk to personal data and can provide the access without the data owner. A number of RC's are used to evaluate the trust of each entity. On the basis of user requirement CSP combine the private, public cloud to fulfill the required requirements. However, it does not consider the integrity of data. Yan et al.'s [6] proposed a scheme which evaluates reputation access and trust relationship on the basis of mobile social networking, behaviors and activities or on performance in different contexts. To provide the data access, it utilizes proxy re-encryption and Attribute-Based Encryption. Cryptographic system is integrated with reputation evaluation and context-aware trust for supporting different scenarios and control strategies. However, it does not consider the data integrity and authentication. Yan et al.'s [11] show control the personal data access based on RC over cloud most existing Reputation system did not consider.

Different scheme was introduced for providing the data integrity, privacy and authentication against the data. Many schemes do not provide the dynamic data operation, privacy against the semi-trust CSP and authentication. Proposed scheme provide an enhancement for protection of data, a reputation center is used for the verification of data integrity, authentication of user and also enhance the evaluation of trust relationship. CSP collaborate the public and private cloud fulfill the user requirement. There can be number of Reputation center which can be used to protect the unauthorized access and verify the integrity of data.

3. PROPOSED METHODLOGY

Proposed scheme provide a solution for the problem of data integrity and secure data access in the cloud environment. It introduces a Reputation authenticator for auditing and preserving data integrity. To secure the data access control, trust level is evaluated on the basis of mobile social networking and authentication.

Authentication

Table 1
Notations Used For Authentication

U_i	User ID
P_i	Password of user U_i
Em_i	Email user register with U_i
$P_{n.}$	Phone Number register with U_i
RC	Reputation Center
MAC_i	MAC address of U_i
C	Cloud
SQ_i	Security Question U_i for security purpose
$IMEI_i$	International Mobile Equipment Identity of U_i device
T	Timestamp
IP_i	Register IP with U_i
tv_i	Trust value of U_i calculated by the RC and data owner
OTP	One Time Password
K_s	Session key generated between RC and U_i
$K_{0,}k_1$	K divided into two parts
puk_RC	Public key of RC
puk_tv_i	Trust value public key of U_i
pk_RC	Private key of RC
pk_tv_i	Private key of U_i trust
TL	Trust level
AP_i	A Access policy set by the user(e.g. set a priority list who can access directly, set a blacklist with whom user does not want to share the data)

Login or Register with Password

Step 1: If the user is new, register with his credentials (U_i, $P_{i,}$ Emi, and Pn). Enter credentials also stored in RC. Whenever a user login, entered credentials (U_i, $P_{i)}$ is sent to RC for verification. User is also required to select a security question (SQ_i) which is stored with the server and RC.

Key Generation

Step 2: A TLS connection is established between Data owner and RC. A session key (k_s) is generated and sends to data owner by RC.

Step 3: Data owner encrypted his data with k_s.

Step 4: Data owner divides the k into two parts: K_0 and K_1.

Step 5: Encrypt the K_0 with public attribute puk_tv_i with regards to evaluated individual trust and K_1 with puk_RC and

Step 6: Data owner upload the encrypt key of k_1 and K_0 with data in the cloud.

Step7: When a user requests to access data, the request goes to CSP. CSP check its blacklist, if user is not present in the blacklist, then CSP sends the user request to RC. RC verified the user TL. If user tv satisfies the access policy, then RC provides the pk_RC and pk_tv_i of K_1 and K_0 to user. User decrypts the keys K_0 and K_1.

Step 8: User combines the K_0 and K_1 and decrypts the data.

Reputation Center

Step 1: Whenever a user login server send credentials to RC, RC stores the credentials in the database.

Step 2: Each time user login server request to RC, RC verified if the user is authenticated or not.

Step 3: If the user is authenticated, RC checks its trust level and instruct server to provide the access.

Trust level

When a user wants to access the data, RC check its trust level and provide the services/access based on the trust level. Data owner provides access policy to RC.

Table 2
Notations used for Trust Evaluation

$C_{n(i,j)}$	Number of calls made between U_j and U_i
$M_{n(i,j)}$	Number of message send by U_j to U_i
$F_{(i,j)}$	Is U_j add in social networks site of $U_{i.}$
$pl_{(i,j)}$	The priority level of U_j set by $U_{i.}$ in its access list
Thr	Threshold value
AC_j	Number of time U_j access to the cloud
UAC_j	Number of time unauthorized access attempted by U_j to the server

Trust level evaluation is divided in three phases i.e. low level, medium level and difficult level. In low level, when a user (U_j) login with same device and IP or MAC address, and want to access the personal data of U_i. RC checks its trust level and provides the access based on trust value. If calculated trust value (tv_j <= thr) [2], access is provided according to the access policy set by the data owner. In medium level, if a user logs-in with different IP and MAC address or IMEI number, then RC checks its trust level and provide the access according to the evaluated trust. In difficult level, when a user login with its $U_{i,}$ RC checks its previous session connectivity. If in the previous

session U_i is not logged-out, then RC send this information to Cloud and Cloud ask for the OTP and SQ_i.

Integrity Verification

The proposed scheme utilizes a reputation authenticator for auditing and verification of data.

We assume that n blocks are created by dividing a file F. Advanced Encryption Scheme (AES) is used to encrypt each block. A symmetric key is chosen for the encryption of data. Data encryption using symmetric key helps in providing the data confidentiality. Add a unique random number with the encrypted file and use SHA (Secure Hash Algorithm) to generate hash string. Then digital signature is attached with each encrypted hash codes to ensure the integrity. Data owner store the index table, unique number and hash value. After storing the data on the cloud, data owner deletes the data from his system and send the index table, unique number, hash value to RC. RC evaluates the trust level of CSP based on performance monitoring or public feedback [6],[1]. RC verifies data integrity whenever new data is inserted or deleted from the cloud. The steps needed to be followed by data owner while storing the file in a cloud are:

Step 1: Divide data file (F) in blocks m_1 ,m_2 , m_3 …….. m_n .

Step 2: A session key (K_s) is generated using a TLS connection between Data owner and RC.

Step 3: Encrypt each data block using AES ⟶ (F').

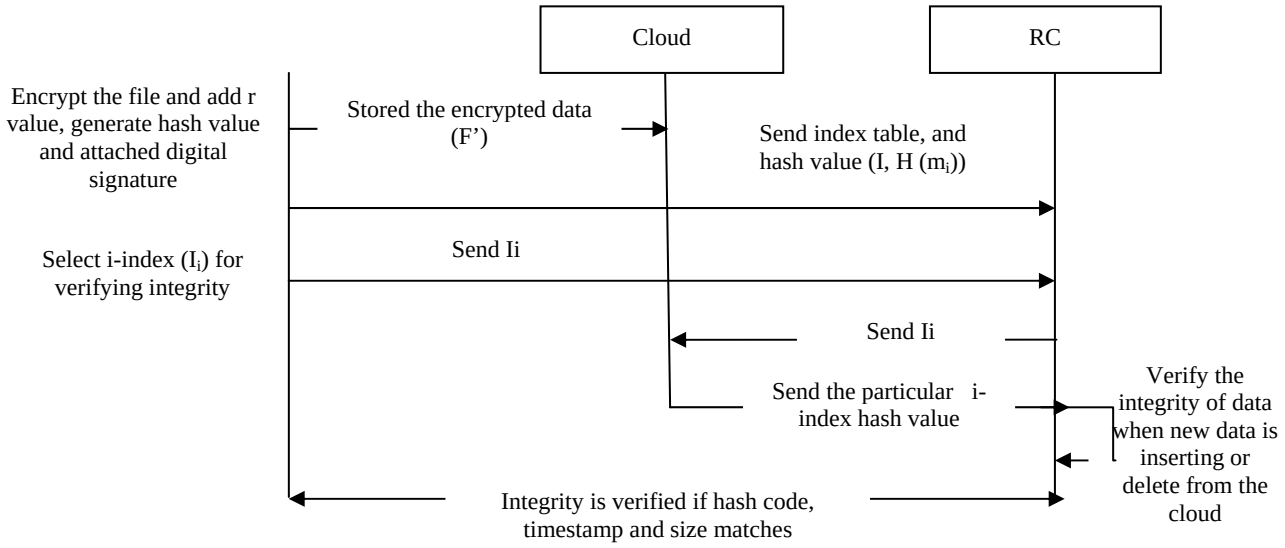

Figure 2: A procedure of Integrity Verification

Step 4: Combine a unique random value ((F'+ r) ⟶ F") and use SHA to compute hash string for each encrypted block.

Step 5: Generate_Digital_Signature (K_s, F): Given F = (m_1,m_2, m_3,…….. m_n), client computes a signature for each block as sig_i ⟶ $(H(m_i)t^{m}{}_{i})^{sig}$

Step 6: Copy of data index table (I), hash value (H (m_i)), timestamp, signature (ds_i) and K_s are sent to RC.

Step 7: User send an auditing request, select i-index (I_i) and send to RC.

Step 8: RC send verification (I_i) to cloud and ask for the particular index data block hash value.

Step 9: Cloud compute the hash value with random value of particular i-index and send to RC.

Step10: RC and data owner match the retrieved hash code.

Step11: On the user end when data is decrypted, digital signatures generated and send to RC.

Step12: RC verified the integrity if hash code, timestamp signature is match.

In recent years, significant growth in E-commerce industry is recorded. Issues related to security and confidentiality has also been increased simultaneously. The easy availability of internet and computer systems leads to growth of large number of trained and equipped intruders which are becoming a threat in the growth of E-commerce industry[13][14]. Similar cases are happening in cloud computing aspects and integration of the proposed techniques can be applied on all these area.

4. CONCLUSION

This research paper focused on a security lifecycle model which is proposed to secure the personal data access at CSP. The propose scheme provides confidentiality, integrity and authentication of personal data. A reputation authenticator is use for verifying the data integrity. CSP will combine the private, public cloud to fulfill the user requirement. On the basis of different login data collected by the RC, it checks the trust level and evaluates the trust value of each user. RC will authenticate the user and accordingly CSP will provide the data access to user. Propose scheme also enhances the security level required for the authentication by using the user's ip address and device unique address (MAC address or IMEI). The previous session of the user is automatically logged out in case the user accesses the account from other than the trusted device. The proposed technique can be implemented with many other technologies as well like internet of things. In future, the factors required for evaluating the user's trust value for authentication can be enhanced.

References

[1] Z. Yan, Xueyun Li, M. Wang, and A. Vasilakos. "Flexible Data Access Control based on Trust and Reputation in Cloud Computing."

[2] Z. Yan, X. Li, and R. Kantola. "Personal data access based on trust assessment in mobile social networking." In Trust, Security and Privacy in Computing and Communications (TrustCom), 2014 IEEE 13th International Conference on, pp. 989-994. IEEE, 2014.

[3] V Nirmala, R. K. Sivanandhan, and R. Shanmuga Lakshmi. "Data confidentiality and Integrity Verification using user Authenticator scheme in Cloud." In Green High Performance Computing (ICGHPC), 2013 IEEE International Conference on, pp. 1-5. IEEE, 2013.

[4] Z. Yan, ed. Trust Modeling and Management in Digital Environments: From Social Concept to System Development: From Social Concept to System Development. IGI Global, 2010.

[5] Z. Yan, "A comprehensive trust model for component software." In Proceedings of the 4th international workshop on Security, privacy and trust in pervasive and ubiquitous computing, pp. 1-6. ACM, 2008.

[6] Z. Yan, Xueyun Li, and R. Kantola. "Controlling Cloud Data Access Based on Reputation." Mobile Networks and Applications 20, no. 6: 828-839, 2015.

[7] A.Giuseppe, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song. "Provable data possession at untrusted stores." In Proceedings of the 14th ACM conference on Computer and communications security, pp. 598-609. Acm, 2007.

[8] W. Qian, C. Wang, K. Ren, W. Lou, and J. Li. "Enabling public auditability and data dynamics for storage security in cloud computing." Parallel and Distributed Systems, IEEE Transactions on 22, no. 5: 847-859, 2011.

[9] D. Kim, H. Kwon, C. Hahn, and J. Hur. "Privacy-preserving public auditing for educational multimedia data in cloud computing." Multimedia Tools and Applications 1-15, 2015.

[10] R. Shaikh and M. Sasikumar. "Trust Model for Measuring Security Strength of Cloud Computing Service." Procedia Computer Science 45, 380-389, 2015.

[11] Z Yan, ed. Trust Management in Mobile Environments: Autonomic and Usable Models: Autonomic and Usable Models. IGI Global, 2013.

[12] Y. Zhu, H. Wang, Z. Hu, G. Ahn, H. Hu, and S. S. Yau. "Dynamic audit services for integrity verification of outsourced storages in clouds." In Proceedings of the 2011 ACM Symposium on Applied Computing, pp. 1550-1557. ACM, 2011.

[13] A.K. Luhach, S.K. Dwivedi, and C.K. Jha, Implementing the Logical Security Framework for E-Commerce Based on Service-Oriented Architecture. In Proceedings of International Conference on ICT for Sustainable Development (pp. 1-13). Springer Singapore. 2016.

[14] A.K. Luhach, and R. Luhach, "Research and implementation of security framework for small and medium sized e-commerce based on soa." Journal of Theoretical and Applied Information Technology, 82(3), 2015.