Application of Private Key Storage by Data Integrity and Confidentiality In Cloud Security

[1]Nemilidindi Anantharami Reddy, [2]Annabattina Harish
Assistant Professor, M.Tech Scholar
Department of Computer Science and Engineering,
QIS College of Engineering &Technology, Ongole, Andhra Pradesh

Abstract:

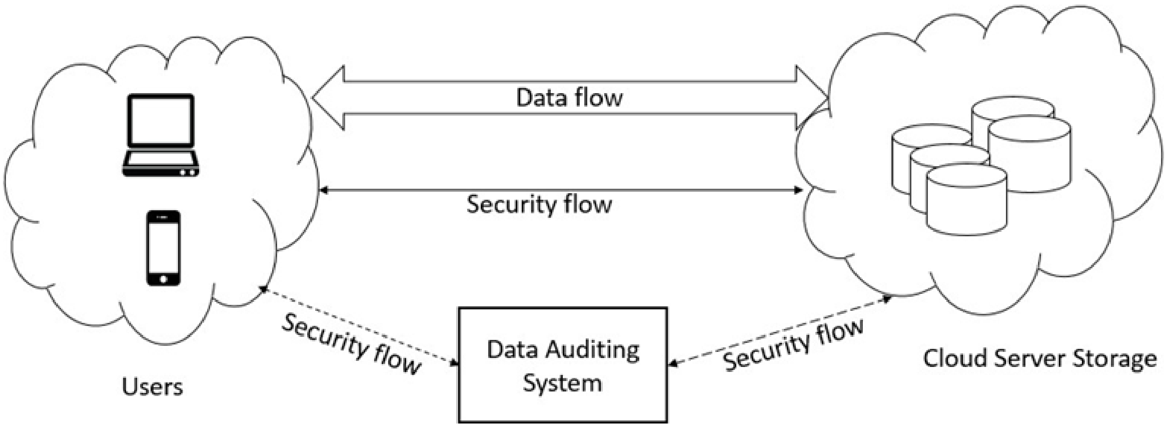
The current generation users are tentatively seen more in uploading their data using cloud based technologies and lessening the storage of copies locally. Cloud users cannot absolutely trust cloud service providers and ensure the integrity of users' with shared data by the cloud storage environment. Everyone approves that Cloud Storage is the best pertaining to hotspots. The present study is to enhance a complete report on secure and efficient sharing of data through dynamic user groups. The operation moves with server as a platform enabling convenient and demand over network accessing a shared pool of configurable server resources (Memory, Networks, Storage, CPU, Applications, and Services) that rapidly provide provision and release by interactions of cloud service providers. Cloud servers source data security to major barriers of storage and their adoptions. Users store large data and use applications on demand. The user identity tracks the addition and deletion of dynamic group users. A new role distributes and protects the privacy. Third party audit is used to verify data integrity. It helps determining specific users a fair audit. The users send encrypted data to the cloud and tag the Rights Distribution Center (RDC) using intuitive gestures of data blind technologies. Security of the schemes is proved experimentally. The data proves the proposed scheme efficiently which is called ultra-modern.

Keywords: *Auditing, Cloud Storage, Data Integrity, Data Security, Biometric Data, Bi-linearity, Data Blindness.*

1. Introduction

Cloud Storage services is a world class technology and powerful weapon demandable by users. Cloud services minimize maintenance and outlay of the hardware and software. The users upload data to the cloud[1],[12]. They lose the physical control of data is not in local. The integrity of the cloud data is hard to be guaranteed due to the inevitable hardware/software failures and error models and human guidance.

One can draw large data integrity auditing schemes proposed to the data owner or Third Party Auditor (TPA) to check the data stored in the cloud intact or not. These schemes focus on different aspects of data integrity auditing, such as data dynamic operation, privacy protection of data and user identities, key exposure resilience, the simplification of certificate management and privacy-preserving authenticators, etc. The above data integrity auditing schemes the user needs to generate authenticators for data blocks with his private key[3]. The user has to store and manage his private key in a secure manner. In general the user needs a portable secure hardware token (e.g. USB token, smart card) to store his private key and memorizes a password that is used to activate this private key. The user needs to remember multiple passwords for different secure applications in practical scenarios which is not user friendly. The hardware token contains the private key may be lost once the password is forgotten. The user is no longer being able to generate the authenticator for any new data block. The data integrity audit will not be functioning usual. It is interesting and appealing to find a method to realize data integrity auditing without storing the private key.



A most advantageous method is biometric data which is used by finger- print and IRIS recognition with the private key. Biometric data of the human body uniquely links the individual and the private key. Biometric data measures inevitable noise and cannot reproduce to a tee. Some factors affect the change of biometric data[14]. For example, the finger of each person generates a different fingerprint image every time due to pressure, moisture, presentation angle, dirt, different sensors, and many. The biometric data cannot directly use the private key to generate authenticators in data integrity auditing.

2. Methodology:

To ensure data integrity in cloud auditing schemes are proposed. In the existing schemes a user employs private key to generate the data authenticators realize data integrity auditing. The user possesses hardware token (e.g. USB token, smart card) to store private key and memorize a password to activate this private key. If the hardware token is lost the current data integrity auditing schemes would be unable to work. This problem can be solved through a new paradigm called data integrity auditing without private key storage and design a scheme further. Biometric data (e.g. fingerprint, face mask) of the user's fuzzy private key is used to avoid usage of hardware token. The scheme effectively completes the data integrity auditing. A linear sketch with coding and error correction processes confirms identity of the user. There is a new signature scheme design which supports block less verification[5]. It is compatible with linear sketch. The security proof and the performance analysis show the proposed scheme which achieves desirable security and efficiency.

3. Progress of the Study:

The primary step is to operate biometric data as fuzzy private key performing data integrity auditing, propose data integrity auditing without private key storage. Users utilize biometric data as fuzzy private key for confirming the identity. The data integrity auditing performs condition that is not hardware token to store private key. The operation formalizes data integrity auditing scheme without private key storage to secure cloud storage. The design is a practical data integrity auditing scheme without private key storage to secure cloud storage. Two fuzzy private keys (biometric data) extract from the user in the phase of registration and phase of signature generation. The respective use of the two fuzzy private keys generates two linear sketches that contain coding and error correction processes. The user’s identity confirms the two fuzzy private keys by removing the “noise”. The two biometric data are sufficiently close and confirms the extracted from the same user; otherwise, from different users. How to design a signa- ture satisfying both the compatibility with the linear sketch and the block less verifiability of a key challenge to realize data integrity auditing without private key storage[9]. This challenge helps overcome the design of a new signature scheme named as MBLSS by modifying the BLS short signature based on the idea of fuzzy signature. The security gives analysis and justifies the performance via concrete implementations. The results show the proposed scheme as secure and efficient.

4. Related Work:

Cloud computing is a boomster with progressive enterprises uploading and storing data in the public cloud. The business enterprises are owned by other enterprise and corresponding data is transferred to acquire the enterprise. The usual case outsources the computation cost of data transfer to cloud to ensure the remote purchase of data integrity. It is important to study provable data possession with outsourced data transfer (DT-PDP)[21]. The novel concept: DT-PDP takes use of DT-PDP with the following three security requirements.

(1) The other un-purchased data security of acquired enterprise can be ensured;

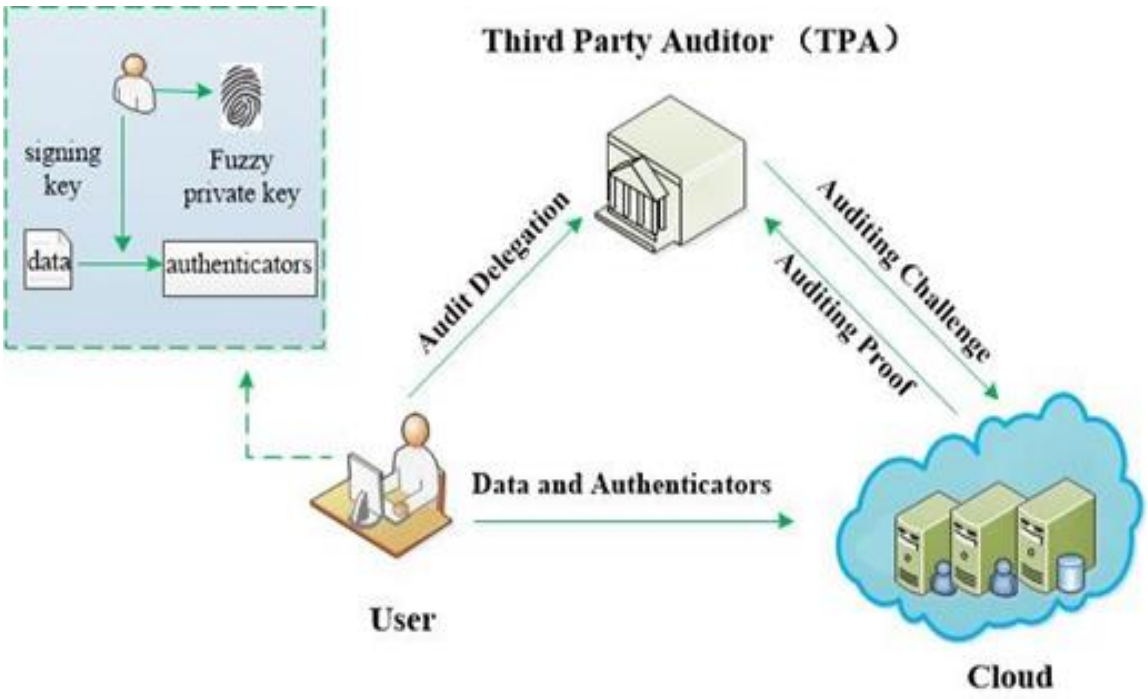
(2) The purchased data integrity and privacy can be ensured;

(3) The data transferability's computation can be outsourced to the public cloud servers for the security concept of DT-PDP.

The random sample technique and homomorphism linear authenticators design a PDP scheme to allow an auditor to verify the integrity of cloud data without downloading the whole data from the cloud. The concept of Proof of Retrievability (PoR) in the proposed scheme is the error- correcting codes and the spot-checking technique ensures retrievability and the integrity of the data stored in the cloud..

User-interactions include data modification, insertion and deletion. A dynamic data integrity auditing scheme exploits the index hash tables. Consider the problem of data dynamics in data integrity auditing and design a data integrity auditing scheme supporting data dynamic operations based on the Divide and Conquer Table. In public data integrity auditing, the TPA derives the contents of user's data by challenging the same data blocks multiple times. To protect the data privacy, Wang et al. exploited the random masking technique to construct the first public data integrity auditing scheme supporting privacy preserving. A data integrity auditing scheme preserves data privacy from the TPA[22]. Cloud storage auditing scheme proposes perfect data privacy preserving by making use of zero-knowledge proof. To relieve the user's computation burden of authenticator generation, a data integrity auditing scheme is constructed using in distinguishability obfuscation technique which reduces the over- head for generating data authenticators. A proposed data integrity auditing scheme which contains a cloud storage server and a cloud audit server. The cloud audit server helps users to generate data authenticators before uploading data to the cloud storage server. Shen et al. designed a light-weight data integrity auditing scheme which introduced a Third Party Medium to generate authenticators and verify data integrity on behalf of users.

Data sharing is used extensively in cloud storage animus. The identity is to protect the privacy of user. Wang et al. proposed a shared data integrity auditing scheme based on the ring signature. Yang et al. Designed a remote data integrity auditing scheme for shared data which supports both the identity privacy and the identity traceability[19]. By using the homomorphic verifiable group signature, Fu et al. proposed a privacy-aware remote data integrity auditing scheme for shared data. In order to achieve efficient user revocation. In this paper, we explore how to achieve data integrity auditing scheme without private key storage for secure cloud storage.



5. Preface:

Bilinear Pairings

Let G_1 and G_2 be two multiplicative groups of the prime order q, and g_1, g_2 be generators of group G_1. A bilinear pairing is a map with three properties.

(1) Bi-linearity

(2) Non-degeneracy

(3) Computability. There is an efficient algorithm to compute this pairing.

Data Blindness

The user A passes the encrypted data to user B and user B cannot infer the plaintext of user A based on these data in Data Blindness. Thus users are protected as privacy. A simple method to complete the blinding of data is as follows: user A blinds the data block by using the random function and sends it to user B. User B cannot obtain the original data.

Security Theory Assumption

DL problem is Unknown $a^{R}z^{*}\leftarrow q$, g is the generator. Giveng^{a}calculateα .

DL assumption- The probabilistic advantage of algorithm B to solve the DL problem in probabilistic polynomial time is

$$\mathrm{Adv}_{DL}\,(B) = pr[\ aB(g,g^{a}\longleftarrow)]$$

If $\mathrm{Adv}_{DL}(B)$ is negligible, it is called the DL problem which is difficult.

DCDH Problem is Known a, $b^R \leftarrow Z^*_p$, given $g^{1/a}$ and g^b, calculate g^{ab}.

DCDH Assumption- Theprobabilitythat algorithm B solves the DCDH problem in probabilistic polynomial time is

$$\mathrm{Adv}_{DCDH}(B) = pr[\, g^b B(\overleftarrow{g,g^{ab}},g^a)]$$

If $\mathrm{Adv}_{DCDH}(B)$ is ignored, it is difficult to call the DCDH problem.

Dynamic Broadcast Technology

Broadcast encryption technology is capable of transmitting encrypted information to group members over a broadcast channel. During the dissemination of this information, only members of the group can decrypt the message. Compared with traditional BE, BE can effectively support the dynamic changes of the group[16].

6. Conclusions

The analysis proposes the desired security goals. Data sharing framework in cloud environment is established and a public auditing scheme with identity privacy and identity traceability is made for group users. The auditing scheme achieves security requirements that a well-constructed auditing scheme shared for cloud data.The study improves the allocation of rights in the data integrity audit process and the security level of user data and protects identity privacy.

References

1. J. Lee, “A view of cloud computing,” Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2013.View at: Google Scholar.
2. Cloud Security Alliance, “Security guidance for critical areas of focus in cloud computing,” 2009, http://www.cloudsecurityalliance.org.
3. B. Wang, B. Li, and H. Li, “Knox: privacy-preserving auditing for shared data with large groups in the cloud,” in Proceedings of the International Conference on Applied Cryptography and Network Security, pp. 507–525, Springer-Verlag, 2012.View at: Publisher Site | Google Scholar
4. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted Stores,” in Proc. of CCS‟07, Alexandria, VA, October 2007, pp. 598–609.
5. A. Juels and J. Burton S. Kaliski, “Pors: Proofs of retrievability or large files,” in Proc. of CCS‟07, Alexandria, VA, October 2007, pp. 584–597.
6. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for secure cloud storage,” IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.View at: Publisher Site | Google Scholar
7. Q.-A. Wang, C. Wang, K. Ren, W.-J. Lou, and J. Li, “Enabling public auditability and data dynamics for storage security in cloud computing,” IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, 2011.View at: Publisher Site | Google Scholar
8. C. Wang, Q. Wang, K. Ren et al., “Privacy-preserving public auditing for data storage security in cloud computing,” in Proceedings of the IEEE INFO-COM, vol. 62, pp. 525–533, IEEE, San Diego, Calif, USA, March 2010.View at: Publisher Site | Google Scholar

9. L. Chen, "Using algebraic signatures to check data possession in cloud storage," Future Generation Computer Systems, vol. 29, no. 7, pp. 1709–1715, 2013.View at: Publisher Site | Google Scholar
10. Y. Zhang, J. Yu, R. Hao, C. Wang, and K. Ren, "Enabling efficient user revocation in identity-based cloud storage auditing for shared big data," IEEE Transactions on Dependable and Secure Computing, 2018.View at: Google Scholar
11. J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1931–1940, 2017.View at: Publisher Site | Google Scholar
12. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings of the IEEE INFOCOM, pp. 534–542, IEEE, Piscataway, NJ, USA, March 2010.View at: Publisher Site | Google Scholar
13. B. Liang, J. Y. Cao, Y. Z. Qin et al., "Survey of proofs on data storage security in cloud computing," Application Research of Computers, vol. 29, no. 7, pp. 2416–2421, 2012.View at: Google Scholar
14. G. Z. Qin, K. S. Wu, and H. Xiong, "A review on data integrity auditing protocols foe data storage in cloud computing," Net Info Security, pp. 1–6, 2014.View at: Google Scholar
15. S. H. Wang, D. W. Chen, Z. W. Wang et al., "A new solution of privacy preserving public auditing scheme foe cloud storage security," Telecommunications Science, vol. 28, no. 9, pp. 15–21, 2012.View at: Google Scholar
16. B. Wang, B. Li, and H. Li, "Oruta: privacy-preserving public auditing for shared data in the cloud," in Proceedings of the IEEE 5th International Conference on Cloud Computing (CLOUD '12), pp. 295–302, IEEE Computer Society, June 2012.View at: Publisher Site | Google Scholar
17. W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium," Journal of Network and Computer Applications, vol. 82, pp. 56–64, 2017.View at: Publisher Site | Google Scholar
18. B. Wang, H. Li, and M. Li, "Privacy-preserving public auditing for shared cloud data supporting group dynamics," in Proceedings of the ICC 2013 - 2013 IEEE International Conference on Communications, pp. 1946–1950, Budapest, Hungary, June 2013.View at: Publisher Site | Google Scholar
19. G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proceedings of International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 319–333, Springer-Verlag, London, UK, 2009.View at: Google Scholar | MathSciNet
20. W. Luo and G. Bai, "Ensuring the data integrity in cloud data storage," in Proceedings of the 2011 IEEE International Conference on Cloud Computing and Intelligence Systems, CCIS2011, pp. 240–243, IEEE, China, September 2011.View at: Google Scholar
21. G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," The Journal of Systems and Software, vol. 113, pp. 130–139, 2016.View at: Publisher Site | Google Scholar
22. G. Ateniese, R. Burns, R. Curtmola et al., "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 598–609, ACM, Virginia, Va, USA, November 2007.View at: Publisher Site | Google Scholar