Enabling authentication and Access Control-Based Data Sharing with personal Information Hiding for Secure Cloud Storage

[1]Dhanprada Bhoite, [2]Ankita Kamble, [3]Vishakha Kamble, [4]Prof. S.G. Dhengre

Department of Computer Engineering
AISSMS COE
Pune, India

***Abstract*: To improve the quality of healthcare and individual's quality of life E-healthcare cloud system shown its potential unluckily, privacy and security slow down its general deployment and application there are many researches focusing on preserving the privacy of the electronic healthcare record (EHR) data. However, these works have two main limitations first, they only works on 'black or white' access control policy. Second, they suffer from the inference attack. This paper, for the first time, we design an inference attack-resistant e-healthcare cloud system with fine-grained access control we first propose a two-layer encryption scheme. To make sure an efficient and fine-grained access control over the EHR data, we design the first-layer encryption, where we develop a specialized access policy for each data attribute in the EHR, and encrypt them individually with high efficiency. To preserve the privacy of role attributes and access policies used in the first-layer encryption, we systematically build the second-layer encryption To take full benefit of the cloud server, we propose to let the cloud execute computationally concentrated works on behalf of the data user without knowing any sensitive information To preserve the access pattern of data attributes in the EHR, we additional construct a blind data retrieving protocol. We also show that our scheme can be easily extended to support search functionality. Finally, we conduct extensive security analyses and performance evaluations.**

***Keywords*: Advance encryption standards, Personal data Abstraction, Anonymous authentication, rotating group signature, elliptic curve cryptography, smart health applications.**

Introduction:

Cloud Computing provides a based way to the user for storing and computing the data. We can use cloud computing to maintain data privacy and confidentiality in the cloud. We need to pay-per-use and it requires an internet connection for work. Due to lack of data security cloud provides an efficient way to store the data in encrypted form on the cloud. The aim is to prevent misuse of patient's documents and search they require data as per patient requirement. The serious secure and protected concerns are the over the form of problems that stand in the way of wide adoption of the framework. IT application plays an important role in the area of health and patient care. Cloud users upload personal or confidential data to the data center of a Cloud. In previous Electronic Health Record Systems cannot handle dynamic changes related to a number of the user. Our main motive is to protect the data from unauthorized access. In the previous system file uploading operation is not performed securely and misused of data increased because of lack of security. The cloud file might contain some sensitive information and The sensitive information should not be exposed to others when the cloud file is shared and Encrypting the whole shared file can realize the sensitive information hiding In some common cloud storage systems such as the Electronic Health Records (EHRs) system, the cloud file might contain some sensitive information. In the cloud storage services, users can slightly store their data in the cloud and recognize the data sharing with others. Remote data integrity auditing is proposed to guarantee the integrity of the data stored in the cloud. In some common cloud storage systems such as the Electronic Health Records (EHRs) system. In this Project, a sanitizer is used to sanitize or mining the data blocks corresponding to the sensitive information of the file and transforms these data blocks' signatures into valid ones for the sanitized file In remote data integrity auditing schemes, the data owner firstly needs to generate signatures for data blocks before uploading them to the cloud. These signatures are used to prove the cloud truly possesses these data blocks in the phase of integrity auditing.

Related work:

In order to verify the integrity of the data stored in the cloud, many remote data integrity auditing schemes have been proposed. To reduce the computation burden on the user side, a Third Party Auditor (TPA) is introduced to periodically verify the integrity of the cloud data on behalf of user. Ateniese etal. [2] firstly proposed a notion of Provable Data Possession (PDP) to ensure the data possession on the untrusted cloud. In their proposed scheme, homo morphic authenticators and random sampling strategies are used to achieve block less verification and reduce I/O costs. Juels and Kaliski [3] defined a model named as Proof of Retrieve ability (PoR) and proposed a practical scheme. In this scheme, the data stored in the cloud can be retrieved and the integrity of these data can be ensured. Based on pseudorandom function and BLS signature, Shacham and Waters [4] proposed a private remote data integrity auditing scheme and a public remote data integrity auditing scheme. In order to protect the data privacy, Wang et al. [5] proposed a privacy-preserving remote data integrity auditing scheme with the employment of a random masking technique.

Solomon et al. [6] utilized a different random masking technique to further construct a remote data integrity auditing scheme supporting data privacy protection. This scheme achieves better efficiency compared with the scheme in [5]. To reduce the computation burden of signature generation on the user side, Guan et al. [7] designed a remote data integrity auditing scheme based on the in distinguish ability obfuscation technique. Shen et al. [8] introduced a Third Party Medium (TPM) to design a light-weight remote data integrity auditing scheme. In this scheme, the TPM helps user generate signatures on the condition that data privacy can be protected. In order to support data dynamics, Ateniese et al. [10] firstly proposed a partially dynamic PDP scheme. Erway et al. [11] used a skip list to construct a fully data dynamic auditing scheme. Wang et al. [12] proposed another remote data integrity auditing scheme supporting full data dynamics by utilizing Merkle Hash Tree. To reduce the damage of users' key exposure, Yu et al. [13–15] proposed key-exposure resilient remote data integrity auditing schemes based on key update technique [16]. The data sharing is an important application in cloud storage scenarios. To protect the identity privacy of user, Wang etal. [17] designed a privacy-preserving shared data integrity auditing scheme by modifying the ring signature for secure cloud storage. Yang et al. [18] constructed an efficient shared data integrity auditing scheme, which not only supports the identity privacy but only achieves the identity traceability of users. Fu et al. [19] designed a privacy-aware shared data integrity auditing scheme by exploiting a homo morphic verifiable group signature. In order to support efficient user revocation, Wang et al. [20] proposed a shared data integrity auditing scheme with user revocation by using the proxy resignature. With the employment of the Shamir secret sharing technique, Luo et al. [21] constructed a shared data integrity auditing scheme supporting user revocation. The aforementioned schemes all rely on Public Key Infrastructure (PKI), which incurs the considerable overheads from the complicated certificate management. To simplify certificate management, Wang et al. [12] proposed an identity-based remote data integrity auditing scheme in multi cloud storage. This scheme used the user's identity information such as user's name or e-mail address to replace the public key. Wang et al. [20] designed a novel identity-based proxy-oriented remote data integrity auditing scheme by introducing a proxy to process data for users. Yu et al. [21] constructed a remote data integrity auditing scheme with perfect data privacy preserving in identity-based cryptosystems. Wang et al. [18] proposed an identity-based remote data integrity auditing scheme for shared data supporting real efficient user revocation. Other aspects, such as privacy-preserving authenticators [11] and data deduplication [11, 19] in remote data integrity auditing have also been explored. However, all of existing remote data integrity auditing schemes cannot support data sharing with sensitive information hiding. In this paper, we explore how to achieve data sharing with sensitive information hiding in identity-based integrity auditing for secure cloud storage.

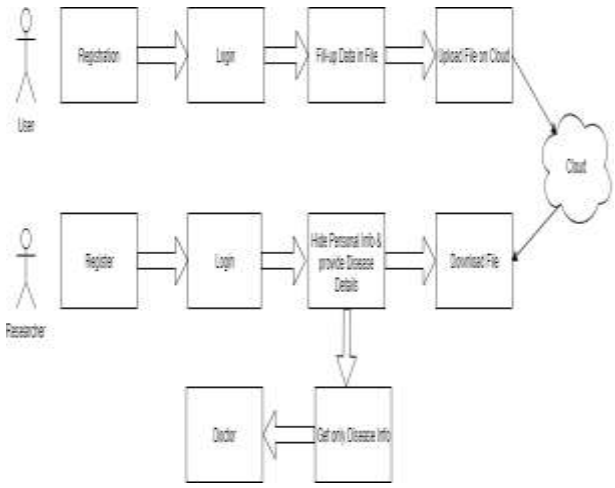
System Modules:

Our System mainly contains three modules one is Doctor and another are Patient and researcher.

System Architecture:

In the system, we design and develop a system for protecting information and confidential data. Our Main Purpose of the System is to protect the data from unauthorized access. Encrypting the whole shared file can realize the secret information hiding, but will make this shared file unable to be used by others. Signatures are used to verify the integrity of the sanitized file in the phase of integrity auditing.

—



Conclusion:

In the project we realize the moment allowed privacy-preserving Keyword indices in search procedure for the EHD reasoning storage space, which could support the automated delegation cancellation. Here Security and protective analysis shows our scheme provides reasonable overhead computation in cloud storage applications compared to traditional systems. This is the first retrievable security plan with the moment allowed encryption function and the specific specialist for the privacy–preserving EHD reasoning record storage space. The solution could ensure the comfort of the EHD and the potential to deal with assume keyword attacks.

References:

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Comput.*, vol. 16, no. 1, pp. 69–73, Jan. 2012.
[2] G. Ateniese *et al.*, "Provable data possession at untrusted stores," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 598–609.
[3] A. Juels and B. S. Kaliski, Jr., "Pors: Proofs of retrievability for large files," in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 584–597.
[4] H. Shacham and B. Waters, "Compact proofs of retriev ability," *J. Cryptol.*, vol. 26, no. 3, pp. 442–483, Jul. 2013.
[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362–375, Feb. 2013.
[6] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy preserving public auditing scheme for cloud storage," *Comput. Electr. Eng.*, vol. 40, no. 5, pp. 1703–1713, 2014.
[7] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetrickey based proofs of retriev ability supporting public verification," in *Computer Security—ESORICS*. Cham, Switzerland: Springer, 2015, pp. 203–223.
[8] 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," *J. Netw. Comput. Appl.*, vol. 82, pp. 56–64, Mar. 2017.
[9] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 6, pp. 754–764, Jun. 2010.
[10] G. Ateniese, 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 an Communications Security, ser. CCS '07, 2007, pp. 598–609.
[11] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 213–222.
[12] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, May 2011.
[13] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1167–1179, Jun. 2015.
[14] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1362–1375, Jun. 2016.
[15] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1931–1940, Aug. 2017.
[16] J. Yu, R. Hao, H. Xia, H. Zhang, X. Cheng, and F. Kong, "Intrusionresilient identity-based signatures: Concrete scheme in the standard model and generic construction," *Inf. Sci.*, vols. 442–443, pp. 158–172, May 2018.
[17] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in *Proc. IEEE 5th Int. Conf. Cloud Comput. (CLOUD)*, Jun. 2012, pp. 295–302.
[18] 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," *J. Syst. Softw.*, vol. 113, pp. 130–139, Mar. 2016.
[19] A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, "NPP: A new privacy-aware public auditing scheme for cloud data sharing with group users," *IEEE Trans. Big Data*, to be published, doi: 10.1109/TBDATA.2017.2701347.
[20] B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," *IEEE Trans. Serv. Comput.*,n vol. 8, no. 1, pp. 92–106, Jan./Feb. 2015.
[21] Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, "Efficient integrity auditing for shared data in the cloud with secure user revocation," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 434–442.