Identity-based Auditing for Electronic Medical Record Systems with Cloud Computing

[1] Vennila .V, [2] Sivaselvam .G
[1,2]Assistant Professor,
Department of Computer Science and Engineering,
K.S.R. College of Engineering,
Tiruchengode, India.

[3] Darshan .B, [4] Jesshwanth S. Joshua,
[5] Karthikeyan .T, [6] Kavibarati .R,
[3,4,5,6] UG Students
Department of Computer Science and Engineering,
K.S.R. College of Engineering,
Tiruchengode, India.

***Abstract*— Sharing digital medical records on public cloud storage via mobile devices facilitates patients (doctors) to get (offer) medical treatment of high quality and efficiency. However, challenges such as data privacy protection, flexible data sharing, efficient authority delegation, computation efficiency optimization, are remaining toward achieving practical fine-grained access control in the Electronic Medical Record (EMR) system. In this work, we propose an innovative access control model and a fine-grained data sharing mechanism for EMR, which simultaneously achieves the above-mentioned features and is suitable for resource-constrained mobile devices. In the model, complex computation is outsourced to public cloud servers, leaving almost no complex computation for the private key generator (PKG), sender and receiver. Additionally, the communication cost of the PKG and users is optimized. Moreover, we develop an extensible library called libabe that is compatible with Android devices, and the access control mechanism is actually deployed on realistic environment, including public cloud servers, a laptop and an inexpensive mobile phone with constrained resources. The experimental results indicate that the mechanism is efficient, practical and economical.**

Keywords : Auditing mechanism, attribute based encryption, secure outsourced computation, cloud computing, Electronic Medical Record.

I. INTRODUCTION

The cloud, the public verifier, and users (who share data as a group). The cloud offers data storage and sharing services to the group. The public verifier, such as a client who would like to utilize cloud data for particular purposes (e.g., search, computation, data mining, etc.) or a third-party auditor who can provide verification services on data integrity, aims to check the integrity of shared data via a challenge-and-response protocol with the cloud. In the group, there is one original user and a number of group users. The original user is the original owner of data. This original user creates and shares data with other users in the group through the cloud. Both the original
and group users are able to access, download and modify shared data. Shared data is divided into a number of blocks.

A user in the group can modify a block in shared data by performing an insert, delete or update operation on the block. In this paper, we assume the cloud itself is semi-trusted, which means it follows protocols and does not pollute data integrity actively as a malicious adversary, but it may lie to verifiers about the incorrectness of shared data in order to save the reputation of its data services and avoid losing money on its data services. In addition, we also assume there is no collusion between the cloud and any user during the design of our mechanism.

Generally, the incorrectness of share data under the above semi-trusted model can be introduced by hardware/software failures or human errors happened in the cloud. Considering these factors, users do not fully trust the cloud with the integrity of shared data. To protect the integrity of shared data, each block in shared data is attached with a signature, which is computed by one of the users in the group. Specifically, when shared data is initially created by the original user in the cloud, all the signatures on shared data are computed by the original user. After that, once a user modifies a block, this user also needs to sign the modified block with his/her own private key. By sharing data among a group of users, different blocks may be signed by different users due to modifications from different users.

II. RELATED WORK

A. Medical Users

Normally the medical user personal tending data (PHI) is especially fictional for observances the patients while not direct interaction with doctors. In Associate in nursing m-Healthcare system, medical users are not any longer required to be monitored among home or hospital environments. Instead, when being equipped with smart-phone and wireless body detector network (BSN) shaped by body detector nodes, medical users will walk outside and receive the high-quality tending observance from medical professionals anytime and anyplace.

B. Cryptographic Cloud Storage

Nowadays, more and more customers begin to use the cryptographic cloud storage for protecting their data security. But the re-encryption caused by revocation is a sure performance killer in such a cryptographic access control system. We propose a novel scheme to reduce the consumption of the re-encryption process. This scheme is built on a series of cryptographic algorithms. The original data is split into several slices and these slices are published to the cloud storage. After a revocation occurs, we re-encrypt only one slice instead of the whole data. The comparison between our scheme and original one shows that the optimized scheme can reduce the costs of re-encryption significantly.

C. Fundamental Search Operation

Cloud computing becomes prevalent due to the fact that it removes the burden of large scale data management in a cost effective manner. Hence, huge amount of data, ranging from personal health records to e-mails, are increasingly outsourced into the cloud. At the same time, transfer of sensitive data to un-trusted cloud servers leads to concerns about its privacy. To mitigate the concerns, sensitive data is usually outsourced in encrypted form which prevents unauthorized access. Although encryption provides protection, it significantly complicates the computation on the data such as the fundamental search operation. Still, cloud services should enable efficient search on the encrypted data to ensure the benefits of a full-fledged cloud computing environment. In fact, sizable amount of algorithms have been proposed to support the task which are called searchable encryption schemes. Traditionally, almost all such schemes have been designed for exact query matching.

D. Drawbacks Statement

In the existing method with the fast advancement of distributed computing innovation, a lot of information now has been put away on to the cloud. Since the information proprietor loses its control of the information, a few security with more, security issues emerge in distributed storage benefit, among which information protection is an exceptionally delicate problem. Encryption is a viable method to shield the information from being spilled. The process may, conventional look components with work for scrambled information. Step by step instructions to effectively seek over scrambled information subsequently turns into a critical and fascinating issue, and has maintain in numerous method consideration. To oppose the KGA assaults, processing with a few thoughts and presented extraordinary thoughts. Generally, the KGA works for reasons method.

To start with, the rival could get the data. Second, it can do the test without reserve. In this way, keeping in mind the end goal to keep an adversary from propelling a KGA attack, one can either protect the trapdoor from being spill to an outside attacker, for instance, setting up a protected channel between the collector and the server so that just the server can get the analyzed data or limit the unapproved collected process from doing the test, i.e. assigned analyzer PEKS the assigned server can do the test, PEKS with approval just the approved one can do the test method of data. The process with, neither one of the methods can keep an inside rival from propel the KGA attack. Henceforth, to construct an open key accessible encryption conspire which is secure against inside saying speculating attack is as yet an open issue.

III. RECENT METHODS

A. Storage Services In Cloud Storage

The first is privacy information retrieval (PIR), the second is symmetric encryption with keyword search and the last one is public key encryption with keyword search. Those are suitable to different kinds of requirements. In PIR systems, the user is able to upload and retrieve his encrypted data securely to/from the server, but he is unable to access a part of them directly. In real life, the smart phone is usually with small storage. If the encrypted data are too many or large, the smart phone might not be affordable or have sufficient storage.

B. Cryptographic Cloud Storage

Nowadays, more and more customers begin to use the cryptographic cloud storage for protecting their data security. But the re-encryption caused by revocation is a sure performance killer in such a cryptographic access control system. We propose a novel scheme to reduce the consumption of the re-encryption process. This scheme is built on a series of cryptographic algorithms. The original data is split into several slices and these slices are published to the cloud storage. After a revocation occurs, we re-encrypt only one slice instead of the whole data. The comparison between our scheme and original one shows that the optimized scheme can reduce the costs of re-encryption significantly. A re-encryption optimization scheme for accelerating the revocation operations.

C. Equations

The equations are an exception to the prescribed specifications of this template. You will need to determine whether or not your equation should be typed using either the Times New Roman or the Symbol font (please no other font). To create multileveled equations, it may be necessary to treat the equation as a graphic and insert it into the text after your paper is styled.

IV. PROPOSED WORK

In this archive, manage this overcome by recommend the primary thought of explanation Key Aggregate Searchable Encryption (KASE), and the design instantiating among actual KASE scheme. The proposed KASE plot applies to any circulated storage that processing of the accessible gathering information sharing usefulness, which implies any client may specifically impart a assembly of preferred report to a gather of preferred clients, while enabling the final to perform saying look over the previous. To verify accessible gathering information sharing the principle necessities for effective key administration are fold. Initial, an information proprietor immediately requirements to appropriate for a solitary total key quite than a assembly of key to a user for allocation any amount of proceedings.

A novel public auditing mechanism for the integrity of shared data with efficient user revocation in the cloud. In our mechanism, by utilizing the idea of proxy re-signatures, once a user in the group is revoked, the cloud is able to resign the blocks, which were signed by the revoked user, with a re-signing key. The PDP mechanism based on symmetric keys. A mechanism for auditing the correctness of data with the multi-server scenario, where these data are encoded with network coding. However, it is not publicly verifiable and only provides a user with a limited number of verification requests. As a result, the efficiency of user revocation can be significantly improved, and computation and communication resources of existing users can be easily saved.

Which indicates it is not only able to efficiently support a large number of users to share data and but also able to handle multiple auditing tasks simultaneously with batch auditing. In addition, by taking advantages of Shamir Secret

Sharing, we can also extend our mechanism into the multi-proxy model to minimize the chance of the misuse on re-signing keys in the cloud and improve the reliability of the entire mechanism.

V. IMPLEMENTATION

A. *Multi-User Searchable Encryption*

There is a rich literature on searchable encryption, including SSE schemes and PEKS schemes. In contrast to those existing work, in the context of cloud storage, keyword search under the multi-tenancy setting is a more common scenario. In such a scenario, the data owner would like to share a document with a group of authorized users, and each user who has the access right can provide a trapdoor to perform the keyword search over the shared document, namely, the "multi-user searchable encryption" (MUSE) scenario.

B. *Multi-Key Searchable Encryption*

In the case of a multi-user application, considering that the number of trapdoors is proportional to the number of documents to search over if the user provides to the server a keyword trapdoor under each key with which a matching document might be encrypted, firstly introduces the concept of multi-key searchable encryption (MKSE) and puts forward the first feasible scheme. MKSE allows a user to provide a single keyword trapdoor to the server, but still allows the server to search for that trapdoor's keyword in documents encrypted with different keys. This might sound very similar to the goal of KASE, but these are in fact two completely different concepts. The goal of KASE is to delegate the keyword search right to any user by distributing the aggregate key to him/her in a group data sharing system, whereas the goal of MKSE is to ensure the cloud server can perform keyword search with one trapdoor over different documents owing to a user.

C. *Key-Aggregate Encryption For Data Sharing*

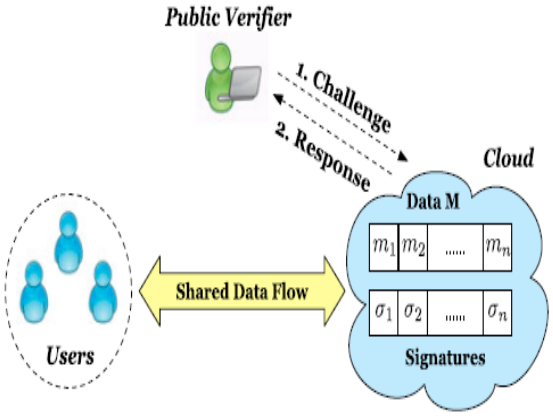
Data sharing systems based on cloud storage have attracted much attention recently. In particular, consider how to reduce the number of distributed data encryption keys. To share several documents with different encryption keys with the same user, the data owner will need to distribute all such keys to him/her in a traditional approach which is usually impractical. Aiming at this challenge, a keyaggregate Encryption (KAE) scheme for data sharing is proposed to generate an aggregate key for the user to decrypt all the documents. To allow a set of documents encrypted by different keys to be decrypted with a single aggregate key, user could encrypt a message not only under a public-key, but also under the identifier of each document.

D. *Security Analysis*

To analyze the security of our scheme, and in particular show that the scheme satisfies the security requirements given data assume that the public cloud is "honest-but-curious". That is, the cloud server will only provide legitimate services according to pre-defined schemes, although it may try to recover secret information based on its knowledge assume that the authorized users may try to access data either within or out of the scopes of their privileges. Moreover, communication channels involving the public cloud are assumed to be insecure. Based on the above considerations, we will prove the security of our scheme in terms of controlled searching and query privacy.

E. *Data Uploading*

The process to upload a document, the owner runs KAE. Encrypt to encrypt the data and KASE. Encrypt to encrypt the keyword ciphertexts, then uploads them to the cloud. The cloud assigns a docID for this document and stores the encrypted data in the path file Path, then inserts a record into the table docs. In addition, the owner can encrypt the keys using the private key and store them into the table docs. Data sharing. To share a group of documents with a target member, the owner runs KAE. Extract to generate the aggregate keys, and distributes them to this member, then inserts/updates a record in table shared Docs.



VI. CONCLUSION

A new public auditing mechanism for shared data with efficient user revocation in the cloud. When a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. Experimental results show that the cloud can improve the efficiency of user revocation, and existing users in the group can save a significant amount of computation and communication resources during user revocation.

When a third-party auditor is introduced into a public auditing mechanism in the cloud, both the content of data and the identities of signers are private information to users, and should be preserved from the TPA. The public mechanism proposed by Wang et al. is able to preserve user's confidential data from the TPA by using random masking. In addition, to operate multiple auditing tasks from different users efficiently, they also extended their mechanism to support batch auditing. Our recent work first proposed a mechanism for public auditing shared data in the cloud for a group of users. With ring signature-based homomorphism authenticators, the TPA can verify the integrity of shared data but is not able to reveal the identity of the signer on each block. The auditing mechanism in is designed to preserve identity privacy for a large number of users.

VII. FUTURE ENHANCEMENTS

The project has covered almost all the requirements. Further requirements and improvements can easily be done since the coding is mainly structured or modular in nature. Improvements can be appended by changing the existing modules or adding new modules. One important development that can be added to the project in future is file level backup, which is presently done for folder level.

Further enhancements can be made to the application, so that the application functions very attractive and useful manner than the present one. The speed of the transactions become more enough now. The data process can be easily analyzed in the future.

VIII. REFERENCES

[1] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing", Proc. IEEE INFOCOM, pp. 534-542, 2010.

[2] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[3] X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multiowner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182- 1191.

[4] C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.

[5] X. Song, D.Wagner, A. Perrig. "Practical techniques for searches on encrypted data", IEEE Symposium on Security and Privacy, IEEE Press, pp. 44C55, 2000.

[6] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

[7] P. Van,S. Sedghi, JM. Doumen. "Computationally efficient searchable symmetric encryption", Secure Data Management, pp. 87-100, 2010.

[8] S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchable symmetric encryption", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965- 976, 2012.

[9] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, pp. 506C522, 2004.

[10] Y. Hwang, P. Lee. "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System", In: Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.