International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

PUBLICLY VERIFIABLE SHARED DYNAMIC LECTRONIC HEALTH RECORD DATABASES WITH FUNCTIONAL COMMITMENT SUPPORTING PRIVACY-PRESERVING INTEGRITY AUDITING

Mr.T. Manigandan(Assist.professor)
dept of Computer Science and Engineering
Sphoorthy Enginnering College
Hyderabad, India

Dr.Subba Rao Kolavennu
Computer Science and Engineering
Sphoorthy Engineering College
Hyderabad, India

P. Vineela
dept of Computer Science And Engineering
Sphoorthy Engineering College
Hyderabad, India
Email : vineelavini509@gmail.com

V. Ramya Reddy
dept of Computer Science and Engineering
Sphoorthy Engineering College
Hyderabad, India
Email:vramyareddy12@gmail.com

k.Neelaveni
dept of Computer Science And Engineering
Sphoorthy Engineering College
Hyderabad, India
Email: kummarineelaveni7@gmail.com

I. ABSTRACT

Electronic health record (EHR) is a system that collects patients' digital health information and shares it with other healthcare providers in the cloud. Since EHR contains a large amount of significant and sensitive information about patients, it is required that the system ensures response correctness and storage integrity. Meanwhile, with the rise of IoT, more low performance terminals are deployed for receiving and uploading patient data to the server, which increases the computational and communication burden of the EHR systems. The verifiable database (VDB), where a user outsources his large database to a cloud server and makes queries once he needs certain data, is proposed as an efficient updatable cloud storage model for resource-constrained users. To improve efficiency, most existing VDB schemes utilize proof reuse and proof updating technique to prove correctness of the query results. In this paper, we propose a publicly verifiable shared updatable EHR database scheme that supports privacy-preserving and batch integrity checking with minimum user communication cost. We modify the existing functional commitment (FC) scheme for the VDB design and construct a concrete FC under the computational assumption. In addition, the use of an efficient verifier-local revocation group signature scheme makes our scheme support dynamic group member operations, and gives nice features, such as traceability and non-frameability.

Keywords: Verifiable database(VDB), ElectronicHealth record(EHR), cloud storage, functional commitment, privacy-preserving auditing, user revocation.

INTRODUCTION

Many cloud service providers are active to launch cloud service platforms and products, such as Amazon, GOOGLE, Alibaba, Microsoft, and Huawei, etc. People start to redistribute their large data storage tasks to cloud service providers (CSPs). As a concrete and high-quality application example of cloud storage, the cloud-based electronic health record (EHR), which is a system that collects the patients' digital health information, is being vigorously promoted by many organizations, such as the Office of the National Coordinator for Health Information Technology (ONC) in the United States and Canada Health Infoway . The patient EHRs are written on the mobile device, and can be accessed and modified later. The patient EHRs uploaded to the cloud can be shared among different medical institutions to help patients get better treatment, help scientific researchers to carry out disease analysis and research, and help public health departments predict, detect and prevent the outbreak of epidemic diseases, etc. If these data are destroyed and not discovered in time, it can cause huge losses in the event of an emergency.

Many audit schemes exist to check the data storage integrity. Some audit schemes provide methods to reduce the number of tags.

The biggest feature of the EHR system is that patients' health information is shared in a group, including clinic, healthcare, hospital, medicine center, insurance and so on. Anyone in the group can upload, download, and modify the database. In most cases, the members in such group are not fixed. And a group manager (GM) is appointed to control members' join or quit. The scheme provided an efficient audit scheme for group members to share cloud data, but only GM can upload the database. scheme involved the dynamic problem of group members, but their scheme can only realize the revocation and the case of users joining group is not considered. They used the group signature scheme with verifier-local revocation (VLR) proposed by Boneh et al. to make group members revocable. However, their VLR group signature scheme does not have even if a member is revoked at a certain time, the signature before that time remains anonymous. It poses a threat to user identity privacy

Database storage, such as EHR. According to the characteristics of EHR system, two aspects of security deserve our attention, namely, the server response correctness and the data storage integrity. In order to deal with above problems, we use a new tool called functional commitment (FC) and design a publicly verifiable updatable database scheme based on functional commitment supporting privacy-preserving integrity auditing and dynamic group operation. Our contributions can be summarized as follows:

1)We modify the existing functional commitment scheme in order to use the function binding of functional commitment to design an auditable VDB scheme. Two algorithms for updating are added based on the original scheme in. And a modified concrete FC with updates under the computational l - BDHE assumption is constructed. Our construction has fewer parameters and is more efficient than the original scheme in.

2)We point out security problems with scheme and propose a publicly verifiable updatable VDB scheme based on the functional commitment and group signature without incurring too much computational overhead and storage cost. Moreover, our scheme is applicable for large-scale data storage with minimum user communication cost. Our proposed scheme not only preserves all the properties of the original VDB scheme, but also implements efficient privacy-preserving integrity auditing, non-frameability and traceability. The scheme preserves data privacy from the auditor by using a random masking technique and the sparse vector is used for sampling auditing. Our scheme supports dynamic group member operations which include join and revocation. In addition, our VDB supports batch auditing and it supports multi-cloud server, multiuser and multi-storage vector scenarios

3)Security analysis and experimental comparison with existing schemes are provided and it shows that our VDB is secure and efficient.

Related Work

Electronic health record is a system that collects the pa◎tients' digital health information. It can reduce the medical errors, save EHR storage costs, and share medical information, etc. The transition from paper to electronic medical records has made the use of medical data more flexible and more usable. Research on data security of elec◎tronic health record system includes searchable encryp◎tion, privacy preserving, access control, and data storage integrity, etc. Many studies have been presented [16] – [19], and our work focuses on the security of the storage of large database, such as electronic health records

Similar to ordinary digital signature, group signature means anyone can verify the correctness of a group signa◎ture. The difference is that after verifying the group signa◎ture, the verifier can only confirm that the message is signed and issued by a member in a group, but it does not know who signed and issued it, which protects the ano◎nymity of the signer. When a dispute arises, there is a trusted group manager (GM) who can identify the member who actually signs the message. It is called traceability.

One of the most important problem in using group signa◎ture scheme in practice is group member revocation.

Boneh *et al.* [2] introduced the verifier-local revocation group signature scheme. In their scheme, the method of revocation is to send the information about the revoked members to the signature verifier. When the verifier checks the signature, he/she checks whether or not the signer of the signature has been revoked. However, their VLR group signature scheme does not have backward unlinkability. Another important property of group signatures is non◎frameability, which is to make sure no one, including group manager, can sign a message on behalf of other group members. Then, an efficient verifier-local signature scheme with these properties is constructed .

LITERATURE SURVEY

We have surveyed the existing projects and finally thought of making necessarymodifications for getting the latest edition.

EXISTING SYSTEM

We modify the existing functional commitment scheme in order to use the function binding of functional commitment to design an auditable VDB scheme. Two algorithms for updating are added based on the original scheme in . And a modified concrete FC with updates under the computational assumption is constructed. Our construction has fewer parameters and is more efficient than the original scheme in . We point out security problems with scheme and propose a publicly verifiable updatable VDB scheme based on the functional commitment and group signature without incurring too much computational overhead and storage cost. Moreover, our scheme is applicable for large-scale data storage with minimum user communication cost.

Disadvantages:

With the rise of IoT, more low performance terminals are deployed for receiving and uploading patient data to the server, which increases the computational and communication burden of the EHR systems.

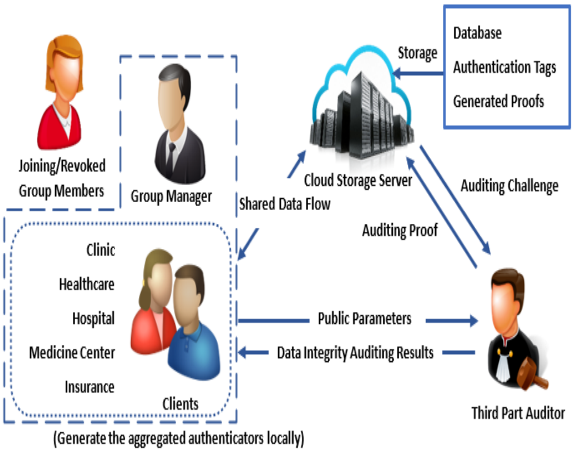
PROPOSED SYSTEM

Proposed the verifiable database (VDB) as a secure and efficient updatable cloud storage model for resource-limited users. In a VDB scheme, a client can outsource the storage of a collection of data items to an un-trusted server. Later, the client can query the server for an item (a message) at position i, the server returns the stored message at this position along with a proof that it is the correct answer. However, the security of only verifying the server response correctness is far from enough for the EHR system, and it is not clear whether data that is not frequently accessed is still stored correctly. If these data are destroyed and not discovered in time, it can cause huge losses in the event of an emergency.

Advantages:

1.Improving the efficiency.
2.Proof reuse and proof updating technique to prove correctness of the query results.

IMPLEMENTATION



MODULES

1. Client
2. TPA
3. Manager
4. Cloud

MODULE DESCRIPTION

Client

In this module client(clinic, health care, hospital, medicine center, insurance) should register with our Application after their successful register they must joined by the manage.

If they joined by the manager into the application he can perform some operations such as upload patient data and view patient data and also can search for other patient data, view patient data and share to other group member.

TPA

here TPA should login with the application after successful login he can perform some operations such as view patients records and audit records if any records has already modified by any user or not and also send the audit request to cloud

Manager

Here manager can login with the application after successful login he can perform some operations such as view client and join client or revoke clients

CLOUD :

Here cloud can login with the application after successful login he can perform some operations such as view clients details and patient details and check audit proof.

CONCLUSION

The concept of verifiable database is a great tool for verifiable EHR storage. However, proof reuse and the technique of proof updating by the server to improve system efficiency fails to achieve data integrity checking. In this work, we propose a novel updatable VDB scheme based on the functional commitment that supports privacy-preserving integrity auditing and group member operations, including join and revocation. Two security requirements of EHR are implemented: the server response correctness and the data storage integrity. Our VDB scheme achieves the desired security goals without incurring too much computational increase. And our VDB scheme provides the minimum communication cost for the terminal with limited performance. To design a functional commitment scheme that applies to our program, two algorithms are added to make the FC scheme updatable. A practical improved concrete VDB scheme under computational l −BDHE assumption is presented. In addition, batch auditing for our VDB scheme supports multi-cloud server, multi-user and multi-storage vector scenarios. It makes the auditing process more efficient. Furthermore, we prove that our functional commitment scheme with updates and our VDB scheme can achieve the desired security properties. The performance of our scheme is more efficient compared with other different algorithms.

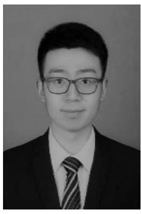
ACKNOWLEDGMENT

This work was supported by the National Nature Science Foundation of China under Grant Nos. 61272091 and 61772311.

REFERENCES

[1] Wei L, Wu C, Zhou S. efficient verifier-local revocation group signature schemes with backward unlinkability. Chinese Journal of Electronics, 2009, e90-a(2):379-384.
[2] Dan B, Shacham H. Group signatures with verifier-local revocation. Acm Conference on Computer & Communications Security. 2004.
[3] Chaum, David, and T. P. Pedersen. Wallet Databases with Observers. International Cryptology Conference on Advances in Cryptology 1992.
[4] B. Dan, X. Boyen, E. J. Goh, "Hierarchical identity based encryption with constant size ciphertext", International Conference on Theory and Applications of Cryptographic Techniques. Springer-Verlag, pp. 440- 456, 2005.
[5] A. Kate, G. M. Zaverucha, I. Goldberg, "Constant-Size Commitments to Polynomials and Their Applications", Advances in Cryptology - ASIACRYPT 2010 -, International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings. DBLP, pp. 177-194, 2010.
[6] Official Website of The Office of the National Coordinator for Health Information Technology (ONC). (2004). Available: https://www.healthit.gov/
[7] Canada Health Infoway. (2001). Available: https://www.infoway-inforoute.ca/en/
[8] J. Hu, H.H. Chen, T.W. Hou, "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations", Computer Standards & Interfaces vol. 32, No. 5-6, pp. 274-280, 2010.
[9] S. Benabbas, R. Gennaro, Y. Vahlis, "Verifiable Delegation of Computation over Large Datasets", Conference on Advances in Cryptology. Springer-Verlag, pp. 111-131, 2011.
[10] D. Catalano, D. Fiore. "Vector Commitments and Their Applications", Public-Key Cryptography – PKC 2013. Springer Berlin Heidelberg, pp. 55-72, 2013.

.



Jiameng Sun received his bachelor degree and Ph.D. degree in school of math ematics in Shandong University, China. His research interests include cloud com puting security and cyber security.

Ye Su received her bachelor degree in School of Mathematical Sciences from the University of Jinan, China, in 2014. She is currently a Ph.D. candidate in school of mathematics in Shandong Uni versity, China. Her research interests in clude cryptography and cloud security.

Appendix

EHR- Electronic Health Record
VDB- Verifiable DataBases
FC - Functional Commitments