SECURE MANAGEMENT OF HEALTH CARE DATA USING HIDDEN CIPHERTEXT POLICY ATTRIBUTE-BASED ENCRYPTION

B.BHAGYA LAKSHMI, S.SUNITHA
PG SCHOLAR.DEPT OF CSE, SIR C.V. RAMAN INSTITUTE OF TECHNOLOGY & SCIENCE, AP, INDIA
ASST. PROFESSOR, DEPT OF CSE, SIR C.V. RAMAN INSTITUTE OF TECHNOLOGY & SCIENCE,, AP, INDIA

ABSTRACT: Since cloud computing has been playing an increasingly important role in real life, the privacy protection in many fields has been paid more and more attention, especially, in the field of Personal Health Record (PHR). The traditional ciphertext-policy attribute based encryption(CP-ABE) provides the fine-grained access control policy for encrypted PHR data, but the access policy is also sent along with ciphertext explicitly. However, the access policy will reveal the users' privacy because it contains too much sensitive information of the legitimate data users. Hence it is important to protect users' privacy by hiding access policies. In most of the previous schemes, although the access policy is hidden, they face two practical problems: (1) these schemes do not support large attribute universe, so their practicality in PHR is greatly limited, and (2) the cost of decryption is especially high since the access policy is embedded in ciphertext. To address these problems, we construct a CP-ABE scheme with efficient decryption, where both the size of public parameters and the cost of decryption are constant. Moreover, we also show the proposed scheme achieves full security in the standard model under static assumptions by using the dual system encryption method..

1.INTRODUCTION

Health care service has been extensively studied to improve medical quality and reduce the cost of medical services [1], [2]. With a large amount of medical data, a health care system must extend its scale to provide efficient and secure services [3]. Media cloud computing, which treats computing as a utility, leases out the computing and storage capacities to the public patients and doctors. It is a revolutionary computing paradigm which enables dynamic resource allocation, self demand services, measurement of service, transparency of resource, etc [4]–[7]. As such, a patient can remotely store her data on the cloud server, namely data outsourcing, and then open her cloud data to the doctors. Note that the outsourced medical data may contain sensitive and private information (e.g., medical case and diagnostic report). It is often necessary to encrypt the medical data before it is uploaded to the cloud. However, the encrypted data cannot provide good usability due to the difficulty of searching over encrypted data. To address this issue, Searchable Symmetric Encryption (SSE) technology has been proposed in the literature as a fundamental approach to enabling keyword search over encrypted cloud data [8]. The existing searchable encryption schemes can achieve fuzzy keyword search, ranked keyword search, multi-keyword search, and so on [9]–[11]. Recently, many ciphertext-policy attribute based encryption(CP-ABE) (e.g., [11]) have been proposed to search over encrypted data. However, in such schemes every search shares the same secret key among users, which may cause disclosure of privacy. On the other hand, it is a challenging issue, especially in the health care system, to develop a dynamic version of SSE (DSSE) in which encrypted keyword search should be supported even if data is arbitrarily inserted into a collection (forward privacy) or deleted from a collection (backward privacy). Stefanov et al. [12] proposed an efficient DSSE scheme, which can achieve forward privacy, but cannot ensure backward privacy. Some researchers [13], [14] use the Oblivious Random Access Memory (ORAM) technique to achieve the forward privacy and backward privacy in DSSE. However, these approaches significantly increase the complexity in storage, search and updating processes. To address the above issues, in this paper, we propose a Secure and Efficient Dynamic Searchable Symmetric Encryption (SEDSSE) scheme over medical cloud data. This work extends and improves our previous research [15]. Specifically, this paper addresses two new issues: the collusion between the cloud server and search users as well as different secret key distribution among search users. In addition, we apply the newdesign to the health care system. Furthermore, the security and performance are analyzed. The original contributions of the paper are:

- Firstly, we combine the ciphertext-policy attribute based encryption(CP-ABE) techniques to propose a Secure and Efficient Dynamic Searchable Symmetric Encryption scheme, named SEPSSE I. The proposed scheme can achieve forward privacy, backward privacy, and collusion resistance between the cloud server and search users. • Secondly, based on the scheme, we further propose an enhanced scheme, named SEPSSE II to solve the key sharing problem which widely exists in the (CP-ABE) based searchable encryption schemes. Compared with the existing DSSE schemes, our proposed schemes are have less storage costs, search and updating complexity. Extensive experiments demonstrate the efficiency of our schemes in term of storage overhead, index building, trapdoor generating and query

2.LITERATURE SURVEY

Verifying individual wellbeing records in distributed computing: Patient-driven and fine-grained information get to control in multi-proprietor settings by M. Li, S. Yu, K. Ren, and W. Lou. Online individual wellbeing record (PHR) empowers patients to manage their very own medicinal records in a brought together manner, which greatly facilitates the capacity, access and sharing of individual wellbeing information. With the development of distributed computing, it is appealing for the PHR service providers to move their PHR applications and capacity into the cloud, in request to appreciate the versatile assets and lessen the operational cost. However, by putting away PHRs in the cloud, the patients lose physical control to their own wellbeing information, which makes it fundamental for each patient to scramble her PHR information before transferring to the cloud servers. Under encryption, it is trying to accomplish fine-grained get to contralto PHR information in an adaptable and productive manner. For every patient, the PHR data ought to be encoded so it is adaptable with the quantity of users having access. Additionally, since there are various proprietors (patients) in a PHR system and each proprietor would encode her PHR documents utilizing a different set of cryptographic keys, it is critical to lessen the key distribution complexity in such multi-proprietor settings. Existing cryptographic enforced access control plans are for the most part intended for the single-proprietor scenarios. In this paper, we propose a novel structure for get to control to PHRs inside distributed computing condition. To empower fine-grained and scalable access control for PHRs, we influence characteristic based encryption(ABE) systems to scramble every patient's PHR information. To decrease the key appropriation multifaceted nature, we separate the framework into numerous security domains, where every area oversees just a subset of the clients. In this way, every patient has full authority over her very own protection, and the key management multifaceted nature is diminished significantly. Our proposed scheme is additionally adaptable, in that it underpins productive and on-request disavowal of user get to rights, and break-glass access under crisis situations

Openings and difficulties of distributed computing to improve social insurance benefits by A. M.- H. Kuo

Distributed computing is another method for conveying figuring assets and administrations. Numerous supervisors and specialists accept that it can improve human services administrations, advantage medicinal services research, and change the substance of wellbeing data innovation. Be that as it may, likewise with any development, distributed computing ought to be thoroughly assessed before its far reaching reception. This paper examines the idea and its present spot in social insurance, and utilizations 4 viewpoints (the executives, innovation, security, and lawful) to assess the chances and difficulties of this registering model. Vital arranging that could be utilized by a wellbeing association to decide its heading, technique, and asset allotment when it has chosen to move from conventional to cloud-based wellbeing administrations is additionally talked about.

3.EXISTING SYSTEM

The concept of SPE was first proposed by Boneh et al. [26], which supports single keyword search on encrypted data but the computation overhead is heavy. Curtmola et al. [27] refined the definition of SSE later. After this work, Boneh et al. [24] proposed conjunctive, subset, and range queries on encrypted data. Recently in static searchable symmetric encryption, Wang et al. have developed the ranked keyword search scheme in [8] and proposed a novel scheme supporting similarity search in [25]. However, these schemes cannot efficiently support multi-keyword search. To overcome this problem, Sun et al. [9] proposed a multi-keyword scheme which also considers the relevance scores of keywords, and it can achieve efficient query by utilizing the multidimensional tree technique.

In [10], Yu et al. proposed a multi-keyword topk retrieval scheme with fully homomorphic encryption, which can return ranked results and achieve high security. Cao et al. [11] proposed a multi-keyword ranked search scheme, which can return ranked results of searching according to the number of matching keywords and its extended versions achieve higher efficiency. As mentioned by Ren et al. [28], there still exists many security challenges for public clouds.

Disadvantages

The system is not implemented Forward privacy and backward privacy.

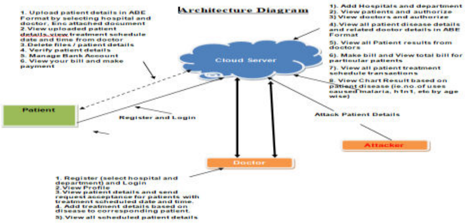
The system is not implemented Attribute-based encryption.

4.PROPOSED SYSTEM

In the proposed system, the system proposes a Secure and Efficient Dynamic Searchable Symmetric Encryption (SEDSSE) scheme over medical cloud data. This work extends and improves our previous research [15]. Specifically, this paper addresses two new issues: the collusion between the cloud server and search users as well as different secret key distribution among search users. In addition, we apply the new design to the health care system. Furthermore, the security and performance are analyzed. The original contributions of the paper are: Firstly, the system combines the ciphertext-policy attribute based encryption(CP-ABE) techniques to propose a Secure and Efficient Dynamic Searchable Symmetric Encryption scheme, named SEPSSE I. The proposed scheme can achieve forward privacy, backward privacy, and collusion resistance between the cloud server and search users.

Secondly, based on the scheme, we further propose an enhanced scheme, named SEPSSE II to solve the key sharing problem which widely exists in the ciphertext-policy attribute based encryption(CP-ABE) based searchable encryption schemes. Compared with the existing DSSE schemes, our proposed schemes are have less storage costs, search and updating complexity. Extensive experiments demonstrate the efficiency of our schemes in term of storage overhead, index building, trapdoor generating and query.

5.SYSTEM ARCHITECTURE


Architecture Diagram
1. Upload patient details in ABE Format by selecting hospital and doctor, Enc attached document
2.View uploaded patient details,view treatment schedule date and time from doctor
3.Delete files / patient details
4. Verify patient details
5. Manage Bank Account
6. View your bill and make payment
1). Add Hospitals and department
2). View patients and authorize
3) View doctors and authorize
4). View all patient disease details and related doctor details in ABE Format
5). View all Patient results from doctors
6). Make bill and View total bill for particular patients
7). View all patient treatment schedule transactions
8. View Chart Result based on patient disease (ie.no.of uses caused malaria, h1n1, etc by age wise)
Cloud Server
Patient
Register and Login
Attack Patient Details
Attacker
Doctor
1. Register (select hospital and department) and Login
2.View Profile
3.View patient details and send request acceptance for patients with treatment scheduled date and time.
4. Add treatment details based on disease to corresponding patient.
5).View all scheduled patient details

6.IMPLEMENTATION

Patient:

A patient outsources her documents to the cloud server to provide convenient and reliable data access to the corresponding search doctors. To protect the data privacy, the patient encrypts the original documents under an access policy using attribute-based encryption. To improve the search efficiency, she also generates some keyword for each outsourced document. The corresponding index is then generated according to the keywords using the secret key of the secure kNN scheme. After that, the patient sends the encrypted documents, and the corresponding indexes to the cloud server, and submits the secret key to the search doctors.

Cloud server:

A cloud server is an intermediary entity which stores the encrypted documents and the corresponding indexes received from patients, and then provides data access and search services to authorized search doctors. When a search doctor sends a trapdoor to the cloud server, it would return a collection of matching documents based on certain operations.

Doctor:

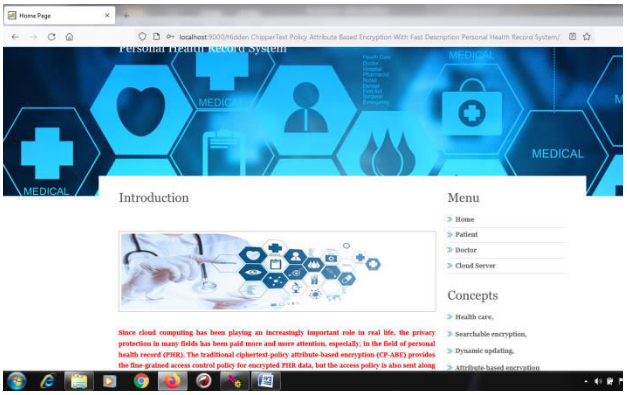
An authorized doctor can obtain the secret key from the patient, where this key can be used to generate trapdoors. When she needs to search the outsourced documents stored in the cloud server, she will generate a search keyword set. Then according to the keyword set, the doctor uses the secret key to generate a trapdoor and sends it to the cloud server. Finally, she receives the matching document collection from the cloud server and decrypts them with the ABE key received from the trusted authority. After getting the health information of the patient, the doctor can also outsource medical report to the cloud server by the same way. For simplicity, we just consider one-way communication in our schemes.

Advantages

The system implemented very strong security scheme of Privacy protection of documents, indexes and trapdoors.

The system provides Collusion resistance between the cloud server and search Users.

7.RESULT


Home Page
localhost:9000/Hidden ChipperText Policy Attribute Based Encryption With Fast Description Personal Health Record System/
Personal Health Record System
MEDICAL
MEDICAL
MEDICAL
MEDICAL
Introduction
Menu
Home
Patient
Doctor
Cloud Server
Concepts
Health care,
Searchable encryption,
Dynamic updating,
Attribute-based encryption

Since cloud computing has been playing an increasingly important role in real life, the privacy protection in many fields has been paid more and more attention, especially, in the field of personal health record (PHR). The traditional ciphertext-policy attribute-based encryption (CP-ABE) provides the fine-grained access control policy for encrypted PHR data, but the access policy is also sent along

8.CONCLUSION

In this paper, we propose two dynamic searchable encryption schemes with high security level. The first one can not only achieve collusion resistance between the cloud server and search users, but also can achieve both forward privacy and backward privacy. The second one further solves the key sharing problem which widely exists in the ciphertext-policy attribute based encryption(CP-ABE). Performance evaluation demonstrates that the proposed schemes can achieve better efficiency than the existing works in terms of storage, search and updating complexity. Extensive experiments demonstrate the efficiency of our schemes in term of storage overhead, index building, trapdoor generating and query.

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in Security and Privacy in Communication Networks. Springer, 2010, pp. 89–106.

[2] A. M.-H. Kuo, "Opportunities and challenges of cloud computing to improve health care services," Journal of medical Internet research, vol. 13, no. 3, 2011.

[3] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[4] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[5] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, "An smdpbased service model for interdomain resource allocation in mobile cloud networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 5, pp. 2222–2232, 2012.

[6] M. M. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 10, pp. 1805–1818, 2012.

[7] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, "Exploiting geodistributed clouds for e-health monitoring system with minimum service delay and privacy preservation," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, pp. 430–439, 2014.

[8] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467–1479, 2012.

[9] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 11, pp. 3025–3035, 2014.

[10] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Towards secure multikeyword top-k retrieval over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 239–250, 2013. [11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multikeyword ranked search over encrypted cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 1, pp. 222–233, 2014.

[12] E. Stefanov, C. Papamanthou, and E. Shi, "Practical dynamic searchable encryption with small leakage," in Proceedings of NDSS, 2014. [13] M. T. Goodrich and M. Mitzenmacher, "Privacy-preserving access of outsourced data via oblivious ram simulation," in Automata, Languages and Programming. Springer, 2011, pp. 576–587.

[14] D. Cash, A. K¨upc¸¨u, and D. Wichs, "Dynamic proofs of retrievability via oblivious ram," in Advances in Cryptology–EUROCRYPT. Springer, 2013, pp. 279–295.

[15] Y. Yang, H. Li, L. Wenchao, H. Yang, and W.

Mi, “Secure dynamic searchable symmetric encryption with constant document update cost,” in Proceedings of GLOBECOM. IEEE, 2014, pp. 775–780.

[16] S. Luo, J. Hu, and Z. Chen, “Ciphertext policy attribute-based proxy reencryption,” in Information and Communications Security. Springer, 2010, pp. 01–415.