Inference Attack-Resistant E-Healthcare Cloud System with Fine-Grained Access

Shiwali Thakur, Pankaj Patil, Prof. Ashwini Shirke
Alard Charitable Trust Alard College of Engineering Management

Abstract

The e-healthcare cloud system has shown its potential to improve the quality of healthcare and individuals' quality of life. Unfortunately, security and privacy impede its widespread deployment and application. There are several research works focusing on preserving the privacy of the electronic healthcare record (EHR) data. However, these works have two main limitations. First, they only support the 'black or white' access control policy. Second, they suffer from the inference attack. In 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 ensure an efficient and fine-grained access control over the EHR data, we design the first-layer encryption, where we devise 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 construct the second-layer encryption. To take full advantage of the cloud server, we propose to let the cloud execute computationally intensive works on behalf of the data user without knowing any sensitive information. To preserve the access pattern of data attributes in the EHR, we further construct a blind data retrieving protocol. We also demonstrate that our scheme can be easily extended to support search functionality. Finally, we conduct extensive security analyses and performance evaluations, which confirm the efficacy and efficiency of our schemes.

Keyword: EHR, Encryption, Decryption, Trusted Authority, Attributes, Data Sharing.

Introduction

The electronic healthcare, providing timely, accurate, and low-cost healthcare services, has shown its potential to improve the quality of healthcare and individuals lives. Many companies all over the world have developed their healthcare services, e.g., Google Fit . Apple Health Kitetc. Meanwhile, with the increasing maturity and benefits brought by cloud computing, the e-healthcare cloud system has attracted many interests from both the academic and the industry. The IBM company has already established its e-healthcare cloud center, i.e., IBM Watson Health Cloud. Unfortunately, security and privacy will impede the widespread deployment and application of thee-healthcare cloud system. The fundamental reason is that, once the sensitive EHR data are outsourced to the cloud, data owners would lose their cont .Although the cloud service providers promise they will preserve these data by installing anti-virus softwares, firewalls, and intrusion detection and prevention systems, they cannot stop their employees from accessing these data. For example, an employee in the department of veterans affairs once takes away 26.5 million sensitive data without authorization, which includes the social security numbers and sensitive health data. When these sensitive data are abused, more serious problems will occur. For example, insurance companies would refuse to provide insurance to those who have serious health problems. Therefore, it is vital to preserve the security and privacy of EHR data stored in the e-health care cloud system.

Problem statement

In this project we are using cloud computing for storage. In the recent years storage is a biggest issue in a organizations, so to secure the data and get at anytime we use cloud. We are applying encryption to the data to avoid the security issue. And in this we are assigning time to the designated tester in conjunctive
keyword search.

Literature Survey

1. Shuttle: Intrusion Recovery for PaaS.
Authors: Dario Nascimento, Miguel Correia
Description: In this paper, Authors present Shuttle, a novel intrusion recovery service. Shuttle recovers from intrusions in applications deployed in PaaS plat-forms. This approach allows undoing changes to the state of PaaS applications due to intrusions, without losing the effect of legitimate operations performed after the intrusions take place. They combine a record-and-replay approach with the elasticity provided by cloud offerings to recover applications deployed on various instances and backed by distributed databases. The service loads a database snapshot taken before the intrusion and replays subsequent requests, as much in parallel as possible, while continuing to execute incoming requests. Authors present an experimental evaluation of Shuttle on Amazon Web Services. They show Shuttle can replay 1 million requests in 10 minutes and that it can duplicate the number of requests replayed per second by increasing the number of application servers from 1 to 3.

2. Privacy Preserving Ranked Multi-Keyword Search for Multiple Data Owners in Cloud Computing
Authors: W. Zhang, Y. Lin, S. Xiao, J. Wu
Description: In this paper, authors propose schemes to deal with Privacy preserving Ranked Multi-keyword Search in a Multi-owner model (PRMSM). To enable cloud servers to perform secure search without knowing the actual data of both keywords and trapdoors, systematically construct a novel secure search protocol. To rank the search results and preserve the privacy of relevance scores between keywords and files, they propose a novel Additive Order and Privacy Preserving Function family. To prevent the attackers from eavesdropping secret keys and pretending to be legal data users submitting searches, we propose a novel dynamic secret key generation protocol and a new data user authentication protocol. Furthermore, PRMSM supports efficient data user revocation. Extensive experiments on real-world datasets confirm the efficacy and efficiency of PRMSM.

3. **Charm: a framework for rapidly prototyping cryptosystems**
Authors: Joseph A. Akinyele · Christina Garman

Description: Authors describe Charm, an extensible framework for rapidly prototyping cryptographic systems. Charm provides a number of features that explicitly support the development of new protocols, including support for modular composition of cryptographic building blocks, infrastructure for developing interactive protocols, and an extensive library of re-usable code. This framework also provides a series of specialized tools that enable different cryptosystems to interoperate. they implemented over 40 cryptographic schemes using Charm, including some new ones that, to their knowledge, have never been built in practice. This paper describes modular architecture, which includes a built-in benchmarking module to compare the performance of Charm primitives to existing C implementations. Authors show that in many cases techniques result in an order of magnitude decrease in code size, while inducing an acceptable performance impact. Lastly, the Charm framework is freely available to the research community and to date, we have developed a large, active user base

4. A Privacy-Preserving Attribute-Based Authentication System for Mobile Health Networks
Authors: Linke Guo**,** Chi Zhang, Jinyuan Sun**,** Yuguang Fang

Description: In this paper, a decentralized system that leverages users' verifiable attributes to authenticate each other while preserving attribute and identity privacy. Moreover, author design authentication strategies with progressive privacy requirements in different interactions among participating entities. Finally, they have thoroughly evaluated the security and computational overheads for our proposed schemes via extensive simulations and experiments.

5. Dynamic Audit Services for Outsourced Storages in Clouds

Authors: Yan Zhu, Gail-Joon Ahn

Description: In this paper, authors propose a dynamic audit service for verifying the integrity of

an un trusted and outsourced storage. Their audit service is constructed based on the techniques, fragment structure, random sampling and index-hash table, supporting provable updates to outsourced data and timely anomaly detection. In addition, they propose a method based on probabilistic query and periodic verification for improving the performance of audit services. Our experimental results not only validate the effectiveness of our approaches, but also show audit system verifies the integrity with lower computation overhead and requiring less extra storage for audit metadata.

6. Dynamic-hash-table based public auditing for secure cloud storage
Authors: H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen
Description: In this paper, authors present a novel public auditing scheme for secure cloud storage based on dynamic hash table (DHT), which is a new two-dimensional data structure located at a third parity auditor (TPA) to record the data property information for dynamic auditing. Differing from the existing works, this scheme migrates the authorized information from the CSP to the TPA, and thereby significantly reduces the computational cost and communication overhead. Meanwhile, exploiting the structural advantages of the DHT, this scheme can also achieve higher updating efficiency than the state-of-the-art schemes. In addition, they extend their scheme to support privacy preservation by combining the homomorphic authenticator based on the public key with the random masking generated by the TPA, and achieve batch auditing by employing the aggregate BLS signature technique. Authors formally prove the security of the proposed scheme, and evaluate the auditing performance by detailed experiments and comparisons with the existing ones. The results demonstrate that the proposed scheme can effectively achieve secure auditing for cloud storage, and outperforms the previous schemes in computation complexity, storage costs and communication overhead.

Existing System
The e-healthcare cloud system has shown its potential to improve the quality of healthcare and individuals' quality of life. Unfortunately, security and privacy impede its widespread deployment and application. There are several research works focusing on preserving the privacy of the electronic healthcare record (EHR) data. However, these works have two main limitations. First, they only support the 'black or white' access control policy. Second, they suffer from the inference attack.

Proposed System
In this algorithm we are using encryption, decryption technique. At the time of data upload the algorithm will be performed. This is the most secure algorithm insecurity because it works on more bits. There are several research works focusing on preserving the privacy of the electronic healthcare record (EHR) data. However, these works have two main limitations. First, they only support the `black or white' access control policy. In 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 ensure an efficient and fine-grained access control over the EHR data, we design the first-layer encryption, where we devise 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 construct the second-layer encryption. To take full advantage of the cloud server, we propose to let the cloud execute computationally intensive works on behalf of the data user without knowing any sensitive information. To preserve the access pattern of data attributes in the EHR, we further construct a blind data retrieving protocol. We also demonstrate that our scheme can be easily extended to support search functionality. Finally, we conduct extensive security analyses and performance evaluations, which confirm the efficacy and efficiency of our schemes.

System Architecture

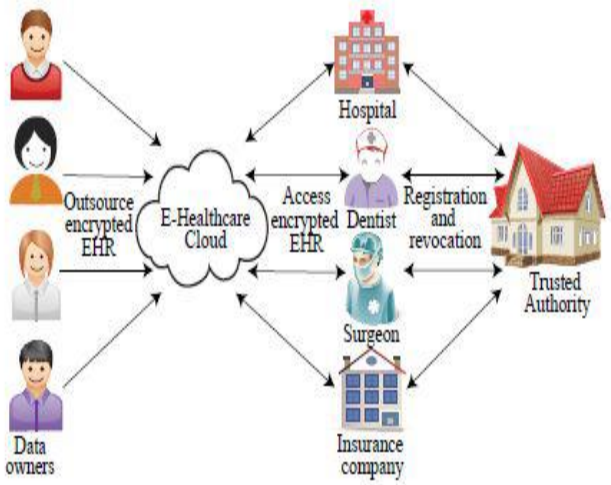


Fig: Architecture Diagram

Advantages

- Our main advantages is to securely save the data on cloud and access it securely.
- E-Health care document could be vulnerable if the server is interrupt or an inside staff misjudge.
- The serious secure and protected concerns are the over form of problems that stands in the way of wide adoption of the framework.

Disadvantages

- Data Security

Data security is one of the major concerns of cloud computing. Most of the time mobile users provide sensitive information through the network, and if it is not protected can cause major damages. You need to choose the most reliable service provider, who can keep your data totally safe and secure.

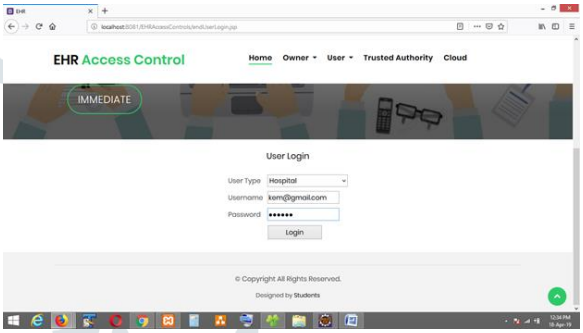
- Performance Issues

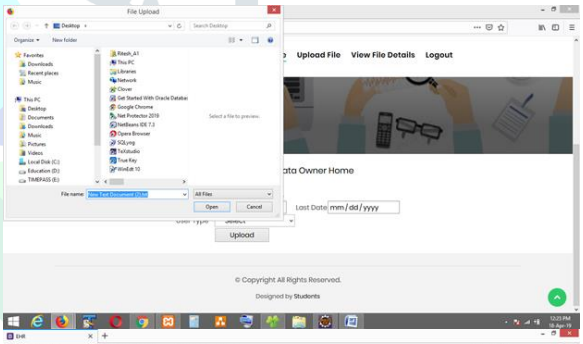
As mobile cloud computing depends on internet, this can affect your access and use. Sometimes you may feel that performance is not up to the mark. Hence, it is better to check the track record of your service provider before undertaking the service. In spite of keeping up high standards of maintenance, cloud service providers may face some serious dysfunction.

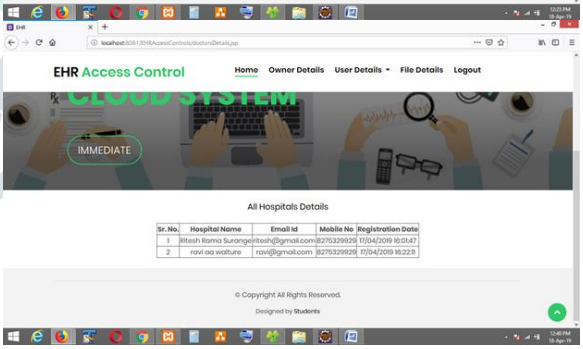
Application

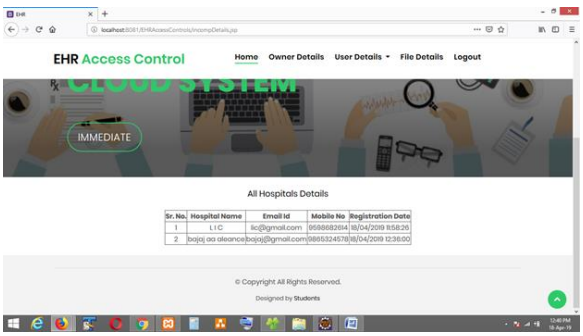
- Hospital Management
- A cloud application, or cloud app, is a software program where cloud-based and local components work together. This model relies on remote servers for processing logic that is accessed through a web browser with a continual internet connection.

Screen Shots:









Conclusion

In 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. In the first-layer encryption, we propose to define a specialized access policy for each data attribute in the EHR, generate a secret share for every distinct role attribute, and reconstruct the secret to encrypt each data attribute, which ensures a fine grained access control, saves much encryption time, and conceals the frequency of role attributes occurring in the EHR. In the second-layer encryption, we propose to preserve the privacy of role attributes and access policies used in the first-layer encryption. Additionally, to take full advantage of the cloud server, we propose to let the cloud execute computationally intensive works on behalf of the data user without knowing any sensitive information. o preserve the access pattern of the data attributes in the EHR, we construct a blind data retrieving protocol based on the Parlier encryption. Furthermore, we how that our scheme can be easily extended to support search functionality. Finally, we conduct extensive security analyses and performance evaluations, which confirm the efficacy and efficiency of our schemes.

Referances

[1] A. Martinez-Balleste, P. A. Perez-Martinez, and A. Solanas, "The pursuit of citizens' privacy: a privacy aware smart city is possible," IEEE Commun. Magazine, vol. 51, no. 6, pp. 136–141, Jun. 2013.

[2] D. Aranki, G. Kurillo, P. Yan, D. M. Liebovitz, and R. Bajcsy, "Realtimetele-monitoring of patients with chronic heart-failure using a smartphone: lessons learned," IEEE Trans. on Affective Computing, vol. 7, no. 3, pp. 206–219, Apr. 2016.

[3] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Commun. Surveys & Tutorials, vol. 15, no. 2, pp. 843–859, May 2013.

s[4] D. Ding, M. Conti, and A. Solanas, "A smart health application and its related privacy issues," in Proc. Smart City Security and Privacy Workshop (SCSP-W), Apr. 2016, pp. 1–5.

[5] P. Gope and T. Hwang, "Untraceable sensor movement in distributed iot infrastructure," IEEE Sensors J., vol. 15, no. 9, pp. 5340–5348, Jun. 2015.

[6] L. Guo, Y. Fang, M. Li, and P. Li, "Verifiable privacy-preservingmonitoring for cloud-assisted mhealth systems," in *INFOCOM,015 Proceedings IEEE*. Hong Kong: IEEE, 2015, pp.
1026–1034.

[7] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in*Advances in Cryptology–EUROCRYPT 2005*. Springer, 2005, pp.457–473

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attributebased
encryption for fine-grained access control of encrypteddata," in *Proceedings of the 13th ACM conference on Computerand communications security*. Acm, 2006, pp. 89–98.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policyattribute-based encryption," in *Security and Privacy, 2007.P'07.IEEE Symposium on*. IEEE, 2007, pp. 321–334.

[10] S. Islam, M. Kuzu, and M. Kantarcioglu, "Inference attack
against encrypted range queries on outsourced databases," in
Proceedings of the 4th ACM conference on Data and application
security and privacy. ACM, 2014, pp. 235–246.