International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 11 | Nov 2019 www.irjet.net p-ISSN: 2395-0072

Privacy, Access and Control of Health Care Data on Cloud using Recommendation System Cloud Storage

Reshma Borhade[1], Pratiksha Pansare[2], Seema Aher[3], Prof. Sachin Dighe[4]

[1,2,3]Student, Dept. of Computer Engg. Sahyadri Valley COE & Technology, Pune, Maharashtra, India
[4]Assistant Professor, Dept. of Computer Engg. Sahyadri Valley COE & Technology, Pune, Maharashtra, India

---

Abstract - *There is a major volume of health care knowledge data generated daily. The data square measure vital and important for higher cognitive process and delivering the simplest look after patients. Cloud computing may be an efficient technique that facilitates period knowledge assortment, knowledge storage and exchange between health care organizations. Security and privacy square measure of the most important considerations for victimisation cloud-based health care services. Personal health record (PHR) is associate rising patient-centric model of health info exchange, that is commonly outsourced to be hold on a cloud. There are wide privacy considerations as personal health info may be exposed to those third-party servers and to unauthorized parties. To assure the patients' management over access to their own PHRs, it's a promising technique to encipher the PHRs before outsourcing. Yet, problems like risks of privacy exposure, quantifiability in coding key management, versatile access have remained the foremost vital challenges toward achieving fine-grained, cryptographically enforced knowledge access management. To achieve fine-grained and ascendible knowledge access management for PHRs, we tend to leverage attribute-based coding (ABE)techniques to encipher every patient's PHR file. We specialise in the multiple knowledge owner state of affairs, supports economical on-demand user/attribute revocation and break-glass access underneath emergency situations.*

Designing healthcare recommendation system is a need for the fast-growing world. In this fast-growing world, the need for the application which recommend a healthcare led to a doctor friendly and hospital free atmosphere for all users all over the world.

Key Words*: *Multi-authority, encrypted data search, e-medical system, cloud storage, forward security.

1. INTRODUCTION

Cloud computing is a successful paradigm offering companies and individuals virtually unlimited data storage and computational power at very attractive costs. Despite its benefits, cloud computing raises serious security concerns for preserving the confidentiality of sensitive data, such as medical, social, and financial information. Once the data is outsourced, it is exposed to careless or even potentially malicious Cloud Service Providers (CSPs). Moreover, the data could also be learned by third party intruders because the cloud platform could be compromised. In this context, the data owner lacks a valid mechanism for protecting the data from unauthorised access. A straight forward method to solve the issue is to encrypt the data with standard cryptographic primitives, such as AES and RSA, before uploading it to the CSP. However, this method is not practical for the applications requiring to perform search over the data, such as relational databases, web applications, and machine learning tools. The reason is that standard cryptographic primitives do not support search operations over encrypted data. If a piece of data is required, a trivial solution is that the user downloads all the content to its local (trusted) environment, decrypts the data, and performs the search operation. Unfortunately, this trivial solution does not scale well when the database is very large. Alternatively, we can provide the CSP with the key to decrypt all data. Then, the CSP can search the decrypted data to retrieve the required part. This method is used in most of the commercial public cloud services, such asAmazonS3 However, this approach still allows the CSP to learn the content of data and queries.

Considering one application scenario of PHR file sharing in electronic medical system, the basic information of patients from different departments can be accessed by all medical staff. Medical workers from different departments can access the PHR file

data which is relevant to their department. Even the workers from the same department, they access different parts of data in accordance with their privilege that is determined by their title, occupation and some other attributes. For example, there is a medical worker who has the highest privilege in neurology department and a medical employee has the best privilege in medicine department. Both of them can access the basic information parts of the PHR files belonging to patients from the two departments. Although each of them has the highest privilege in its own department, one can access some parts that the other can't access and vice versa. The challenge is a way to give a fine-grained and multi-privilege access management theme at low value during this case.

To motivate our design, we consider the following scenario in a smart PHR system. Assume that there are various doctors in different hospitals and they can write information to PHRs. Due to the sensitive nature of the data, the access right will always be restricted to certain clients only. For example, a general practitioner could be authorized to read the records of their patients only, whereas a cardiologist could be authorized to read all records relating to heart conditions. In addition, patients may go to more than one hospital, and doctors may want to read patient's former records for diagnosis in another hospital. Therefore, the clients should be enforced with read and search privileges under a scenario of multiple authorities. Furthermore, due to the privacy of medical data, the access control of the data should be refined to authorized keywords for searching. For example, cardiologists are only authorized to query medical information about heart disease and cannot search a patient's history of skin diseases. Therefore, the search capability of the clients must be managed so that they are only allowed to perform queries for authorized keywords.

2. EXISTING SYSTEM

In existing system each and every one can store the data in cloud. Day by day cloud user's increases rapidly. Secure search over encrypted remote knowledge is crucial in cloud computing to ensure the info privacy and usefulness. Fine-grained access control is necessary in multi-user system. However, licensed user could by choice leak the key for money. Also because of the high value of building and maintaining specialized knowledge centers, several PHR services are outsourced to or provided by different service suppliers for e.g. Microsoft Health Vault. The main concern is concerning whether or not the patients might truly management the sharing of their sensitive personal health data, particularly after they are hold on another sever which individuals may not fully trust.

3. LITERATURE REVIEW

1 .Title: Fine-grained Access Control for Personal Health Records in Cloud Computing

Year: 2017

Details: Paper presents a completely unique access management theme for private health record (PHR) knowledge in cloud computing. The scheme utilizes attribute-based encryption (ABE), hash function and symmetric encryption to realize a fine-grained, multi-privilege access control to PHR. The patients will share their PHR with medical workers from varied departments with completely different privileges firmly. The experimental results show the efficiency of our scheme in terms of running-time, communication cost and storage overhead.

2. Title: Enabling Encrypted Rich Queries in Distributed Key-value Stores.

Year: 2018

Details: Paper presents to accommodate large digital information, distributed information stores became the most resolution for cloud services. Among others, key-value stores are widely adopted due to their superior performance. But with the rapid growth of cloud storage, there are growing concerns about data privacy. In this paper, we design and build EncKV, an encrypted and distributed key-value store with rich query support. First, EncKV partitions data records with secondary attributes into a set of encrypted key-value pairs to hide relations between data values. Second, EncKV uses the most recent scientific discipline techniques for looking on encrypted information, i.e. searchable symmetric encryption (SSE) and order-revealing encryption (ORE) to support secure exact-match and range-match queries, respectively. It any employs a framework for encrypted and distributed indexes supporting question process in parallel. To address inference

attacks on ORE, EncKV is equipped with an enhanced ORE scheme with reduced leakage. For sensible issues, EncKV also enables secure system scaling in a minimally intrusive way. We complete the example implementation and deploy it on Amazon Cloud. Experimental results ensure that EncKV preserves the potency and quantify ability of distributed key-value stores.

3 .Title: Secure Data Sharing of Personal Health Records in Cloud Using Fine-Grained and Enhanced Attribute-Based Encryption

Year: 2018

Details: Paper presents a Personal Health Records (PHR) is essential health related management system to preserve the health data for someone. These facts are stored on un-trusted servers which make secure Information sharing System. The accessing process of cloud servers are normally access by 3rd-User, Generally the PHR policies done through on these cloud, the Major Encryption Strategies is used can be carried out – encrypted Public Health Records are stored on storage Cloud. To recommend these troublesome commitments, the Enhanced Attribute-Based Encryption (ABE) strategies are used. Fine-grained information collects the right of entry to manipulate is guaranteed on un-trusted servers. In these methodologies, the data owners are in charge of encrypting the data before upload or downloading them on the cloud and also re-encryption done when there is a change in client credentials. To perform the fine–grained enhanced ABE is able to access the information data securely for PHR from these access and share each patient's PHR file by securely. The results show the efficient and effectiveness of our methodology for data access and sharing in cloud computing. Our methodical approach will reasonable for the resources constrained gadgets. Our Approach will diminish the computational cost of customers is finished by outsourcing process.

4. PROPOSED SYSTEM

In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. Also, propose a novel healthcare recommendation system which work in the aspects of user preference and doctor feature extraction. We compare with previous healthcare recommendation methods & dataset details results which can provide a higher predication rating and increases the accuracy of healthcare recommendation significantly.

Advantages:

1. More secure.

2. There is no unauthorized data usage.

3. Authorized person should generate the user secret key.

4. We can easily find the malicious users.

4.1 Modules Information

1) Module 1: (GUI and Cloud Setup)

This module contains GUI, registration, login of users and setup for cloud.

2) Module 2: (Access Structure creation)

In this module a data owner generate access structure and send to TPA.

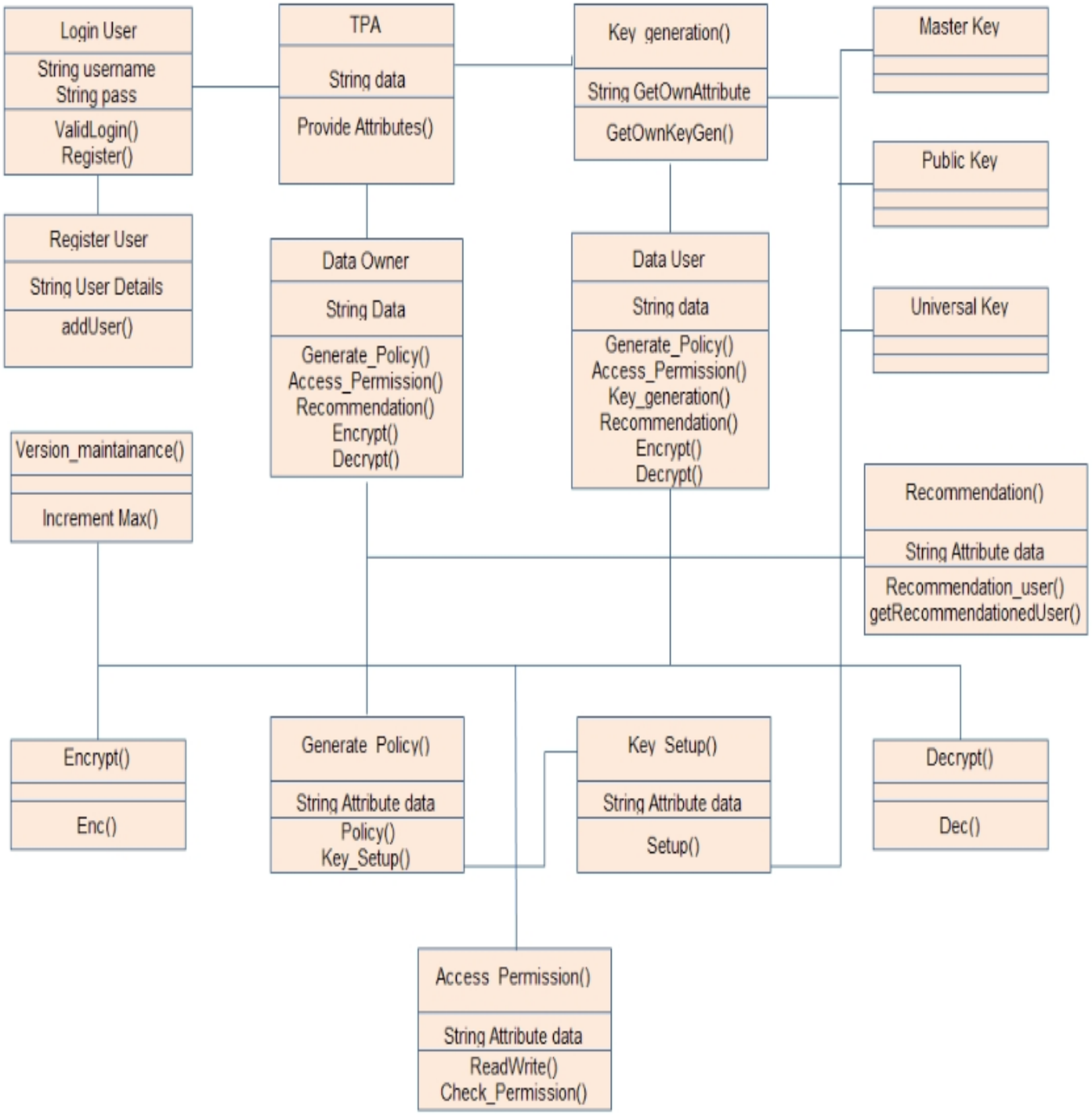
3) Module 3: (Third Party Auditor)

This module consists of Third Party Auditor who is responsible to distribute Encryption and Decryption data to store on cloud and send to personal domain.

4) Module 4: (Contribution Work)

In this module we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file with secure file access gain policies & scalable offering doctor Recommendation System.

4.2 Architecture



5. ALGORITHM

A] AES

AES Algorithm

• AES is a symmetric block cipher that it uses the same key for both encryption and decryption.

• The AES standard states that the algorithm can only accept a block size of 128 bit.

• The entire data block is processed in parallel during each round using substitutions and permutations.

• Single 128 bit block in decryption and encryption use as input and is known as the in matrix.

Inner Workings of a Round: The algorithm begins with an Add round key stage followed by 9 rounds of four stages and a tenth round of three stages. For both encryption and decryption this applies with the exception that each step of a round the decryption algorithm is the opposite of its counterpart in the encryption algorithm. The four steps are as follows:

1. Substitute bytes.

2. Shift Rows.

3. Mix Columns.

4. Add Round Key.

The tenth round simply leaves out the Mix Columns stage. The first nine rounds of the decryption algorithm consist of the following:

1. Inverse Shift rows.

2. Inverse Substitute bytes.

3. Inverse Add Round Key.

4. Inverse Mix Columns

5.1 Methodology Implementation:

1] User System first encrypts the plaintext (Normal Information) then create index (i.e metadata) and encrypt it.

2] Encrypted index is authenticated with homomorphic MAC technique. This produces authentication tags for the encrypted index.

a] The holder of a dataset{m1,...,m} uses her secret key sk to produce corresponding tags (σ1,...,σl) and stores the authenticated dataset on a remote server.

b] Later the server can (publicly) compute m p= $f(m_1,...,m_l)$ together with a succinct tag σ certifying that m is the correct output of the computation f.

c] A nice feature of homomorphic authenticators is that the validity of this tag can be verified without having to know the original dataset.

3] Next, the index and authentication tags are uploaded to the cloud. Then the client can generate a search trapdoor, and uses our homomorphic MAC technique to authenticate the trapdoor.

4] With the authenticated trapdoor, the cloud server can homomorphically execute the search function over the authentication tags to derive the result with a proof, which can certify the search result.

6. CONCLUSION

In this paper we proposed privacy, access and control of health care data on cloud using recommendation system cloud storage. to provides PHR system where are multiple PHR owners and PHR users .personal health record (PHR) is an rising patient-centric model of health data exchange, which is often outsourced to be stored at a third party, such as cloud providers.

REFERENCES

1] Li, W., Ni, W., Liu, D., Liu, R. P., Wang, P., & Luo, S. (2017). Fine-Grained Access Control for Personal Health Records in Cloud Computing. 2017 IEEE 85th Vehicular Technology Conference(VTCSpring). doi:10.1109/vtcspring.2017.8108549.

2] Guo, Y., Yuan, X., Wang, X., Wang, C., Li, B., & Jia, X. (2018). Enabling Encrypted Rich Queries in Distributed Key-value Stores. IEEE Transactions on Parallel and Distributed Systems, 1–1.

3] Selvam, L., & Arokia, R. J. (2018). Secure Data Sharing of Personal Health Records in Cloud Using Fine-Grained and Enhanced Attribute-Based Encryption. 2018 International Conference on Current Trends Towards Converging Technologies (ICCTCT).

4] Z. Deng, K. Li, K. Li, and J. Zhou, "*A multi-user searchable encryption scheme with keyword authorization in a cloud storage*," Future Generation Comput. Syst., vol. 72, pp. 208–218, 2017.

5] Guoxing Chen, Ten-Hwang Lai, Michael K. Reiter, and Yinqian Zhang. *Differentially private access patterns for searchable symmetric encryption*. In INFOCOM 2018, pages 810–818. IEEE, 2018.

BIOGRAPHIES

Miss. Reshma Borhade, Student, Bachelor of Engineering, Dept. Of Computer Engineering, Sahyadri Valley COE & Technology, Pune.

Miss. Pratiksha Pansare, Student, Bachelor of Engineering, Dept. Of Computer Engineering, Sahyadri Valley COE & Technology, Pune.

Miss. Seema Aher, Student, Bachelor of Engineering, Dept. Of Computer Engineering, Sahyadri Valley COE & Technology, Pune.

Prof. Sachin Dighe, Assistant Professor, Dept. Of Computer Engineering, Sahyadri Valley COE & Technology,