Dynamic Traceable Permission Search System For Secure Cloud Storage

D Guru Teja[1], R Hendra Kumar[2]
[1, 2] Dept of CSE
[2]Associate Professor, Dept of CSE
[1, 2]KMMInstituteofTechnology&Science,Ramireddipalli,AndhraPradesh-517 102

Abstract- *Medical Field is an Emerging Technology. Where only some doctors providing access to the patients to search her medical data from the server. Encrypting the data before outsourcing is a commonly used approach, where the patient only needs to send the corresponding encryption key to the authorized doctors. But all people's wants an access for outsource her medical data from the server. This is the limitation in previous existing systems. In this paper, we propose two Secure and Efficient Dynamic Searchable Symmetric Encryption (SEDSSE) schemes over medical cloud data. Firstly, we leverage the secure k-Nearest Neighbor (kNN) and Attribute-Based Encryption (ABE) techniques to propose a dynamic searchable symmetric encryption scheme, which can achieve two important security features, i.e., forward privacy and backward privacy which are very challenging in the area of dynamic searchable symmetric encryption. Compared with existing proposals, our schemes are better in terms of storage, search and updating complexity. Extensive experiments demonstrate the efficiency of our schemes on storage overhead, index building, trapdoor generating and query*

Keywords- SEDSSE, kNN, ABE, Trusted authority, Cloud Server

I. INTRODUCTION

The main aim of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games. In this section we are discussing about previous existing systems Jiangnan Li, Xiangyu Niu, Jinyuan Stella Sun [1] review and give a comparison of the state-of-the-art searchable symmetric encryption schemes, and analyze why these schemes are not appropriate for smart grid application. Finally, they implement a prototype based on statistical AMI data to show the effectiveness of our scheme

V. NAVEEN KUMAR, A. SIVA SANKAR [2] they proposed 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 kNN based searchable encryption scheme. Performance evaluation demonstrates that the proposed schemes can achieve better efficiency

Dr.G. Sushmitha Valli, Harika Arete [3] paper, they reviewed different techniques available for de duplication. Different levels of data de duplication strategies are covered. They include block level techniques, byte level techniques and file level techniques. It also covers general de duplication process and how it works. The data de duplication technology is presented. In future they intend to research on medical records for more effective and secure de duplication

Dr. A. Radhakrishnan, Ajilin Femi. T, Theepshika. L [4] designed and implemented a cloud based electronic health records system. Cloud computing is a trending technology and it offers many advantages like low cost, data backup recovery etc. The solution in this paper solves the problem of denial of medical records among the medical institutions. And this system is also useful in emergency situations

Chen Guo, Xingbing Fu, Yaojun Mao, Guohua Wu, *, Fagen Li and Ting Wu [5] scheme only supports single- keyword search. In our future work, they will consider how to make our scheme support multi-keyword search, which can achieve expressive search operations in multi-user settings. In addition, they will consider the verifiability of search results

II. PROPOSED SYSTEM DESIGN

In this section we are discussing about proposed system architecture which is shown in the below Fig.1. Fig.2 and Fig.3 shows data flow diagrams for cloud server and data owners

Fig.1 Proposed System Architecture

Cloud Server:

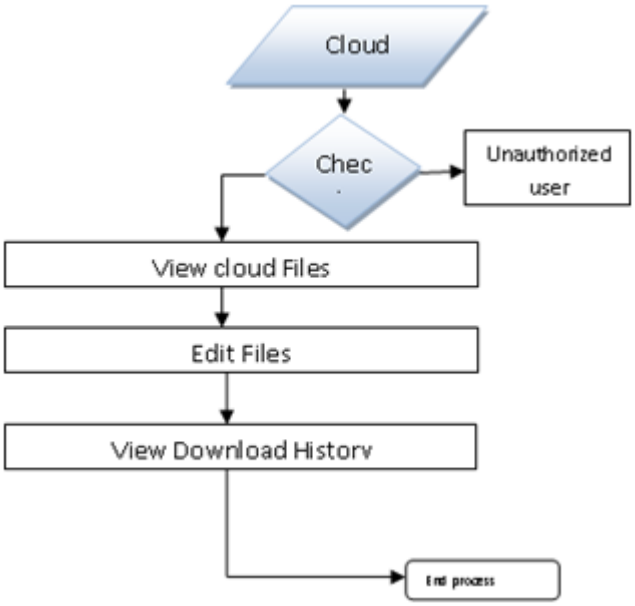

Fig.2 Data Flow diagram for Cloud Server

Data Owner:

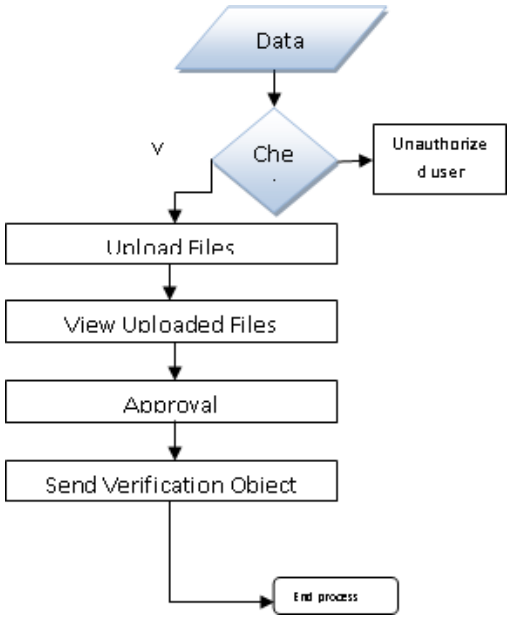

Fig.3 Data Flow diagram for Cloud Server

III. IMPLEMENTATION OF PROPOSED SYSTEM

In this section we are discussing about implementation of proposed system in the form of 4 modules that are

- ❖ Trusted authority
- ❖ Patient
- ❖ Cloud server
- ❖ Doctor

Trusted authority:

A trusted authority (TA) is a trusted third party. We use it to generate attribute-based encryption (ABE) key to encrypt the medical documents. Patients' documents will be encrypted and only some doctors satisfying the corresponding access policy can decrypt them.

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.

IV. RESULTS AND DISCUSSIONS

In this section we are discussing about results shown in below figures. For checking the reports from server patient should login first. That means patient should register by entering his / her details shown in below Fig.4

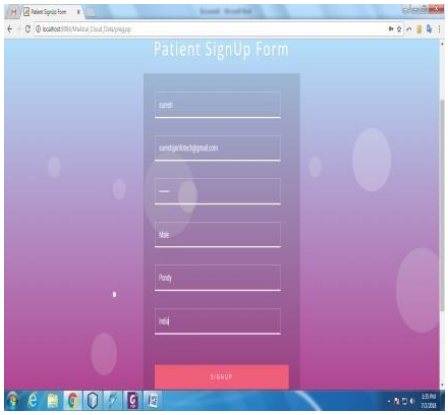

Fig.4PatientRegistrationForm

After that patient can directly go for login and upload his / her files. Next doctors can login to their accounts as shown inbelowFig.5

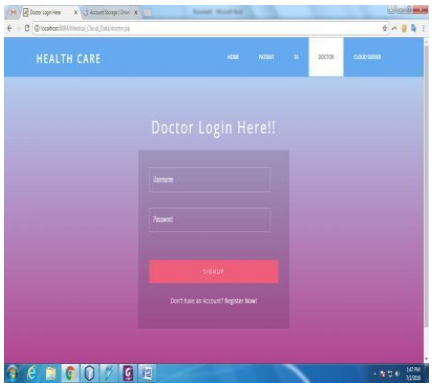

Fig.5DoctorsLoginPage

Trusted authorities also go for login page. And enter their details. So they will go for their account. Next attributed based key was generated to the file as shown inbelowFig.6

Fig.6 ABE Key Generated

Doctors can approve it. After that patients will enter the key to search their reports

V. CONCLUSION

In this paper, we propose two dynamic searchable encryption schemes with high security level. The first one cannot 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 kNN based searchable encryption scheme. 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] Jiangnan Li, Xiangyu Niu, Jinyuan Stella Sun, “A Practical Searchable Symmetric Encryption Scheme for Smart Grid Data”, arXiv:1808.00645v2 [cs.CR] 30 Oct 2018

[2] V.NAVEEN KUMAR, A. SIVA SANKAR, “Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data”, IJECEC, ISSN(Online):2533-8945 VOLUME 5 ISSUE 6

[3] Dr.G. Sushmitha Valli, Harika Arete, “A Survey of Secure and Deduplication Frameworks for Cloud Based Application”, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 9, ISSUE 04, APRIL 2020 ISSN 2277-8616

[4] Dr. A. Radhakrishnan, Ajilin Femi. T, Theepshika. L, “Secure Management of Health Care Data using Cloud Computing”, International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887 Volume 7 Issue III, Mar 2019

[5] Chen Guo, Xingbing Fu, Yaojun Mao, Guohua Wu, *, Fagen Li and Ting Wu, "Multi-User Searchable Symmetric Encryption with Dynamic Updates for Cloud Computing", mdpi, Information 2018, 9, 242; doi:10.3390/info9100242