DATA AUTHENTICATION FOR ELECTRONIC MEDICAL RECORDS

M. Navaneethakrishnan, Professor of Computer Science Engineering,
Surya Kumar M, Student of Computer Science Engineering,
Ragulraj K, Student of Computer ScienceEngineering,
St. Joseph College of Engineering, Sriperumbudur, Chennai.

ABSTRACT:

With cloud storage services, users can remotely store their data to the cloud and realize the data sharing with others. Remote data integrity auditing is proposed to guarantee the integrity of the data stored in the cloud. In some common cloud storage systems such as the Electronic Health Records (EHRs) system, the cloud file might contain some sensitive information. The sensitive information should not be exposed to others when the cloud file is shared. Encrypting the whole shared file can realize the sensitive information hiding, but will make this shared file unable to be used by others. How to realize data sharing with sensitive information hiding in remote data integrity auditing still has not been explored up to now. In order to address this problem, we propose a remote data integrity auditing scheme that realizes data sharing with sensitive information hiding in this paper. In this scheme, a sanitizer is used to sanitize the data blocks corresponding to the sensitive information of themfile and transforms these data blocks' signatures into valid ones for the sanitized file. These signatures are used to verify the integrity of the sanitized file in the phase of integrity auditing. As a result, our scheme makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing is still able to be efficiently executed. Meanwhile, the proposed scheme is based on identity-based cryptography, which simplifies the complicated certificate management. The security analysis and the performance evaluation show that the proposed scheme is secure and efficient.

Keywords:EHR-Electronic Health Records, SQL-Standard Query Language, MAIBS –Multiple authorities of identity based signature scheme.

INTRODUCTION:

Cloud based health system's main focus is the patient's data collection, storage, access,analysis, and presentation etc. The current patient data collection techniques are time consuming,inefficient, laborious for the staffs. It is also obvious that currents technique is violating the real time data access for monitoring the patients.

LITERATURE SURVEY:

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 EncryptionPersonal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. 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. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

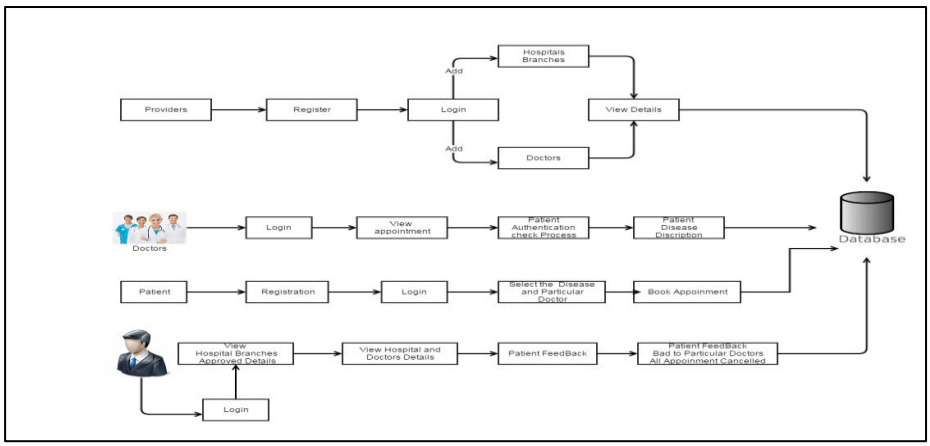
H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng.An SMDP-Based Service Model for Inter domain Resource Allocation in Mobile Cloud Networkssecure dynamic searchable symmetric encryption scheme. Our scheme can achieve two important security features, i.e., forward privacy and backward privacy which are very challenging in Dynamic Searchable Symmetric Encryption (DSSE) area. In addition, we evaluate the performance of our proposed scheme compared with other DSSE schemes. The comparison results demonstrate the efficiency of our proposed scheme in terms of the storage, search and update complexity.

Yang, H. Li, L. Wenchao, H. Yang, and W. MiSecure Dynamic Searchable Symmetric Encryption with Constant Document Update Cost has developed.With the development of cloud computing, data sharing has a new effective method, i.e., outsourced to cloud platform. In this case, since the outsourced data may contain privacy, they only allow to be accessed by the authorized users. In this paper, we leverage the secure k-nearest neighbor to propose. Mobile cloud computing is a promising technique that shifts the data and computing service modules from individual devices to geographically distributed cloud service architecture. In this paper, we propose a service decision making system for inter domain service transfer to balance the computation loads among multiple cloud domains. To this end, we formulate the service request decision making process as a semi-Markov decision process. The optimal service transfer decisions are obtained by jointly considering the system incomes and expenses. Extensive simulation results show that the proposed decisionmaking system can significantly improve the system rewards and decrease service disruptions compared with the greedy approach.

Q. Shen, X. Liang, X. Shen, X. Lin, and H. LuoExploiting Geo-Distributed Clouds for a E-Health Monitoring System With Minimum Service Delay and Privacy Preservation.In this paper, we propose an e-health monitoring system with minimum service delay and privacy preservation by exploiting geo-distributed clouds. In the system, the resource allocation scheme enables the distributed cloud servers to cooperatively assign the servers to the requested users under the load balance condition. Through the numerical analysis, we show the efficiency of the proposed traffic-shaping algorithm in terms of service delay and privacy preservation. Furthermore, through the simulations, we demonstrate that the proposed resource allocation scheme significantly reduces the service delay compared to two other alternatives using jointly the short queue and distributed control law.

SYSTEM DESIGN:

Cloud based health system solution is based on the concept of "Cloud Computing" a distributed computing system where a pool of virtualized, dynamically-scalable, managed computing power, storage, platforms, and services are delivered. This system provides an environment where patient's records are stored and it will be referenced by the doctors to improve the efficiency of the treatment. This handles the medical history of each individual of the country and provides access to all registered hospitals to read or update the data. The hospital which accesses the database must be registered and must have got a license. The license number is used as a unique code to access the database. The details of the patients will be stored and an identification number will be generated when their data are stored into the database for the first time after the implementation of the system. Whenever they go for a treatment, their medical data will be stored into the database using their identification number. For security reasons, any person who wants to view their data will be allowed only to read the data. They will not be given access to update the database. For hospitals to update the database they require the license number along with the identification number of the person whose record has to be stored.



ARCHITECTURE DIAGRAM

SYSTEM IMPLEMENTATION:

A software application in general is implemented after navigating the complete life cycle method of a project. Various life cycle processes such as requirement analysis, design phase, verification, testing and finally followed by the implementation phase result in a successful project management. System implementation is an important stage of theoretical design is turned into practical system.

Implementation Procedure:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user and so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly. The final stage is to document the entire system which provides components and the operating procedures of the system.

CONCLUSION AND FUTURE ENHANCEMENT:

CONCLUSION:

In this project, proposed a system which monitors the health care details of each individual of the country. It comprises of modules like generating the unique ID and store and retrieve data of a person. The cloud computing is an emerging computing mode. It promises to increase the velocity with which applications are deployed, increase innovation, and lower costs, all while increasing business agility. The nature of cloud computing is useful for constructing the data center. To the new generation of cloud based health system, cloud computing is better approach in the future.

Future Work:

The need of an online certificate authority (CA) and one unique key encryption for each symmetric key k for data encryption at the portal of authorized physicians made the overhead of the construction grow linearly with size of the group. Furthermore, the anonymity level depends

on the size of the anonymity set making the anonymous authentication impractical in specific surroundings where the patients are sparsely distributed.

REFERENCE:

1. M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A Berkeley View of cloud computing," Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, Tech. Rep. UCB/EECS-2009-28, 2009.
2. D. Huang, X. Zhang, M. Kang, and J. Luo, "Mobicloud: A secure mobile cloud framework for pervasive mobile computing and communication," in Proc. 5th IEEE Int. Symp. Service-Oriented Syst. Eng., 2010, pp. 27–34.
3. E. Cuervo, A. Balasubramanian, D.-K. Cho, A. Wolman, S. Saroiu, R. Chandra, and P. Bahl, "MAUI: Making smartphones last longer with code offload," in Proc. ACM MobiSys, 2010, pp. 49–62.
4. M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," IEEE Pervasive Computers., vol. 8, no. 4, pp. 14–23, Oct.–Dec. 2009.
5. B. Chun and P. Maniatis, "Augmented smartphone applications through clone cloud execution," in Proc. USENIX HotOS XII, 2009, p. 8.
6. R. Jain, "Quality of experience," IEEE Multimedia, vol. 11, no. 1, pp. 95– 96, Jan.–Mar. 2004.
7. Secure Networking and Computing (SNACT) Research Group, Mobicloud. [Online]. Available: http://mobicloud.asu.edu/
8. M. Puterman, Markov Decision Processes: Discrete Stochastic Dynamic Programming. New York: Wiley, 2005.
9. S. M. Ross, Introduction to Probability Models, 9th ed. New York: Elsevier, 2007.
10. C. E. L. Thomas, H. Cormen, R. L. Rivest, and C. Stein, Introduction to Algorithms, 3rd ed. Cambridge, MA: MIT Press, 2009.
11. X. H. Li, H. Zhang, and Y. F. Zhang, "Deploying mobile computation incloud service," in Proc. 1st Int. Conf. CloudCom, 2009, pp. 301–311.
12. X. Zhang, J. Schiffman, S. Gibbs, A. Kunjithapatham, and S. Jeong,"Securing elastic applications on mobile devices for cloud computing," in Proc. ACM Workshop Cloud Computer. Security, 2009, pp. 127–134.

BIOGRAPHY:

Dr. M. Navaneethakrishnan M.E., PhD is a Head of the Department in the Department of Computer Science and Engineering at St. Joseph College of Engineering, Sriperumbudur, Chennai, Tamil Nadu. He has completed his Ph.D, in Cyber Security - Computer Science and Engineering in 2017 from Manonmaniam Sundaranar University (MSU) Tirunelveli, Tamilnadu. He has done his M.E, CSE in Anna University Chennai in the year 2008

Surya Kumar M, Student of Computer Science Department, St. Joseph College of Engineering, Sriperumbudur, Chennai. I had attended workshops, participated in blockchain webinar. I have also attended the conference on blockchain which is conducted by Indian Institute of Technology, Kanpur and E&ICT Academy.

Ragulraj K, Student of Computer Science Department, St. Joseph College of Engineering, Sriperumbudur, Chennai.I had attended workshops, participated in blockchain webinar. I have also attend the conference on blockchain which is conducted by Indian Institute of Technology, Kanpur and E&ICT Academy.