ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Special Issue 2, March 2019

Sharing and Monitoring of Medical Health Records

T.Yeswanth[1], S.Sathyanarayanan[2], K.Mohammed ziaudeen[3], Dr.E.Sujatha[4]

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology. Chennai, Tamil Nadu, India [1]

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology. Chennai, Tamil Nadu, India [2]

UG Student, Department of Computer Science and Engineering, Velammal Institute of Technology. Chennai, Tamil Nadu, India [3]

Professor, Department of Computer Science and Engineering, Velammal Institute of Technology. Chennai, Tamil Nadu, India [4]

ABSTRACT: Unsecured sharing of data leading to major medical flaws and organ theft is a serious issue hence to address this issue and to provide solution a semi-confided in intermediary called setup and Re-encryption Server (SRS) is acquainted with setting up people in general/private key combines and to create the re-encryption keys. Besides, the technique is secure against insider dangers and furthermore implements a forward and in reverse access control. Besides, formally dissect and confirm the working of secure sharing philosophy through the High-Level Petri nets. Execution assessment with respect to time utilization shows that the Secure Sharing Of Personal Health Records can possibly be utilized for safely sharing the PHRs in the cloud. A user wants the organs or if he wants to donate the organs he can approach to the hospitals. The donor can send the request to the hospital to test the process or the organ. The hospital module is used to test the organs which are donated by the donor. If the hospital tested the organs which were donated, that particular organ will be viewed by the sponger, where they can select the organs of their use. The admin can be able to view all the details of the owners and the details of sponger and also about the hospital request. All the information is securely outsourced to the cloud server.

I. OBJECTIVE

This work focuses on the multi-data owner/patient scenario, where the PHR system users are divided into two security domains-the private domain and public domain, each of which is encrypted using its own set of mechanisms. We present the advantages of using the Hierarchical Attribute Set Based Encryption (HASBE) technique rather than the Multi-Attribute ABE, an extension of Cipher text ABE, for situations where complex access control policies are required. Hierarchical ASBE uses dynamic constraints while combining attributes and thereby provides greater flexibility.

II. EXISITING SYSTEM

The cloud computing also integrates various important entities of healthcare domains,such as patients, hospital staff including the doctors, nursing staff, pharmacies, and clinical laboratory personnel, insurance providers, and the service provider.Therefore, the integration of aforementioned entities results in the evolution of a cost effective and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

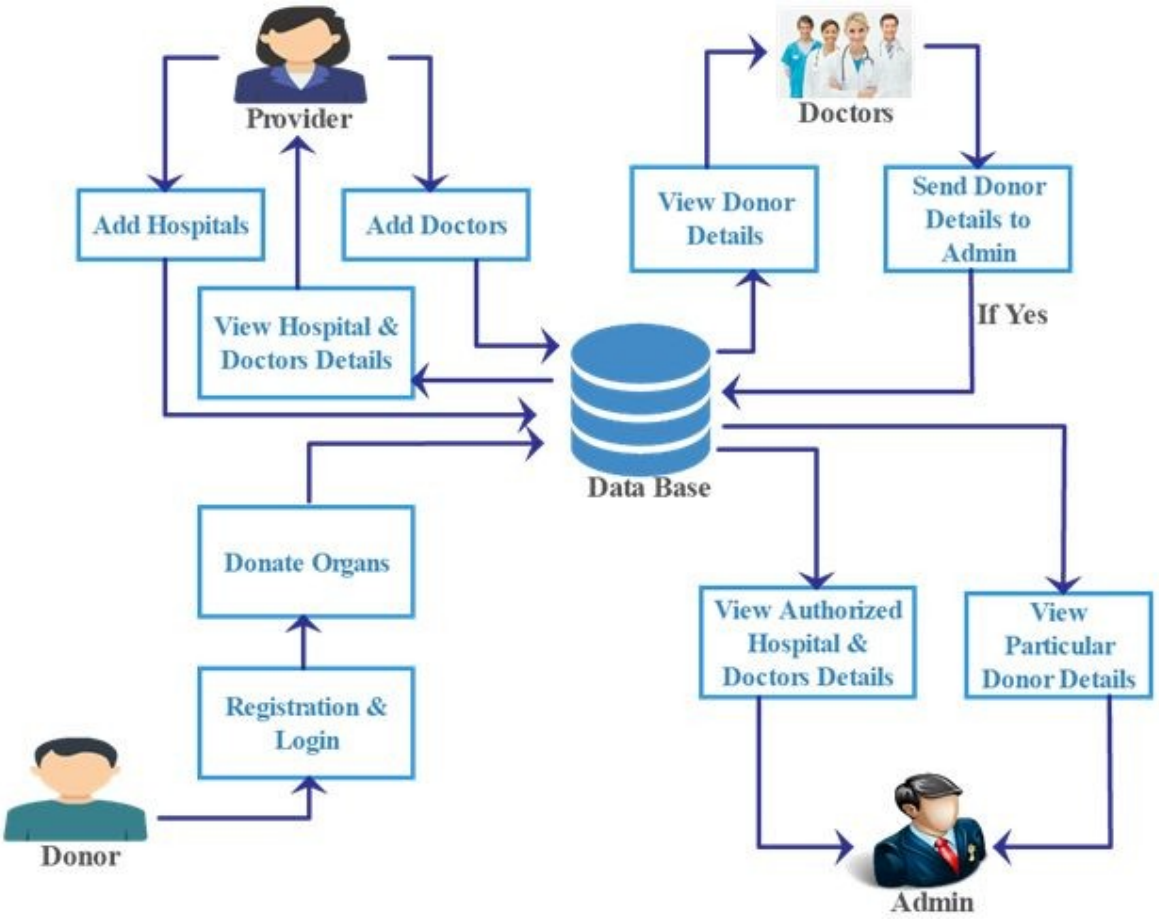
Vol. 8, Special Issue 2, March 2019

collaborative health ecosystem where the patients can easily create and manage their Personal Health Records (PHRs). Generally, the PHRs contain information, such as: (a) demographic information, (b) patients' medical history including the diagnosis, allergies, past surgeries, and treatments, (c) laboratory reports,(d) data about health insurance claims, and (e) private notes of the patients about certain important observed health conditions.

III. PROPOSED SYSTEM

The proposed system of this project is the donor can register their details including the organs which they are ready to donate their organs. The sponger means the getting the organs from the donor. By clicking the request the sponger can get the organs. The organ can be donated by the donor. There will be a register form who wants to donate the organs or getting the organs through the hospital. The donor who wants to get the organ or want to donate the organ can also request or approaches to the hospital. The donor who wants to test the organs can also request to the hospital. The sponger can also get the organ through the hospital donations.

Architecture Diagram:



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Special Issue 2, March 2019

Literature Survey

Communication of Medical Images, Text,and Messages in Inter-Enterprise Systems: A Case Study in Norway
YEAR: VOL. 11, NO. 1, JANUARY 2007

AUTHOR: Ilangko Balasingham, Member, IEEE, Halfdan Ihlen, Wolfgang Leister, Per Røe, and Eigil Samset

ABSTRACT:

- There is an increasing demand to discuss diagnostic images and reports of difficult cases with experienced staff. A possible solution besides physically transporting patients and material is to use high-speed communication networks to transfer images and reports electronically. With the web application PACSflow we have developed a solution to transfer images, reports, and messages as a single package in a one-step procedure.
- The PACSflow is an interoperable and standard compliant web-based application, which gives clinicians a user-friendly in terface for their work on a daily basis. The solution assumes that the diagnostic images are compatible with the digital imaging and communications in medicine (DICOM) format.
- The Department of Cardiology at the Rikshospitalet University Hospital in Oslo, Norway, and the Department of Internal Medicine at the Sørlandet Sykehus in Arendal, Norway, are making clinical use of the system. Initial tests indicate that use of PACSflow has reduced the time required to prepare and transfer data by a factor of 3.

An SMDP-Based Service Model for Interdomain Resource Allocation in Mobile Cloud Networks

AUTHOR: Hongbin Liang, Student Member, IEEE, Lin X. Cai, Member, IEEE,Dijiang Huang, Senior Member, IEEE, Xuemin (Sherman) Shen, Fellow, IEEE, and Daiyuan Peng, Member, IEEE
YEAR: VOL. 61, NO. 5, JUNE 2012

ABSTRACT:

- Mobile cloud computing is a promising technique that shifts the data and computing service modules from individual devices to a geographically distributed cloud service architecture. A general mobile cloud computing system is comprised of multiple cloud domains, and each domain manages a portion of the cloud system resources, such as the Central Processing Unit, memory and storage, etc. How to efficiently manage the cloud resources across multiple cloud domains is critical for providing continuous mobile cloud services. In this paper, we propose a service decision making system for interdomain service transfer to balance the computation loads among multiple cloud domains.
- Our system focuses on maximizing the rewards for both the cloud system and the users by minimizing the number of service rejections that degrade the user satisfaction level significantly. 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 decision making system can significantly improve the system rewards and decrease service disruptions compared with the greedy approach.

Exploiting Geo-Distributed Clouds for a E-Health Monitoring System With Minimum Service Delay and Privacy Preservation

AUTHOR: Qinghua Shen, Student Member, IEEE, Xiaohui Liang, Student Member, IEEE, Xuemin (Sherman) Shen, Fellow, IEEE, Xiaodong Lin, Senior Member, IEEE, and Henry Y. Luo
YEAR: VOL. 18, NO. 2, MARCH 2014

ABSTRACT

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. Thus, the service delay for users is minimized. In addtion, a traffic-shaping algorithm is proposed.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Special Issue 2, March 2019

- The traffic-shaping algorithm converts the user health data traffic to the nonhealth data traffic such that the capability of traffic analysis attacks are largely reduced. 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

IV. 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.

REFERENCES

1. Sawand, S. Djahel, Z. Zhang, and F. Naït-Abdesselam, "Toward Energy-Efficient and Trustworthy eHealth Monitoring System, " China Commun., vol.12, no. 1, pp. 46-65, Jan. 2015.
2. M. S. Shin, H. S. Jeon, Y. W. Ju, B. J. Lee, and S. P. Jeong, "Constructing RBAC Based Security Model in u-Healthcare Service Platform," The Scientific World J., vol. 2015, Article ID 937914, 13 pages, http://dx.doi.org/10.1155/2015/937914, 2015.
3. C. Wang, B. Zhang, K. Ren, J. M. Roveda, C. W. Chen, and Z. Xu. "A Privacy-aware Cloud-assisted Healthcare Monitoring System via Compressive Sensing," in Proc. of 33rd IEEE INFOCOM, 2014, pp. 2130-2138.
4. M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," in Proc. of 35th IEEE Symp. on Security and Privacy, 2014, pp. 524-539.
5. C. Bekara and M. Laurent-Maknavicius, "A New Protocol for Securing Wireless Sensor Networks against Nodes Replication Attacks," in Proc. of 3rd IEEE Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), 2007, pp. 59-59.
6. P. T. Sivasankar and M. Ramakrishnan, "Active key management scheme to avoid clone attack in wireless sensor network," in Proc. of 4th Int. Conf. on Computing, Communications and Networking Technologies (ICCCNT'13), 2013, pp. 1-4.
7. Marcos, J. Simplicio, H. I. Leonardo, M. B. Bruno, C. M. B. C. Tereza, and M. N¨aslund, "SecourHealth: A Delay-Tolerant Security Framework for Mobile Health Data Collection," IEEE J. Biomedical and Health Informatics (IEEE Trans. INF TECHNOL B), vol. 19, no. 2, pp. 761-772, Mar. 2015.
8. R. X. Lu, X. D. Lin, and X. M. (Sherman) Shen, "SPOC: A Secure and Privacy-Preserving Opportunistic Computing Framework for Mobile-Healthcare Emergency," IEEE Trans. Parall. distr., vol. 24, no. 3, pp. 614-624, Mar. 2013.
9. Amirbekyan and V. Estivill-Castro, "A New Efficient Privacy-Preserving Scalar Product Protocol," in Proc. of Sixth Australasian Conf. Data Mining and Analytics (AusDM '07), 2007, pp. 209-214.