International Journal of Gender, Science and ..ISSN: 2040-0748
UGC Care Group I Journal Vol-13 Issue-01 June 2024

Electronic Health Record Databases That are Dynamically Shared and Verifiable by the Public

Mrs. MOUNIKA.S [1], Mr. MURAHARI.P [2]

#1 Assistant professor in the department of IT at DVR & DR. HS MIC College ofTechnology (Autonomous), Kanchikacherla, NTR District.

#2 MCA student in the Department of Computer Applications (DCA) at DVR & DR.HS MIC COLLEGE OF TECHNOLOGY, Kanchikacherla, NTR District

ABSTRACT:

An electronic health record (EHR) is a system that collects and shares individuals' digital health information with other healthcare providers via the cloud. Because EHR contains a huge number of important and sensitive patient information, it is critical that the system maintains response accuracy and storage integrity. Meanwhile, with the rise of IoT, more low-performance terminals are being deployed to receive and upload patient data to the server, increasing the computational and communication stress on EHR systems. The verifiable database (VDB), in which a user outsources his huge database to a cloud server and conducts queries when he needs specific data, is presented as an efficient updatable cloud storage paradigm for resource-constrained users.

INTRODUCTION

With the development of healthcare big data and wearable technology [1], as well as cloud computing and communication technologies [2], cloud-assisted healthcare big data computing becomes critical to meet users' ever-growing demands on health consultation However, it is a challenging issue to personalize specific healthcare data for various users in a convenient fashion Previous work suggested the combination of social networks and healthcare service to facilitate the trace of the disease treatment process for the retrieval of Realtime disease information Healthcare social platform, such as Patients Like Me can obtain information from other similar patients through data sharing in terms of user's own findings. Though sharing medical data on the social network is beneficial to both patients and doctors, the sensitive data might be leaked or

stolen, which causes privacy and security problems without efficient protection for the shared data Therefore, how to balance privacy protection with the convenience of medical data sharing becomes a challenging issue.

With the advances in cloud computing, a large amount of data can be stored in various clouds including cloudlets and remote clouds facilitating data sharing and intensive computations However, cloud-based data sharing entails the following fundamental problems:

How to protect the security of user's body data during its delivery to a cloudlet?

How to make sure the data sharing in cloudlet will not cause privacy problem?

As can be predicted, with the proliferation of electronic medical records (EMR) and cloud-assisted applications, more and more attentions should be paid to the security problems regarding to a remote cloud containing healthcare big data. How to secure the healthcare big data stored in a remote cloud?

How to effectively protect the whole system from malicious attacks?

In terms of the above problems, this paper proposes a cloudlet-based healthcare system. The body data collected by wearable devices are transmitted to the nearby cloudlet. Those data are further delivered to the remote cloud where doctors can access for disease diagnosis. According to data delivery chain, we separate privacy protection into three stages. In the first stage, the user's vital signs collected by wearable devices are delivered to a closet gateway of cloudlet. During this stage, data privacy is the main concern. In the second stage, user's data will be further delivered toward remote cloud through cloudlets. A cloudlet is formed by a certain number of mobile devices whose owners may require and/or share some specific data contents. Thus, both privacy protection and data sharing are considered in this stage. Especially, we use trust model to evaluate trust level between users to determine sharing data or not. Considering the users' medical data are stored in remote cloud, we classify these medical data into different kinds and take the corresponding security policy. In addition to above three stages-based data privacy protection, we also consider collaborative IDS based on cloudlet mesh to protect the cloud ecosystem.

RELATED WORK

Feldman's Verifiable Secret Sharing for a Dishonest Majority

Verifiable secret sharing (VSS) protocols enable parties to share secrets while guaranteeing security (in particular, that all parties hold valid and consistent shares) even if the dealer or some of the participants are malicious. Most work on VSS focuses on the honest majority case, primarily since it enables one to guarantee output delivery (e.g., a corrupted recipient cannot prevent an honest dealer from sharing their value). Feldman's VSS is a well-known and popular protocol for this task and relies on the discrete log hardness assumption. In this paper, we present a variant of Feldman's VSS for the dishonest majority setting and formally prove its security. Beyond the basic VSS protocol, we present a publicly-verifiable version, as well as show how to securely add participants to the sharing and how to refresh an existing sharing (all secure in the presence of a dishonest majority). We prove that our protocols are UC secure, for appropriately defined ideal functionalities.

Public-Key Cryptosystems Based on Composite Degree Residuality Classes

This paper investigates a novel computational problem, namely the Composite Residuality Class Problem, and its applications to public-key cryptography. We propose a new trapdoor mechanism and derive from this technique three encryption schemes: a trapdoor permutation and two homomorphic probabilistic encryption schemes computationally comparable to RSA. Our cryptosystems, based on usual modular arithmetic's, are provably secure under appropriate assumptions in the standard model

A privacy-preserving data aggregation scheme for dynamic groups in fog computing

Fog computing has garnered significant attention in recent years, since it can bridge the cloud and terminal devices and provide low latency, location awareness, and geo distribution at the edge of the network. Data aggregation is a prime candidate for fog computing applications. However, most previous works about data aggregation do not focus on the fog computing. In addition, existing secure data aggregation schemes in fog computing usually do not support dynamic groups and arbitrary aggregation functions. In this paper, we construct concrete data encryption, data aggregation and data decryption algorithms, and further

propose a privacy-preserving and collusion-resistant data aggregation scheme for dynamic groups in fog computing. Specifically, in the proposed protocol, the cloud server can periodically collect raw data and compute arbitrary aggregation functions on them. Even if some malicious terminal devices collude with the fog device or the cloud server, the honest terminal devices' privacy cannot be breached. The fog device can filter out false data and aggregate all terminal devices' ciphertexts to save the bandwidth. Besides, dynamic join and exit of terminal devices is achieved. Detailed security analysis shows that our scheme holds k-source anonymity. Our scheme is also demonstrated to be efficient via extensive experiments.

METHODOLOGY

Wearable Device

In this module, the wearable device Collect Patient data and Upload to Cloudlet attach about symptoms with Digital sign, and view all patient collect data in encrypted format with digital sign.

Cloud Server

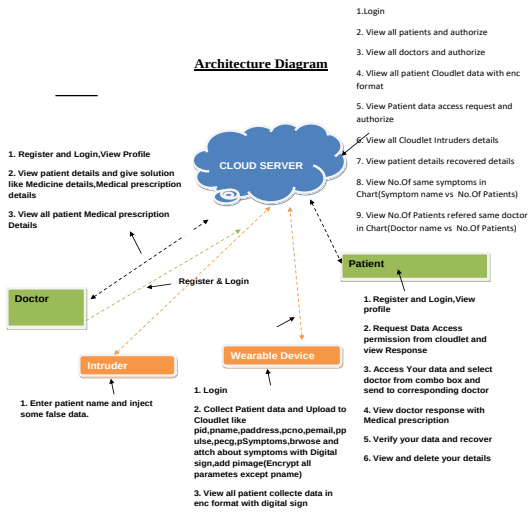
The Cloud server manages which is to provide data storage service for the wearable devices and also View all patients and authorize and view all doctors and authorize, View all patient Cloudlet data with enc format, View Patient data access request and authorize, View all Cloudlet Intruders details and View patient details recovered details, View No. Of same symptoms in Chart (Symptom name vs No. Of Patients), View No. Of Patients referred same doctor in Chart (Doctor name vs No. Of Patients).

Patient

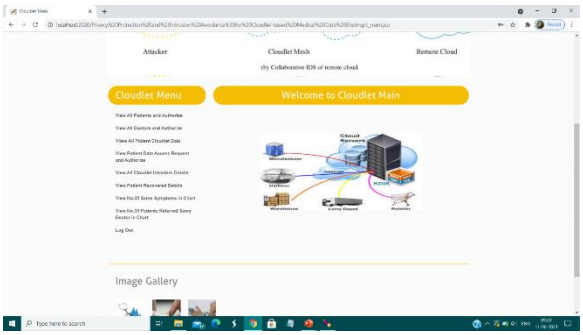
In this module, the patient Register and Login, View profile, Request Data Access permission from cloudlet and view Response, Access Your data and select doctor from combo box and send to corresponding doctor and View doctor response with medical prescription, verify your data and recover and view and delete your details.

Doctor

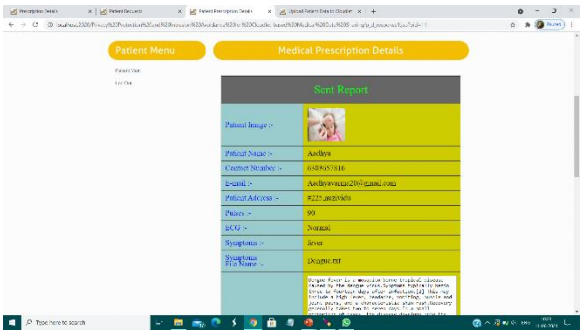
The doctor is the one who will perform the following operations such as Register and Login, View Profile, View patient details and give solution like Medicine details, medical prescription details View all patient medical prescription Details



RESULT AND DISCUSSION



In above Screen we got the Home page of the Project.



In above Screen it is sending the Data.

In above Screen shows the data is verified.

CONCLUSION

Firstly, we can utilize wearable devices to collect users' data, and in order to protect users' privacy, we use NTRU mechanism to make sure the transmission of users' data to cloudlet in security. Secondly, for the purpose of sharing data in the cloudlet, we use trust model to measure users' trust level to judge whether to share data or not. Thirdly, for privacy-preserving of remote cloud data, we partition the data stored in the remote cloud and encrypt the data in different ways, so as to not just ensure data protection but also accelerate the efficacy of transmission. Finally, we propose collaborative IDS based on cloudlet mesh to protect the whole system. The proposed schemes are validated with simulations and experiments.

REFERENCES

[1] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for telecom healthcare," in Engineering in Medicine and Biology Society, 2004. IEMBS'04.26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.

[2] M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," 2015.

[3] J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Koozie, A. Streit, and D. Georgakopoulos, "A security framework in g-Hadoop for big data computing across distributed cloud data centres," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.

[4] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (riot)–enabled framework for health monitoring," Computer Networks, vol. 101, pp. 192–202, 2016.

[5] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in Cloud Computing (CLOUD), 2010 IEEE 3rdInternational Conference on. IEEE, 2010, pp. 268–275.

[6] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "Dipos: DE duplicatable dynamic proof of storage for multi-user environments," 2016.

[7] L. Griffin and E. De Lea star, "Social networking healthcare," in Wearable Micro and Nano Technologies for Personalized Health (health), 2009 6th International Workshop on. IEEE, 2009, pp. 75–78.

[8] W. Xiang, G. Wang, M. Pickering, and Y. Zhang, "Big video data for light-field-based 3d telemedicine," IEEE Network, vol. 30, no. 3, pp. 30– 38, 2016.

[9] "https://www.patientslikeme.com/."

[10] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks: challenges and opportunities," Network, IEEE, vol. 24, no. 4, pp. 13–18, 2010.

[11] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014.

[12] K. T. Pickard and M. Swan, "Big desire to share big health data: A shift in consumer attitudes toward personal health information," in 2014 AAAI Spring Symposium Series, 2014.

[13] D. Bernstein and D. Vij, IEEE PROJECT 2302 – Standard for Intercloud Interoperability and Federation (SIIF), IEEE Standards Association Department Std., 2012. [Online]. Available: https://standards.ieee.org/develop/project/2302.html

[14] C. K. Law, W. Xie, Z. Xu, Y. Dou, C. T. Yu, H. C. B. Chan, and D.W. K. Kwong, "System and protocols for secure intercloud communications," in 11th International Conference for Internet Technology and Secured Transactions, ICITST 2016, Barcelona, Spain, December 5- 7, 2016, 2016, pp. 399–404.

[15] C. T. Yu, H. C. B. Chan, and D. W. K. Kwong, "Discovering resources in an intercloud environment," in 2017 IEEE Global Communications Conference, GLOBECOM 2017, Singapore, December 4-8, 2017, 2017, pp. 1–6.

[16] Y. H. Ho, P. M. F. Ho, and H. C. B. Chan, "Mobile inter cloud system and objects transfer mechanism," in 2017 IEEE Global Communications Conference, GLOBECOM 2017, Singapore, December 4-8, 2017, 2017, pp. 1–6.

[17] T. H. Noor, Q. Z. Sheng, S. Feudally, and J. Yu, "Trust management of services in cloud environments: Obstacles and solutions," ACM Compu. Surf., vol. 46, no. 1, pp. 12:1–12:30, Jul. 2013.

[18] T. H. Noor, Q. Z. Sheng, L. Yao, S. Dustan, and A. H. Ngu, "Cloud Armor: Supporting reputation-based trust management for cloud services," IEEE Trans. Parallel Disturb. Syst., vol. 27, no. 2, pp. 367–380, 2016.

[19] O. Hasan, L. Brunie, E. Bertino, and N. Shang, "A decentralized privacy preserving reputation protocol for the malicious adversarial model," IEEE Trans. Inf. Forensics Security, vol. 8, no. 6, pp. 949–962, 2013.

[20] S. tideless, "The economics of reputation and feedback systems in e-commerce marketplaces," IEEE Internet Computing, vol. 20, no. 1, pp. 12–19, 2016.

[21] O. Adedoyin, R. Araya, and J. Vassilevs, "Peer review in mentorship: Perception of the helpfulness of review and reciprocal ratings," in Intelligent Tutoring Systems - 13th International Conference, ITS 2016, Zagreb, Croatia, June 7-10, 2016. Proceedings, 2016, pp. 286–293.

[22] C. Castlecrag, A. C. Chan, E. Mykelti, and G. Tzadik, "Efficient and provably

secure aggregation of encrypted data in wireless

sensor networks," TOSN, vol. 5, no. 3, pp. 20:1–20:36, 2009.

[23] P. Parlier, "Public-key cryptosystems based on composite degree residuality classes," in Advances in Cryptology - EUROCRYPT '99, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding, 1999, pp. 223–238.

[24] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in 28th Annual Symposium on Foundations of Computer Science, Los Angeles, California, USA, 27-29 October 1987, 1987, pp. 427–437.

AUTHOR PROFILES:

Mrs. MOUNIKA.S completed her Bachelor of Technology in Computer Science and Engineering. She completed her Masters of Technology in Computer Science and Engineering from JNTU KAKINADA UNIVERSITY. Currently working as an Assistant Professor in the department of IT at DVR & DR HS MIC COLLEGE OF TECHNOLOGY(Autonomous), Kanchikacherla, NTR(Dist), AP. Her areas of interest are Data Mining, Cloud Computing and Machine Learning & Networks.

Mr.MURAHARI.P as MCA Student in the Department of DCA at DVR &DR.HS MIC COLLEGE OF TECHNOLOGY, Kanchikcherla, NTR(DT).He completed his BCA in K.B.N College. His areas of interests are C, Java, Python,Web development.