An Efficient And Secure Encrypted Emrs Deduplication Scheme For Cloud-Assisted Ehealth Systems

Shaik Karimulla, Sri.G.Ramesh Kumar, Sri.V.Bhaskara Murthy
MCA Student, Assistant Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

ABSTRACT: In this paper, we analyze the inherent characteristic of electronic medical records (EMRs) from actual electronic health (eHealth) systems, where we found that (1) multiple patients would generate large amounts of duplicate EMRs and (2) cross patient duplicate EMRs would be generated numerously only in the case that the patients consult doctors in the same department. We then propose the first efficient and secure encrypted EMRs deduplication scheme for cloud-assisted eHealth systems (HealthDep). With the integration of our analysis results, HealthDep allows the cloud server to efficiently perform the EMRs deduplication, and enables the cloud server to reduce storage costs by more than 65% while ensuring the confidentiality of EMRs. Security analysis shows that HealthDep is more secure than the Marforio et al.'s scheme (NDSS 2014) and Bellare et al.'s scheme (USENIX Security 2013). Algorithm implementation and performance analysis demonstrate the feasibility and high efficiency of HealthDep.

I. INTRODUCTION

Privacy preserving e-healthcare systems outsourced to cloud consists of medical data which is in image and text format. The data is collected frequently by sensor devices and it will processed by mobile devices. This data must be encrypted before it is outsourced to the cloud as cloud is honest but curious and can try to extract individual information. But as the mobile device is resource restricted, the encryption used should be lightweight and computational cost should be minimum. Secondly, cloud work as pay as you go model, so the content outsourced and the computation used should be minimum. Health provider will also use health cloud to deploy some of its health template. The comparison of personal health information to health template of physician‟s sample needs computation and this needs the cloud‟s virtual machine

Generally, the storage server needs to store the outsourced EMRs, such as prescriptions, for a prolonged period of time to satisfy several government regulations or hospital requirements on EMRs archiving. With the volume of EMRs generated from eHealth systems grows over

time, the costs of storing EMRs are persistently increase in practice. Actually, the storage costs can be reduced significantly after deduplication, where the storage server checks duplicate EMRs and deletes the redundant ones. For example, as shown in Fig. 1(a) and 1(b), both two patients (one is diagnosed with coronary heart disease and stable angina pectoris, and the other one is diagnosed with hypertension) need to use "Aspirin Entericciated Tablets", "Metoprolol Tartrate Tablets", and "Nifedipin

Sustained-release Tablets" with the same usage and dosage. Table I shows the savings of storage costs that performing deduplication on prescriptions from an actual eHealth system, these prescriptions are selected randomly from 10000 prescriptions generated by doctors from Department of Cardiology during 2013-2017. The results demonstrate that the storage costs can be reduced by more than 66% in the case of 500 prescriptions. However, from the perspective of data owners including both medical institutions and patients, the content of EMRs should not be leaked for security reasons. Therefore, privacy protection of the EMRs' content against anyone who does not own the EMRs should be guaranteed. This can be achieved by conventional encryption, but its randomness (i.e. for the same message, different users produce different ciphertexts) makes deduplication impossible.

The main problem of the e-healthcare of the system to aggregate data from multiple patients and keep them secure from cloud [2] provider itself. As the data is encrypted before outsourcing, the computation should also be performed on outsourced data. The solution to the above mentioned problem is the use of fully homomorphic algorithm. The homomorphic encryption is the technique where we can perform the operation on ciphertext and which can give result exactly like what the plain text can give. The partial homomorphic encryption gives capability to perform only specific operations. We have to apply the scheme where we can perform the addition and multiplication operation both. In this proposed SPHS solution a set of body sensors is deployed on, in or around the patient to gather the real-time personal health information in terms of both text and image (i.e. electrocardiogram (ECG), and endoscopy), which is further aggregated and transmitted to the healthcare provider for the authorized physicians to access and decide corresponding treatment. In smart e-healthcare systems, collected PHI is required to match kinds of medical templates from physicians‟ experience in the cloud based on specific similarity metrics, to judge the state of the patient suffering/recovering from certain diseases. Required properties are security and privacy are as follows.

1) Privacy of patient‟s i.e. original identity and medical data has to be kept secret against any unauthorized person while it stored in the cloud or computed by it

including malicious administrators in the cloud.

2) Medical data should be secret even for the data processing cloud

Secured e-Healthcare System is a secure and energy efficient privacy preserving dynamic medical text mining and image feature extraction scheme in e-healthcare system is based on new technique of fully homomorphic data aggregation which simultaneously supports addition and multiplication with unified mechanism from every individual data in encrypted domain, requiring any one-way trapdoor function computation only once. It significantly reduces computational and communication cost, which also supports privacy-preserving inner product in computing the similarity in the encrypted domain.

II. Proposed method

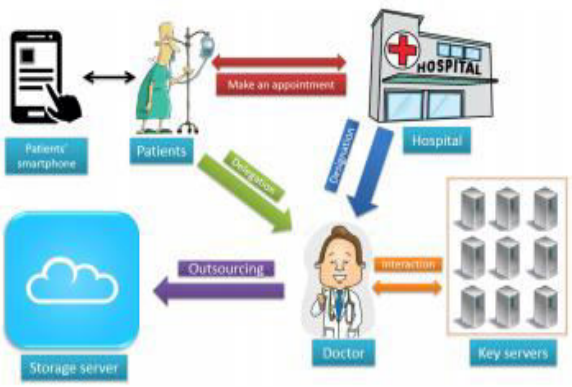
Since a patient always consults a doctor without heavy luggage, it is impractical to require patients to be well equipped in eHealth systems [24]. As most persons already are equipped with smartphones, deployment of the mobile device to make delegation and store MLE keys is practical. To ensure the security, the key technique used in HealthDep is system-wide TEEs [14], such as ARM TrustZone [15]. Prior to make an appointment with the hospital and see a doctor, we assume that each patient has already installed two applications provided by the hospital on his device: a companion application running in the normal world and a trusted application running in the secure world. We also assume that each patient has completed a registration such that the hospital has stored the device certificate of patient's smartphone. We make use of the IMEI of the patient's device as the identity, since it is written by the device manufacturer and stored in a read-only memory on the device. This binds the patient to his/her device TEE

Each patient first obtains a treatment key from the hospital, and seals the treatment key in the secure world of his/her smartphone TEE. All the subsequent interactive messages between the patient and the hospital are protected under the treatment key. The patient first makes an appointment with the hospital, and receives his/her diagnosing information. At the treatment time, the patient delegates to the doctor, and the doctor generates the EMRs. Next, the doctor divides the EMRs into two parts: the one involves the individual information, such as patient information and clinical diagnosis, which is the most sensitive data; the other one involves the medical records, such as medicines and their usage and dosage, which would be duplicate. Then the doctor encrypts the first part (e.g., the content contained within the yellow rectangle described in Fig. 1) by using conventional encryption (e.g AES), encrypts the later part (e.g., the content contained within the red rectangle shown in Fig. 1) by using the server-aided MLE, outsources the ciphertexts as well as

some auxiliary information corresponding himself/herself to the storage server, and sends the keys to the patient. The storage server first checks the validity of the patient's delegation to authenticate the doctor, if the checking passes, it accepts the outsourced ciphertexts.

In HealthDep, to thwart online brute-force attacks discussed in Section II-C, in which attackers (curious doctors) impersonate a valid doctor to request MLE keys and further violate the confidentiality of the EMRs, the number of MLE keys request for each doctor during a fixed time interval, called an epoch, should be limited. A bound ρ is pre-defined at the initialization phase; Each key server keeps track of the total number of the queries made by each doctor, and stops responding after ρ is reached.

III. SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

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.

V. CONCLUSION

In this paper, we have proposed the first secure and efficient encrypted EMRs deduplication scheme for cloud-assisted eHealth systems, namely HealthDep. HealthDep is able to resist brute-force attacks without suffering from the singlepoint-of-failure problem; the patients in HealthDep make use of their smartphones to secure delegation and MLE keys. We have analyzed EMRs in actual eHealth systems and pointed out that patients consulted the doctors with the same department would generate numerous duplicate EMRs, while patients consulted the doctors with the different departments would generate few duplicate EMRs, which is integrated into HealthDep to improve the performance that the storage server checks duplicate EMRs. We have provided implementation to demonstrate the feasibility of HealthDep, and conducted a comprehensive performance comparison between HealthDep and the existing schemes, which has shown that HealthDep provides a strong security guarantee with a high efficiency.

REFERENCES

[1] L. D. Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233– 2243, 2014.

[2] H. Ren, H. Li, Y. Dai, K. Yang, and X. Lin, "Querying in internet of things with privacy preserving: Challenges, solutions and opportunities," IEEE Network, 2018, to appear.

[3] G. Xu, H. Li, C. Tan, D. Liu, Y. Dai, and K. Yang, "Achieving efficient and privacy-preserving truth discovery in crowd sensing systems," Computers & Security, vol. 69, pp. 114–126, 2017.

[4] W. Quan, Y. Liu, H. Zhang, and S. Yu, "Enhancing crowd collaborations for software defined vehicular networks," IEEE Communications Magazine, vol. 55, no. 8, pp. 80–86, 2017.

[5] V. Casola, A. Castiglione, K. R. Choo, and C. Esposito, "Healthcarerelated data in the cloud: Challenges and opportunities," IEEE Cloud Computing, vol. 3, no. 6, pp. 10–14, 2016.

[6] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot) - enabled framework for health monitoring," Computer Networks, vol. 101, no. 4, pp. 192–202, 2016.

[7] Y. Zhang, C. Xu, X. Liang, H. Li, Y. Mu, and X. Zhang, "Efficient public verification of data integrity for cloud storage systems from indistinguishability obfuscation," IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, pp. 676–688, 2017.

[8] H. Li, Y. Yang, Y. Dai, J. Bai, S. Yu, and Y. Xiang, “Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data,” IEEE Transactions on Cloud Computing, 2017, to appear.

[9] M. Bellare, S. Keelveedhi, and T. Ristenpart, “Message-locked encryption and secure deduplication,” in Proceedings of EUROCRYPT. Springer, 2013, pp. 296–312.

[10] “List of antibiotics,” https://en.wikipedia.org/wiki/List of antibiotics.

[11] M. Bellare, S. Keelveedhi, and T. Ristenpart, “Dupless: Server-aided encryption for deduplicated storage,” in Proceedings of USENIX Security Symposium. USENIX, 2013, pp. 179–194. [12] Y. Duan, “Distributed key generation for encrypted deduplication achieving the strongest privacy,” in Proceedings of CCSW, 2014, pp. 57–68.

[13] Y. Zheng, X. Yuan, X. Wang, J. Jiang, C. Wang, and X. Gui, “Enabling encrypted cloud media center with secure deduplication,” in Proceedings of ASIACCS. ACM, 2015, pp. 63–72.

[14] J. Ekberg, K. Kostiainen, and N. Asokan, “Trusted execution environments on mobil devices,” in Proceedings of CCS. ACM, 2013, pp. 1497–1498.