ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Secured Cloud-Assisted e-Healthcare System

Pooja Kolte

M.E. Student, Dept. of Computer Science, RMD Sinhgad School of Engineering, Savitribai Phule University, Pune, India

ABSTRACT: E-healthcare systems provide patients health monitoring, disease modeling and evidence based solutions from recognized healthcare providers or physicians. For this dynamic health condition of patients is gathered on some small wearable devices like PDA with some sensors applied on or in patients body. This collected information is dynamic means there is always recovery or deteriorating conditions occur in patient's body having some disease. This collected data is too large to store on small devices or to compute on it. So need to outsource that data onto cloud which will help us to store and compute data easily. But problem is that cloud might be semi-honest or we can say honest but curious means it will help to store patient's private data like identity his diseases securely but it's also curious to know this private data. So based on my survey we need some application which will help us to provide services securely and privately also. So this is what we are going to propose this privacy preserving protocol for such dynamic text mining and image feature extraction from cloud in e-healthcare systems (SPHS).

KEYWORDS: privacy preservation, security, e-healthcare systems, data mining, image feature extraction.

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.

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

computational and communication cost, which also supports privacy-preserving inner product in computing the similarity in the encrypted domain.

II. RELATED WORK

In this section we briefly review the existing systems for this problem. Recently in [3] Jung et. al. proposed a privacy preserving data aggregation which supports multivariate polynomial evaluation technique without secure communication channel, respectively in one aggregator model and participants only model. When it is implemented to outsourced medical text mining, it only suggests static statistics computation, without including the patient's dynamic health condition monitoring which can more precisely reflect his suffering status untouched. Moreover, the summation and multiplication aggregation are acquired in independent systems that leads an additional burden on power-restricted users. Then also author hsu et al.[4] proposed an image feature extraction with privacy-preserving scale-invariant feature transform (SIFT), by explaining paillier's cryptosystem. But, it's unable to apply in outsourced medical image feature extraction. Because paillier's cryptosystem supports only addition homomorphism. Additionally, the feature descriptor matching in the encrypted domain does not support privacy-preserving inner product, which would result in the template medical image privacy exposure.

Many more existing systems are tried to solve this problems with some anonymous identity, generating dynamic keys, different energy efficient algorithms are developed for security but to maintain privacy SPHS is proposed [5,6,7,8,9].

Therefore here we are proposing a secure and efficient privacy-preserving dynamic medical text mining and image feature extraction scheme in e-healthcare system which is based on our newly-devised technique of fully homomorphic data aggregation.

It simultaneously also supports addition and multiplication aggregation with a unified mechanism from *n* individual data in the encrypted domain, requiring to perform one-way trapdoor function computation once. Compared to recently proposed system by hsu et al.[4], the SPHS which achieves privacy-preserving medical image feature extraction and that is with a higher CCA2 security in the semi-honest model and significantly decreases computational and communication cost, that also supports privacy-preserving inner product in computing the similarity in the encrypted domain.

III. PROPOSED WORK

This Proposed SPHS network model is consists of efficient and very secure privacy preserving data outsourcing for medical text mining and image feature extraction. This model mainly has three components as shown in fig. 1: the patient, the physicians, and the cloud. Patients are bounded by some sensors deployed on, or in his body which provides dynamic health condition information to the handheld devices. These devices are not able to store much data and to compute it.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Fig. 1 Network Model of SPHS

So we need to outsource that data onto the cloud. As we know cloud is the best platform to store and calculate the big amount of data in a very efficient manner. Cloud storage means the storage of data online in the cloud wherein a organization's data is stored and accessible from multiple distributed and connected resources that comprise a cloud.

Cloud storage can provide the benefits of greater accessibility and reliability; rapid deployment; strong protection for data backup, archival and disaster recovery purposes; and lower overall storage costs as a result of not having to purchase, manage and maintain expensive hardware. However, cloud storage does have the potential for security and compliance concerns. Cloud computing practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer. Physicians are unable to tolerate these energy consuming and costly task of storing all information on personal computer. So medical cloud provides "pay-per-use" service for patients and physicians. So it helps to minimize the computation and communication cost. This medical data is stored in encrypted form so that our semi-honest that is curious cloud should not try to find out the original details of any patients or physicians. Medical text mining is our one module and another is the image feature extraction. In medical text the patient's information regarding his identity and diseases, dynamic health conditions is stored. And in image feature extraction the patients ECG, endoscopy like reports are scanned and stored in image format. So these to modules are implemented in our proposed work with security and maintaining privacy of original data and patients also. By executing proposed scheme, the cloud server performs privacy-preserving function correlation matching for medical text mining and SIFT for image feature extraction in the encrypted domain. This text and image information is known as PHI that is personal health information of patients.

The proposed system is composed of four algorithms, namely AGG.KGen, AGG.Enc, AGG.Eval and AGG.Dec, which can be defined as follows.

AGG.KGen- Generates one-way trapdoor function.

AGG.Enc- Polynomial-time encryption algorithm runs by the patient.

AGG.Eval- Evaluation algorithm runs by cloud.

AGG.Dec- Polynomial-time decryption algorithm runs by the physician.

With these four aggregation algorithms our proposed work will minimizes cost and maintains privacy and security of patients and physicians also. This proposed algorithm SPHS serves these four fully homomorphic algorithms and provide security for cloud users. First AGG.KGen is run by system which is generator of any one-way trapdoor function. Using that function patients encrypts his private medical data with the help of AGG.Enc algorithm. Then evaluation of that encrypted data is done by cloud in AGG.Eval algorithm. As its encrypted cloud will not get any private data of patients and store and compute that data securely. Then with the help of AGG.Dec algorithm physicians decrypt that data and check patients details, his reports and prescribes him further procedural treatment. In such a way our SPHS algorithm works and so our e-healthcare system is secure and privacy preserving also.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

IV. SIMULATION RESULTS

To better understand system proposed here we need some proof and that's why some experiments are taken into account to differentiate our system from existing one. So in this section, some evaluations are performed for our proposed system like the computational and communication cost comparison between our proposed efficient privacy-preserving fully homomorphic data aggregation scheme, privacy-preserving dynamic medical text mining and privacy-preserving medical image feature extraction and the existing work fully homomorphic encryption (FHE)[3] and Paillier's cryptosystem then, also evaluate both the dynamic medical text and image feature matching probability at each stage of disease suffering.

Now we will see some results performed over data with both algorithms FHE and SPHS and then we will easily understand how effectively our algorithm works .Fig. 2 shows the computation cost required for existing FHE algorithm [3] and proposed SPHS system. We can see that as the number of aggregated data increases the cost required for FHE algorithm is also increases significantly and cost for SPHS is so negligibly increases with data increase. It is obviously observed that as the number of aggregated data increases, the computational cost and communication cost of SPHS negligibly increases which mainly focused on the most costly one-way trapdoor function, which contains a number of most energy consuming modular exponentiation operations and has the most ciphertext expansion. These two elements significantly contribute to both the computational and communication cost.

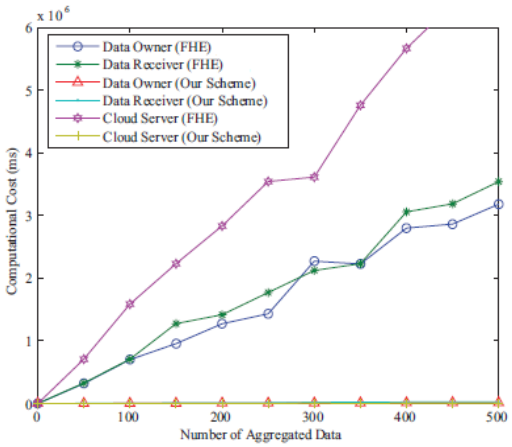

Fig. 2: Computational Cost Comparison of Privacy-preserving Data Aggregation

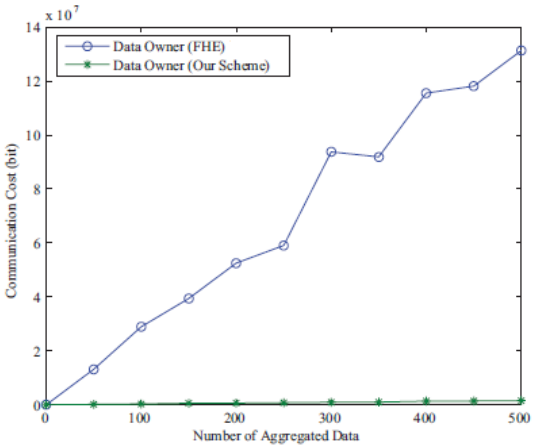

Fig. 3: Communication Cost Comparison of Privacy-preserving Data Aggregation

Fig. 3 shows comparison between communication cost required for FHE and SPHS. In figure we can see cost of FHE highly increases with number of aggregated data and very opposite situation in SPHS cost increases in a very small amount.

V. CONCLUSION

The simulation results showed that the proposed algorithm SPHS performs better than existing FHE system. Also the communication and computation cost of proposed system is lower than existing system. The proposed algorithm provides energy efficient service and maximizes the lifetime of entire data. The most important secure and privacy preserving dynamic medical text mining and the image feature extraction with one-way trapdoor by using fully homomorphic aggregation. As the performance of the proposed algorithm is analyzed between two metrics security and privacy, in future with some modifications in design considerations the performance of the proposed algorithm can be compared with other energy efficient algorithm.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

REFERENCES

[1] Jun Zhou, Zhenfu Cao, Xiaolei Dong, Xiaodong Lin, ''PPDM: Privacy-Preserving Protocol For Dynamic Medical Text Mining And Image Feature Extraction From Secure Data Aggregation In Cloud-Assisted E-Healthcare Systems', IEEE Journal of Selected Topics In Signal Processing, Volume:9, Issue No: 7, pp.1332 – 1344, September 2015.
[2] Xiaokui Shu, Danfeng Yao, ''Privacy Preserving Detection Of Sensitive Data Exposure '', IEEE Transactions On Information Forensics And Security, Vol. 10, Issue-4, pp. 5, May 2015.
[3] K. Lauter, M. Naehrig and V. Vaikuntanathan, ''Can Homomorphic Encryption Be Practical?'', In ACM Conference, vol. 1, no. 4, pp. 485–509, 2011.
[4] P. Paillier, ''Public Key Cryptosystems Based On Composite Degree Residuosity Classes'', In Eurocrypt 1999, vol. 20, o. 5, pp. 725–739,May 2009.
[5] Larry A. Dunning And Ray Kresman, ''Privacy Preserving Data Sharing With Anonymous Id Assignment', IEEE Transactions On Information Forensics And Security, Vol. 8, No. 2, pp. 249–257., February 2013.
[6] Jian Liu, Kun Huang, Hong Rong, Huimei Wang And Ming Xian, ''Privacy-Preserving Public Auditing For Regenerating-Code-Based Cloud Storage', IEEE Transactions On Information And Security, vol. 57, no. 18,pp. 4047–4064, Dec. 2013.
[7] Kaitai Liang, Willy Susilo, Senior Member, IEEE And Joseph K. Liu, ''Privacy-Preserving Ciphertext Multi-Sharing Control For Big Data Storage'', IEEE Transactions On Information Forensics And Security, vol. 18, no. 6, pp. 333–340, 2015.
[8] Jason Croft, Matthew Caesar, ''Towards Practical Avoidance Of Information Leakage In Enterprise Networks'', in NSDI journal on research and science, ol. 41, no. 4, pp. 23–28, Apr. 2012.
[9] Xiaokui Shu and Danfeng (Daphne) Yao, ''Data Leak Detection As A Service'', in Securecomm Conference, vol. 31, Issue no 11, Pp. 222–240, 2013.

BIOGRAPHY

Pooja Gokul Kolte is pursuing her Masters of Engineering in the Computer Science Department, Sinhgad School of Engineering, Savitribai Phule University. She received Bachelor of Engineering degree in Information Technology from University Of Pune, Pune, India.