International Journal of Recent Trends in Engineering & Research
ISSN(ONLINE) : 2455-1457
IMPACT FACTOR : 3.344

MEDICAL REMAINDER AND PREDICATOR APP

Menaka.T[1], Gomathi.N[2],Venkatesan.S[3]
[1,2] Department of Information Technology, SKP Engineering College
[3]Assistant Professor,Informaion Technology ,SKP engineering college

Absract: Cloud-assisted mobile health (health) monitoring, which applies the widespread mobile communications and cloud computing technologies to provide feedback decision support, has been considered as a activist approach to improving the quality of healthcare service while lowering the healthcare cost. Unfortunately, it also poses a serious risk on both clients' privacy and intellectual property of monitoring service providers, which could discourage the wide adoption of Health technology. This project is to address this important problem and design a cloud-assisted privacy preserving mobile health monitoring system to protect the privacy of the involved parties and their data. Moreover, the outsourcing decryption technique and a newly proposed key private proxy re encryption are adapted to shift the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' intellectual property. Finally, our security and performance analysis demonstrates the effectiveness of our proposed design. Proving secure and performance analysis demonstrates the effectiveness in Cloud Computing environment.

I. INTRODUCTION

Providing secure and performance analysis demonstration the effective in medical data retrieving process in web service the problems to be recover in this project health record is crucial information ,because network hackers may be harmful for our record in between client to server data transaction process.

II. PROPOSED SYSTEM

It preserving to protect the privacy of the involved parties and their data.Our proposed system we also includes automatic health record generator. System will frequently ask questions relevant to the patients' health issue. Previously we need to complete all the possibilities of relevant issue Naive byes is the classification algorithm will improve this session effectively important for generating the records in accurate and gentle manner. Data will be forward with secure whenever user accessing the server unit. Also we can include small remainders for continuing medical assistants. We are going to show the solution for heart related health issues.

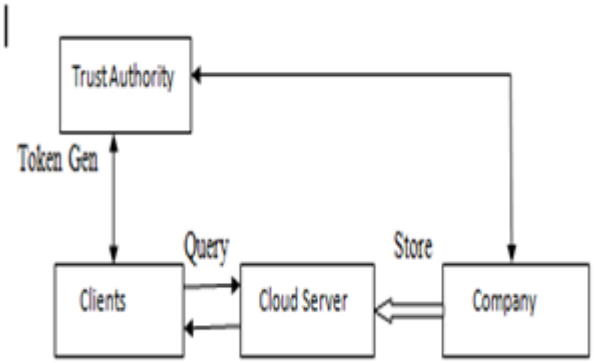

Fig: Architecture Diagram

III. MODULES

RAW DATA COLLECTION

The company stores its encrypted monitoring data or program in the Web. Individual clients collect their medical data and store them in their data base , which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the Web through a patient. TA is responsible for distributing private keys to clients and collecting service fees from clients according to a certain business model such as "pay-peruse" model.

CONEXT ANALYSIS

The context analysis layer takes the processed raw data collected in the lower layer as input, so that it may extract multiple types of events from the users' life. Each event is produced by a mining component, and we develop multiple types of mining components in the system. To better manage the reuse of resources, we propose a novel sustainable mining model, which decomposes a mining component's algorithm procedure into separate processing units. These units will continuously shuffle raw data, and provide the relevant ones to all the mining components where events are assembled. From those raw data, users can easily access the raw data collection with the help of Naïve Bayes classification algorithm. It will mine and navigate all the relevant data from that dataset and generates health record effectively.

EVENT PERSONALIZATION&RETREIVAL

After generating the health record, system will send the health record as cipher form. If a authenticated user he/she knows the respective key for decrypting the data. So data should be secure in processing time. Event personalization is the scheme for keeping personalized information in web with security. Users will collect their health information according to the personalized information those stored in a database.

DAIRY GENERATION

Finally user can access everything by their smart web search . It can be extend to store medical remainder, BMI (body mass index) generator etc. This services will handle everything; web server is the major controller to generate secure health record system.

IV. NETWORK ARCHITECURE AND SECURITY

A. Network Architecture:

privacy-preserving out sourced dynamic medical text mining and image feature extraction, mainly comprises three entities: the patient ,the healthcare provider (physicians), and the cloud. Fig. 1 illustrates the network architecture. A set of body sensors is deployed on, in or around the patient to monitor the real time PHI in terms of medical texts and images, which are frequently aggregated in the patient's hand-held devices such as PDA and outsourced to the cloud in the encrypted form. Both body sensors and hand-held devices are generally assumed to be resource-constrained for both computation and communication.

Therefore, it is required to devise a lightweight encryption or blinding algorithm to locally encode the PHIs from the programmed circuits embedded in the patient's hand-held device before they are transmitted to the cloud. On the other hand, the resource-constrained body sensors and hand-held devices cannot afford locally storing a large number of frequently monitored PHI text and even medical images, or are also intolerable of energy-consuming task of medical image feature extraction and matching. Medical cloud provides a convincing solution for the patients to outsource both their storage

and computation in a "pay-per-use" manner in such a resource asymmetrically-allocated environment. The physicians in the healthcare provider also delegate their medical template from their experience encrypted by their local programmed circuits to the medical cloud. By executing our proposed scheme PPDM, the cloud server performs privacy-preserving function correlation matching for medical text mining and SIFT for image feature extraction in the encrypted domain. The cloud server is assumed to work under a honest-but-curious model where it perfectly executes the protocol specification, but intends to extract the patient's secret PHI from the interactions with both the patient and the physician. It is noted that in the proposed network architecture, the entities providing PHI text/images and medical templates are distinct. Our proposed PPDM can be also applied to a special case where PHI text/image and medical template providers are the same entity (i.e., the healthcare provider), under the assumption that the physicians have outsourced a series of encrypted medical templates into the cloud, and will delegate the privacy preserving medical text.

B. Security Model:

The proposed PPDM is constructed on the basis of our newly-devised efficient privacy-preserving fully homomorphism data aggregation, since it simultaneously supports addition and multiplication operations in a unified way and serves as the core of the function correlation matching and SIFT in the encrypted domain. Therefore, we mainly focus on the formal security model of the privacy-preserving fully homorphism data aggregation.

The proposed scheme is composed of the following four algorithms, namely AGG .K Gen, AGG .Enc, AGG . E val and AGG.

Dec, which can be defined as follows.

AGG. K Gen: On input where is the security parameter, the system runs a trapdoor function generator denoted as a probabilistically polynomial time (PPT) algorithm and outputs the public parameters , and a pair of public key and secret key .

AGG. Enc: This is the probabilistically polynomial-time encryption algorithm run by the patient. Takes as input a message, the public key and the public parameter , outputs a cipher text .

AGG. Eval: This is the evaluation algorithm run by the cloud that takes as input , a function and the public parameter , outputs the cipher text .

AGG. Dec: This is a deterministic and polynomial-time decryption algorithm run by the physician. Takes as input the cipher text and the secret key (trapdoor) , outputs either the function value or the special symbol . It is noted that the function in the privacy-preserving data aggregation simply refers to addition and multiplication operations. Then, using a standardized overall approach to privacy-preserving data mining (PPDM) algorithm evaluation, namely the survey of quantification of PPDM algorithms [46] proposed by Bertino et al., we formally define the data privacy and result privacy in the security model of our newly-devised privacy-preserving fully homomorphism data aggregation which serves as a steppingstone for the proposed system.

V. CONCLUTION

In this paper, a secure and efficient privacy-preserving dynamic medical text mining and image feature extraction scheme PPDM in cloud-assisted e-healthcare systems is proposed. Firstly, an efficient privacy-preserving fully homomorphism data aggregation from any one-way trapdoor function is proposed, which serves the basis for our proposed PPDM. Then, an outsourced disease modeling and early intervention is achieved, respectively by devising an efficient privacy-preserving function correlation matching PPDM1 from dynamic medical text mining and designing a privacy-preserving medical image feature extraction PPDM2. Finally, the formal security proof and extensive performance evaluation demonstrate our proposed PPDM achieves a higher security level (i.e., information-theoretic

security for input privacy and CCA2 security for output privacy) in the honest but curious model with optimized efficiency advantage over the state-of-the-art in terms of both computational and communication overhead.

1. REFERENCES

1. L.Gatzoulis and I.Iakovidis, "Wearable and portable e-health systems," IEEE Eng. Med. Biol. Mag., vol. 26, no. 5, pp. 51–56, 2007.
2. I. Iakovidis, "Towards personal health record: Current situation, obstacles and trends in inplementation of electronic healthcare records in Europe," Int. J. Med. Inf. , vol. 52, no. 1, pp. 105–115, 1998.
3. E. Villalba, M. T. Arredondo, S. Guillen, and E. Hoyo-Barbolla, "A new solution for a heart failure monitoring system based on wearable and information technologies," in Proc. Int. Workshop Wearable and Implantable Body Sens. Netw. 2006-BSN 2006, Apr. 2006.
4. R. Sandhu and P. Samarati, "Access Control: Principles and Practice," in Proc. IEEE Commun., vol. 32, no. 9, pp. 40–48.
5. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A Berkeley view of cloud computing," Univ. of California, Berkerley,
6. J. Taeho, X. Mao, and X. Li, "Privacy-preserving data aggregation without secure channel: Multivariate polynomial evaluation," in Proc.IEEE INFOCOM, 2013, pp. 2634–2642.
7. C. Y. Hsu, C. S. Lu, and S. C. Pei, "Image feature extraction in encrypted domain with privacy-preserving SIFT," IEEE Trans. Image Process., vol. 21, no. 11, pp. 4593–4607, Nov. 2012.
8. J. Zhou, Z. Cao, X. Dong, X. Lin, and A. V. Vasilakos, "Securing m-healthcare social networks: Challenges, countermeasures and future directions," IEEE Wireless Commun., vol. 10, no. 4, pp. 12–21, 2013.
9. M. Bellare aand P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in Proc. ACM CCS, 1993.
10. T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.
11. C. Castelluccia, A. C.-F. Chan, E. Mykletun, and G. Tsudik, "Efficient and provably secure aggregatioin of encrypted data in wireless sensor networks," ACMTrans. Sen. Netw., vol. 5, no. 20, pp. 1–36, 2009.
12. I. Damgard, M. Geisler, and M. Kroigard, "Homomorphic encryption and secure comparison," Int. J. Appl. Cryptography, vol. 1, no. 1, pp. 22–31, 2008.
13. M. V. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in Proc. EUROCRYPT '10, LNCS 6110, 2010, pp. 24–43, Springer.
14. J. Domingo-Ferrer, "A provably secure additive and multiplicative privacy homomorphism," in Proc. ISC'02. LNCS, Heidelberg, Germany, 2002, vol. 2433, pp. 471–483, Springer.
15. J. Zhou, X. Lin, X. Dong, and Z. Cao, "PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributed m-healthcare cloud computing system," IEEE Trans. Parallel Distrib. Syst., to be published.
16. Z. Erkin, A. Piva, S. Katzenbeisser, R. L. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," EURASIP J. Inf. Security, vol. 7, no. 2, pp. 1–20, 2007.
17. Z. Erkin and G. Tsudik, "Private computation of spatial and temporal power consumption with smart meters," in Proc. ACNS'12, LNCS 7341, 2012, pp. 561–577.
18. "Free medical image databases," [Online]. Available: http://www.bestmedicallinks.com/free-medical-images-databases
19. F. D. Garcia and B. Jacobs, "Privacy-friendly energy-metering via homomorphic encryption," in Proc. STM'10. LNCS, Heidelberg, Germany, 2010, vol. 6710, pp. 226–238, Springer.
20. R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in Proc. CRYPTO, 2010.

