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

CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring

Bharathi.S[1] ,Christina jenifer.S[2] ,Venkatesan.S[3]
[1,2] *Department of Information Technology, SKP Engineering College*
[3] *Assistant professor, SKP Engineering College*

Abstract*:* E-healthcare system have been increasingly facilitating health condition monitoring, disease modeling and early intervention, and evidence-based medical treatment by medical text mining and image feature extraction. Owing to the resource constraint of wearable mobile devices, it is required to outsource the frequently collected personal health information (PHI) into the cloud. Unfortunately, delegating both storage and computation to the un trusted entity would bring a series of security and privacy issues. The existing work mainly focused on fine-grained a privacy-preserving static medical text access and analysis, which can hardly afford the dynamic health condition fluctuation and medical image analysis. In this paper, a secure and efficient privacy-preserving dynamic medical text mining and image feature e extraction scheme PPDM in cloud-assisted e-healthcare system sis proposed. Firstly, an efficient privacy-preserving fully data aggregation 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 adaptive chosen cipher text attack (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.

Index Terms—E-healthcare system, data mining, image feature extraction, security, privacy preservation.

I. INTRODUCTION

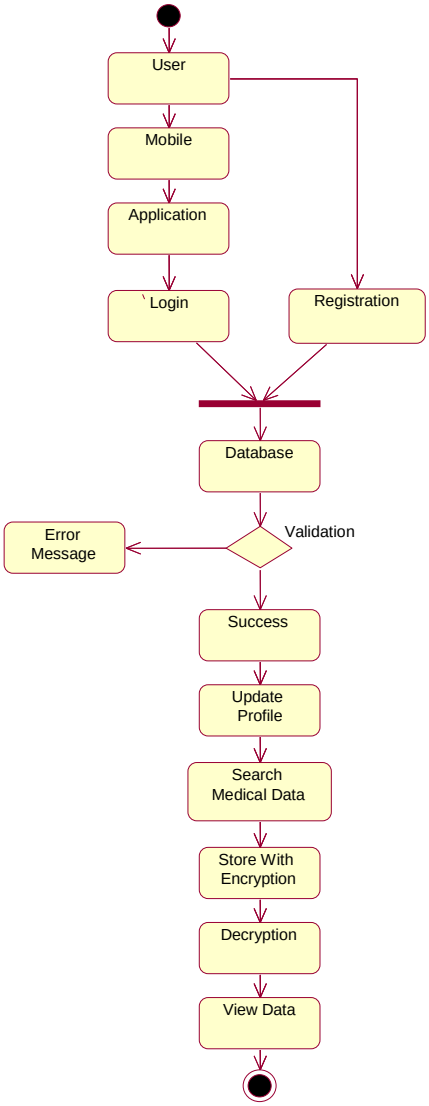
Proving secure and performance analysis demonstrates the effectiveness in Cloud Computing en E-HEALTHCARE systems significantly facilitate the health condition monitoring, disease modeling and early intervention, and evidence-based medical treatment [1], [2].A set of body sensors is deployed on, in or around the patientCloud-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 m 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.

II. PROPOSED SYSTEM

This paper is to address this important problem and design a cloud-assisted privacy.
It preserving mobile health monitoring system to protect the privacy of the involved parties and their data.
The outsourcing decryption technique and a newly proposed key private proxy re encryption are adapted.
It uses to shift the computational complexity of the involved parties to the cloud without compromising clients' privacy and service providers' intellectual property.



III. DATA FILOWDIAGRAM

STEP1:User enter the user name and password into the mobile . If the user already registered means directly access the application but not registered means first complete the registration process **.**

STEP2:The user will access the application by using internet connection. The user given the username and password into the mobile
STEP3: Check whether the username and password are valid or not in database .
STEP4:the username and password are valid means system passed the message success .But not valid means system passed the error message to the user.
STEP5:The fifth step is profile update. The user select discuss and given the input to system
STEP6:The system search the medical data in database and generate the report .The system generate the report by using Naïve Bayes algorithm
STEP7:The report should be store encryption format in database
STEP8:The system to provide user ID to user The user ID should very important to retrieve the report
STEP9:The user enter the user ID in the system then get report
STEP10:After the completion of the decryption process report should be view

IV. MODULES

- Health data collection
- AES implementation
- Token generation
- Cipher text retrieval

HEALTH DATA COLLECTION

The company stores its encrypted monitoring data or program in the cloud. Individual clients collect their medical data and store them in their mobile devices, which then transform the data into attribute vectors. The attribute vectors are delivered as inputs to the monitoring program in the cloud through a mobile (or smart) phone. TA is responsible for distributing private keys to clients and collecting service fees from clients according to a certain business model such as “pay-per-use” model.

AES IMPLEMENTATION

To protect the client’s privacy, we apply the anonymous AES in medical diagnostic branching programs. To reduce the decryption complexity due to the use of AES, we apply recently proposed decryption outsourcing with privacy protection to shift client’s pairing computation to the cloud server

TOKEN GENERATION

To generate the private key for the attribute vector, a client first computes the identity representation set of each element in and delivers all the identity representation sets to TA. Then TA runs the on each identity in the identity set and delivers all the respective private keys to the client.

CHIPHER TEXT RETRAIVAL

The cloud is required to generate the cipher texts for clients by running the Re Encryption algorithm. Each run of Re Encryption algorithm costs the cloud exactly two pairing computations. For each client, the cloud needs to perform those Computations. The resulting public key cipher texts along with the original symmetric key cipher texts constitute the Cipher text sets for the client

V. CONCLUSION

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 out sourced 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.

REFERENCES:

1. L. Gatzoulis and I. Iakovidis, "Wearable and portable e-health. L. Gatzoulis and I. Iakovidis, "Wearable and portable e-health systems,"IEE[E 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, CA, USA, Tech. Rep. USB-EECS-2009-28, 2009.
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 and 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.

