ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Privacy Preserving for Cloud Assisted Data with Correlation Matching Technique Using Information Theoretic Security

S.Amutha[#1], A.Dharshana[#1], K.Prithika[#1], M.Priya[#1], B.Sasikala[#2]
#1 Bachelor of Computer Science and Engineering
#2 Assistant Prof.Department of Computer Science and Engineering
Bharathiyar Institute of Engineering for Women

ABSTRACT

E-healthcare systems have providing several facilities for monitoring health conditions, disease identification and early finding of any interception in database. It is report-based treatments through text mining and image feature extraction. The resource conditions of storage devices are required to frequently collect personal healthcare information into the cloud database. Unfortunately, both storage and computation to the untrusted parties would bring a series of security and privacy problems. The existing system mainly focused on homomorphic data aggregation in privacy-preserving text access and image extraction, which will allow the dynamic health condition problems and medical image analysis (eg.scan reports).Here, we provide a secure and more efficient privacy-preserving for cloud-assisted data in e-healthcare systems. Firstly, an efficient privacy-preserving fully heteromorphic data aggregation is proposed, which act as the basis for our proposed system. Then, disease identification and early finding of any interception is achieved by an efficient privacy-preserving function interrelationship matching from dynamic medical text mining and design privacy-preserving extraction of medical image feature. Finally, the security proof by inter relationship matching and extended performance will provide higher security level.

I. INTRODUCTION

E-Health care systems significantly facilitate the health condition monitoring, disease modeling and early interruption, and evidence-based medical treatment set of body sensors is extend, in or around the patient to collect the individual health information of text (i.e. body temperature and blood pressure) and image(i.e.electrocardiogram,electroencephalogr amand and endoscopy which is further aggregated and transmitted to the server for the authorized practitioner to access and decide appropriate treatment. In smart e-healthcare systems, collected PHI is required to match kinds of medical results from physicians' experience in the cloud based on specific similarity metrics, to judge the state of the patient suffering or recovering from certain diseases.

However, when it is applied to deploy medical text mining, it only suggests static computation (i.e. the mean and the sum), leaving the patient dynamic health condition monitoring that can more squarely reflect her/his suffering status unharmed. Moreover, the addition aggregation and multiple gathering are achieved in independent mechanisms, which lead an additional burden on power-barred users. An image extraction in encrypted privacy-preserving scale-unvaried feature transform by manuever cryptosystem. However, it cannot be applied in outsourced medical image feature extraction for the following reasons: Firstly, directly executing Paillier's cryptosystem on image signal processing deviates from the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
ernational Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
l. 3, Special Issue 2, March 2016

principle that it is generally required to use public key encryption to encode the relatively short session key, which is further exploited to encode the underlying data (image signals) of a longer size. Therefore, its inefficiency cannot well adapt to the resource-constrained wearable devices of both patients and physicians. First, efficient privacy-preserving homomorphic data aggregation, support both addition and multiplication operations, from any one-way wormhole function is proposed, which serves the basis of our privacy preserving text mining. Based on the observation that the aggressive medical text mining and image aspect extraction only requires the privacy-preserving data gathered result, not requiring to expound each individual data afterwards, our newly-congitate data aggregation achieves this goal with a accord between the functionality and the optimized competent, compared to the existing homomorphic encryption. Second approach based on our technique of efficient privacy-preserving homomorphic data aggregation, a secure and competent privacy-preserving aggressive medical text mining scheme1 and image feature extraction scheme2 are respectively proposed, by designing privacy preserving function pendant matching and a privacy preserving SIFT.

II. LITERATURE SURVEY

2.1 SINGLE AGGREGATOR MODEL:

In the first model, we have one aggregator who wants to compute the function f(x). We assume the aggregators are untrustful and inquisitive.That is healways eavesdrops the communication between participants and tries to harvest their input data. We also assume participants do not trust each other and that they are curious as well. We should have multiple aggregators, but this is a simple extension which can be superficially achieved from our first model. We call this model the Single Aggregator Model. Note that in this model, any single contributor is not allowed to compute the final result.

CONTRIBUTORS ONLY MODEL: The second one is similar to the first except that there are n cotributor only and there is no aggregator. In this model, all the contributors are equal and they all need to calculate the final aggregation result.We call this model the Participants Only Model. In these two models, participants are assumed not to connive with each other. Relaxing this assumption is one of our future works.

2.2 PRIVACY-PRESERVING HEALTH DATAAGGREGATION:

In MHNs, the data transmission (or forwarding) overheads are exponentially increased due to the large number of health sensing data from wearable devices. Particularly, in a D2D-based smart community as shown in Fig. 4, users continuously upload their physiology parameter records to a health data centre via social spots deployed in the community by using short-range communication techniques. Furthermore, the multihop relay is adopted to aggregate the data with a tolerable delay. However, in accordance with different types of health data, the transmission delay may be significantly different. Meanwhile, privacy protection during data transmission is also necessary for MHNs. In [11], a priority-based privacy-preserving data aggregation scheme is proposed for MHNs, which not only aggregates different types of health data within tunable delay requirements but also protects the data and identity privacy during transmission. According to various types of health data, users select different forwarding strategies, which not only forward data within the given delay but also consume reasonable network resources. Having the health data priority shown in Fig. 4b, users with P1 data can greedily forward their data and make use of the network resources to minimize the delay. Furthermore, doctors may request vital health data from patients in emergencies for continuous monitoring. In addition, the regular health data are not for emergency use, so the delay

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
ernational Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
l. 3, Special Issue 2, March 2016

requirement may be tolerant. Both vital and regular data are labeled as small data (i.e., physiology parameters with small data size) and big data (i.e., ECG or images with large size) [11]. Given the relay selection strategy, the sender selects the optimal relay for different data priorities (or different forwarding schemes). Then the relays store carry-and-forward the data to social spots connected to cloud servers so that the data can finally be forwarded to the cloud servers. The security and privacy issues cannot be negligible as the cloud servers are not fully trusted and may maliciously delete or modify the stored data. Moreover, the data owner cannot trust the relays who are anonymous and even strangers. Since the health data are separated into different categories, the security protection levels should also be adjusted. Therefore, to enhance the health data aggregation from the QoP perspective, privacy preserving aggregation is desirable.

2.3 A FULLY HOMOMORPHIC SCHEME

We now proceed to turning the somewhat homomorphic scheme into a fully homomorphic scheme. Since we have shown that our scheme is a specialisation of Gentry's scheme, we only need to recast Gentry's method
for our parameters. At certain we can simplify the method somewhat, since our ciphertext is an integer rather than a vector. We assume that our scheme is secure under key dependent encryptions, purely to keep the notation simpler; to deal with the more common case is immediate from our discussion. At a high level we need to define a new algorithm called Recrypt, which takes a ciphertext c and rencrypts it to cnew, whilst at the same time removing some of the errors in c. Ostensively this takes a "dirty ciphertext" c and "cleans it" to obtain the ciphertext cnew. To do this we augment the encryption key with some additional information, by extending the algorithm KeyGen with the following additional operations, based on two integer parameters s1 and s2. We make use of the fact that we are only interested in the coefficients of Z(x) modulo 2p.

2.4 NON-INTERACTIVE COMPARISON USING SOMEWHAT OR FULLY HOMOMORPHIC ENCRYPTION

For a non-interactive solution, fully-homomorphic encryption schemes could be used as described in §1. Boolean circuits for secure comparison can be built with logarithmic multiplicativedepth2, has multiplicative depth dlog2 `e for comparing `-bit values. Hence, it is also possible to use somewhat homomorphic encryption schemes that allow a fixed number of multiplications of ciphertext. In contrast to fully-homomorphic encryption schemes, these schemes do not require an expensive bootstrapping step and hence can be implemented more efficiently, cf. [LNV11].The authors of [LNV11] report on practical implementation results for the somewhat homomorphic encryption scheme of BV11b where parameters are chosen to allow up to 15 multiplications, i.e.,it can be used to non-interactively compare numbers of up to 215 = 32 768 bits which is sufficient for the privacy-preserving SIFT application of hlp12 where numbers fit into the plaintext space with jNj bits.

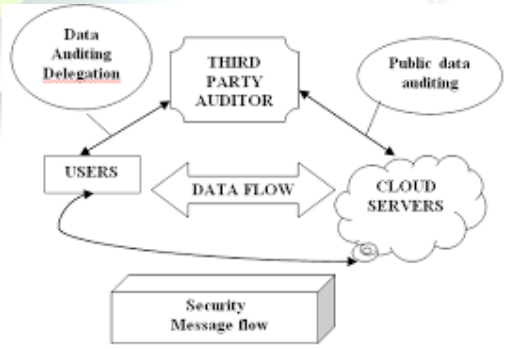

Fig 2.4.1 Network Architecture of Cloud-assisted E-Healthcare Systems

2.5 ACHIEVING AGGREGATOR AMNESIC SECURITY

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
ernational Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
l. 3, Special Issue 2, March 2016

In this section, we describe a cryptographic construction that allows us to achieve aggregator amnesic security. For simplicity, in this section, we assume that each participant includes preservative noise r to her data x before encrypting it. To avoid writing the plaintext and noise terms separately, we use the notation bxi;t := xi;t+ri;t to denote participant i's noisy plaintext in time t. When the context is clear, we omit one or more of the subscripts and write bxi or bx instead. One challenge we face when designing the mechanism is how to reduce the necessary communication between the contributors and the data aggregator. If one allows the contributors and the aggregator to engage in an interactive multiple-party protocol in every time period, then standard Secure Multi-Party Estimation techniques can be used to ensure that the data aggregator learns only the sum. However, the requirement that all contributors must be simultaneously online and interact with each other regularly furnishes many applications impractical, especially large-scale cloud application

III. RELATED WORK

In this concept, we review the existing work for privacy protection in data aggregation on which serves the function target efficient privacy-preserving dynamic medical text mining and image feature extraction. Privacy protection for data aggregation provides a potential solution for Homomorphic Encryption techniques. In proposed, simple and secure additively homomorphic stream cipher that permits efficient aggregation of encrypted data. The main theme for replace the exclusive-OR (XOR) operations in stream ciphers with modular addition.

NETWORK ARCHITECTURE AND SECURITY MODEL:

Privacy preserving for dynamic medical text mining and image feature extraction are classified into three entities: the patient, the healthcare provider and the cloud. A set of body sensors is deployed on patient to monitor the medical texts and images, which are frequently aggregated in patient's handheld devices such as PDA and expanded to cloud in the encrypted level. Both body sensors and handheld devices are used as resource constraints for computation and communication systems. Therefore, it required to design a lightweight encryption technique to encode the PHIs from programmed circuits embedded in patient's handheld device. On the other hand, the resource constrained body sensors and handheld devices cannot allow to locally storing a large number of frequently monitored PHI text and medical images.

Medical cloud provides a convincing solution for patients to deploy both the storage and computation in a"pay-per-use" manner in such a resource asymmetrically allotted in the environment. By executing the PPDM technique, the cloud server performs privacy preserving from correlation matches for medical text mining and Scale Invariant Feature Transform for image feature extraction in encrypted domain. The cloud server is affected to work under a honest but curious model where it executes the protocol specification, but it designate to extract the patient's secret PHI from interactions with both the patient and the physician. In proposed network architecture, the entities provide a PHI text/images and medical templates are different. Our proposed PPDM can be applied to a special case where PHI text/image and medical template providers are the same entity, the assumption that the physicians have deployed a series of encrypted medical arrangements into the cloud, and then delegate the privacy preserving medical text mining and image feature extraction to the cloud.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
ernational Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
l. 3, Special Issue 2, March 2016

IV.CONCLUSION

A secure and efficient privacy-preserving medical text mining and extraction of image feature scheme PPDM is proposed cloud assisted e-healthcare system. Firstly, an efficient privacy-preserving fully homomorphic data aggregation from any one-way trapdoors function is proposed, which acts the basis for our proposed PPDM. Then, an outsourced disease modeling and early interposition is achieved, respectively by devising an efficient privacy preserving function inter relationship matching PPDM1 from medical text mining and design a privacy-preserving extraction of medical image feature PPDM2. Finally, the formal security proof and extensive performance evaluation demonstrate our proposed PPDM achieves a higher security level 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] J. Taeho, X. Mao and X. Li, *Privacy-preserving Data Aggregation without Secure Channel: Multivariate Polynomial Evaluation*, IEEE INFOCOM 2013.

[2] Shreyas Hrimant Shinde and Dhanshri Patil, *Review on Security and Privacy for Mobile Healthcare Networks: From a Quality of Protection Perspective, 2015.*

[3] N. P. Smart and F. Vercauteren, *Fully homomorphic encryption with relatively small key and ciphertext sizes*, 2010.

[4] C.Y. Hsu, C.S. Lu and S.C. Pei, *Image Feature Extraction in Encrypted Domain with Privacy-preserving SIFT*, IEEE Trans. on Image Processing, 2012.

[5] E. Shi, T.-H.H. Chan, E.G. Rieffel, R. Chow and D. Song, *Privacy preserving aggregation of time-series data*, 2011.

[6] C. Castelluccia, A.C.-F. Chan, E. Mykletun and G. Tsudik, *Efficient and provably secure aggregatioin of encrypted data in wireless sensor networks*, 2009.

[7] I. Damgard, M. Geisler, and M. Kroigard, *Homomorphic encryption and Secure comparison*, 2008.

[8] M. V. Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, *Fully homomorphic encryption over the integers*, 2010.

[9] J. Domingo-Ferrer, *A provably secure additive and multiplicative privacy homomorphism*, 2002.

[10] V. Goyal, O. Pandey, A. Sahai and B. Waters, *Attribute-based Encryption for Fine-grained Access Control of Encrypted Data*, 2006.

[11] 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*, 2007.

[12] Z. Erkin and G. Tsudik, *Private computation of spatial and temporal power consumption with smart meters*, 2012.

[13] C. Gentry, *Fully homomorphic encryption using ideal lattices*, 2009.

[14] F.D. Garcia and B. Jacobs, *Privacy-friendly energy-metering via homomorphic Encryption*, 2010.

[15] R. Gennaro, C. Gentry and B. Parno, *Non-interactive verifiable computing: outsourcing computation to untrusted workers*, 2010.