International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Techniques for Securing Medical Datas in Cloud

Sanjeevan T, Sundar Murthi K A, Bhuvaneshwaran S, Dr. Kalaichelvi T
Department of CSE, Panimalar Institute of Technology, Chennai, Tamil Nadu, India

ABSTRACT

The multiple number of Hospital records are integrated into the Cloud server. Mongo lab is used as Data storage cloud server.Personal information & Medical Data are separately Encrypted & stored in different servers. Medical data is anonymised, Re-encrypted and stored in the main cloud server. Data is transferred / retrieved from cloud server after verifying the OTP. Big Data is used here.Data Anonymization enables dual i.e double security for the sensitive medical details of the user.By hiding the sensitive informations of every end users.
Keywords : Mongo lab, OTP, EHR, IND-KGA, SCF-PEKS, PEKS, PKEET, CSI

I. INTRODUCTION

The Electronic health records (EHR) system will make medical records to be computerized with the ability to prevent medical errors.Initially they are stored in cloud environment.It will facilitate a patient to create his own health information in one hospital and manage or share the information with others in other hospitals.Every user has to create an account according to their stream.The details of patients such as name,address,contact details and medical details are maintained in cloud.In the traditional time-release system, the time seal is encapsulated in the cipher text at the very beginning of the encryption algorithm.Patient details can be encrypted once and the details are only visible to doctor and hospital staffs.After the double encryption process details are the exact details of patients are hidden.Thus they enables high security to the sensitive medical datas which are at risk of attack in the existing system

II. METHODS AND MATERIAL

A. Literature Survey

1. Electronic Health Records:Challenges And Opportunities

Jaymeen R. Shah et.all

Department of Computer Information Systems & Quantitative Methods
Texas State University,USA

Says that the adoption of electronic health records has been controversial and challenging in the US during last few years. In this paper authors have discussed the legal, issues in security and privacy are emerged with EHRs. Best practices are adopted related to the privacy and security of healthcare data that are at rest are the pivot to the trust relationships needed when exchanging health data across the healthcare networks. Healthcare practice chiefs need guidance for implementing the best security and practices. The best practices include understanding of the legal framework involved, managing information context and content,implementingand identifying suitable technical solutions including the architectures and technical standards,and procedural frameworks are necessary to achieve secure and effective management of health information exchange and storage policies. EHR systems are expensive, and they risks of attack by stealing security and privacy of patients. However, it is certain that the use of EHRs would improve efficiency and quality of health care for the patients. It is required that IT staff at medical facilities use data management and network best practices, follow management and risk assessment guidelines, and be on the forefront of

technological advances to ensure the privacy and security of patients' data. If the EHR and their technologies are effectively implemented, they can decrease medical errors, improve the quality of patient care provided, which makes healthcare more efficient.

2. Public Key Encryption With Keyword Search Secure Against Keyword Guessing Attacks Without Random Oracle
   Liming Fanget.all
   Nanjing University of Aeronautics and Astronautics

Says that ,in this paper provides a formal model of SCF-PEKS secure against keyword guessing attacks. Furthermore, we present an SCF-PEKS scheme secure against ciphertext attacks and chosen keyword, and keyword guessing attacks. Based on the DBDH assumption,the truncated q-ABDHE assumption andSXDH assumption, we first proved its indistinguishability of secure channel free PEKS against ciphertext attack (IND-SCFCKCA) security without random oracle and chosen keyword. We also analyzed the security and computational consistency against keyword guessing attacks (IND-KGA) of our scheme. This work motivates a few interesting questions. First, how to achieve a more systematic SCF-PEKS scheme without random oracle is advantageous. We opened the new direction on how to achieve this notion, but the more effective variant is certainly required. Second, how to construct SCF-PEKS scheme secure against keyword guessing attacks without requiring bilinear pairing operations would be very fascinating.

3. Conjunctive, Subset, And Range Queries On Encrypted Data
   Dan Bonehet.all

Says that,in public key systems supporting queries on encrypted data a secret key can produce tokens for testing any supported query predicate. The token lets anyone test the predicate on a given ciphertext without learning any other information about the plaintext. We presented a general framework for analyzing security of searching on encrypted data systems. We then constructed systems for comparisons and subset queries as well as conjunctive versions of these predicates. The underlying tool behind these new constructions is a primitive we call HVE. The onedimensional version of HVE (namely ` = 1) is essentially an Anonymous IBE system. For large ` we obtain a new concept that is extremely useful for a large variety of searching predicates. We note that by setting ` = 1 in our HVE construction we obtain a new simple anonymous IBE system secure without random oracles. This work posses many challenging open problems. For example, the best non-conjunctive (i.e. w = 1) comparison system we currently have requires ciphertexts of size O($\sqrt{}$ n) where n is the domain size. In principal it should be possible to improve this to O(log n), but this is currently a wide open problem that will require new ideas. Similarly, for non-conjunctive subset queries the best we have requires ciphertexts of size O(n). Again, can this be improved to O(log n)? Our results mostly focus on conjunction. Are there similar results for disjunctive queries? More generally, what other classes of predicates can we search on?

4. Public Key Encryption Schemes Supporting Equality Test With Authorization Of Different Granularity
   Qiang Tang
   DIES, Faculty of EEMCS University of Twente,7522 NB Enschede, The Netherlands

Says that in the paper they have reviewed the concepts of PKEET, AoN-PKEET, and FG-PKEET, and discussed their capabilities in authorizing users to control who can perform equality test on their the available security guarantees and ciphertexts. Our analysis has shown that offline message recovery attack is a security concern for all primitives, although only semi-trusted proxies can carry out the attack in the case of FG-PKEET andAoN-PKEET. To address the concern, we have proposed the concept of FG-PKEET+, namely FGPKEET in two-proxy setting. The tradeoff is clear: an FG-PKEET+ cryptosystem can prevent offline message recovery attacks but it is more expensive to carry out the test because it requires an interactive protocol between two proxies. When to choose which primitive to use is depending on the efficiency requirements and security of the specific application scenario. It is an interesting future work to further investigate on. Recall from Section 6, one of the motivations of the two-proxy setting is to mitigate the caveat that the proxy can test equality of Ui 'sciphertexts, given a token Ti,j . It remains as an interesting future work to propose a FG-PKEET cryptosystem without this caveat, where the attack game for fine-grained authorization property is

identical to that in Figure 3 except that i = j and t = w are allowed in the game.

5. On A Security Model Of Conjunctive Keyword Search Over Encrypted Relational Database
Jin WookByunet.all

Palo Alto Research Center 3333 Coyote Hill Road Palo Alto, CA 94304, USA

Says that,most schemes have just considered on insider security on indistinguishability of CSI and they have focused on a problem of how the scheme can prevent insider attackers like server manager from obtaining keyword information through CSI in the database. In practice, however, it is also important to guarantee the security against the outsider attackers which cannot see encrypted documents but tries to retrieve information on keywords by modifying protocol messages and capturing. In fact, the work of [5, 15] first addressed problems of keyword guessing attacks by outsider attacker, but it has no investigation of formal behavior of outsider attackers. In this paper, we presented a security model for conjunctive keyword search in UDU setting. The model defines not onlyoutsider security for trapdoor security but also insider security for CSI value. We analyzed the existing protocol under the suggested security model and we demonstrated its weakness and countermeasure. In the SDU setting, HVE scheme [7] first handled the problems of conjunctive search, comparison, subset range queries, but there is still opportunity for improvements both in computation and communication costs as mentioned in [7]. However, in the UDU setting, it still remains an open problem to securely design a conjunctive keyword search scheme without user's PKI-based approach under standard assumption, requires constant communication, computation, storage costs.

6. A New Public Key Encryption With Conjunctive Field Keyword Search Scheme
Min-Shiang Hwang et.all

Asia University, Department of Computer Science and Information Engineering No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan

Says thatthey present an efficient SCF-PECKS scheme that can stand against the off-line keyword-guessing attack. Our scheme is constructed in bilinear pairing based on ElGamal system and the security is under decisional Diffie-Hellman assumption without random oracle. Our scheme is more efficient than other conjunctive keyword searchable schemes and is more suitable for the weak devices. In addition, this scheme can be extended into the multi-user conjunctive keyword search scheme in the future.

B. Existing System

The privacy and security of the sensitive personal information are the major concerns of the users, which could hinder further development and widely adoption of the systems.

C. Proposed System

Timing enabled proxy re-encryption searchable encryption model is applied to Electronic Health Records (EHR) to formally proved secure against chosen-keyword chosen-time attack. Furthermore, offline keyword guessing attacks can be resisted too. Data owner outsource their encrypted data with time period to EHR storage provider. Proxy server encapsulates time into re-encryption cipher text.

D. Architecture Diagram

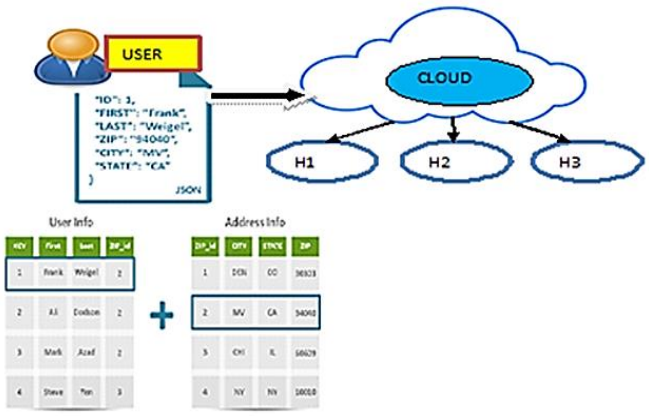

Figure 1. Architecture diagram

Fig 1:The multiple Hospital records integrated in the Cloud server. Mongo lab is used as Data storage cloud server.Personal information & Medical Data are separately Encrypted& stored in different servers.Medical data is anonymised, Re-encrypted and stored in the main cloud server.Data is transferred / retrieved from cloud server after verifying the OTP. Big Data is used.

III. CONCLUSION

The Electronic health records(EHR) maintained in cloud environment.The Personal information & Medical Data are separately Encrypted & stored in different servers. Medical data is anonymised, Re-encrypted and stored in the main cloud server.So,it enables high security to the sensitive medical datas which are at the risk of attack.

IV.REFERENCES

[1] J. C. Leventhal, J. A. Cummins, P. H. Schwartz, D. K. Martin, and W. M. Tierney, "Designing a system for patients controlling providers' access to their electronic health records: Organizational and technical challenges," J. General Internal Med., vol. 30, no. 1, pp. 17–24, 2015.

[2] Microsoft. Microsoft HealthVault.May 1, 2015.

[3] Google Inc. Google Health.Jan. 1, 2013.

[4] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. EUROCRYPT, vol. 3027. Interlaken, Switzerland, May 2004, pp. 506–522.

[5] Q. Tang, "Public key encryption schemes supporting equality test with authorisation of different granularity," Int. J. Appl. Cryptogr., vol. 2, no. 4, pp. 304–321, 2012.

[6] P. Liu, J. Wang, H. Ma, and H. Nie, "Efficient verifiable public key encryption with keyword search based on KP-ABE," in Proc. IEEE 9th Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA), Nov. 2014, pp. 584–589.

[7] L. Fang, W. Susilo, C. Ge, and J. Wang, "Public key encryption with keyword search secure against keyword guessing attacks without random oracle," Inf. Sci., vol. 238, pp. 221–241, Jul. 2013.

[8] M.-S. Hwang, S.-T. Hsu, and C.-C. Lee, "A new public key encryption with conjunctive field keyword search scheme," Inf. Technol. Control, vol. 43, no. 3, pp. 277–288, 2014.