WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Scalable and Secure Sharing Of Personal Health Records in Cloud Computing Using CP-Attribute-Based Encryption

B. Basheera[#1], F. Asmathunnissa[#2]

[#1] M.Sc, Department of Computer Science, Kamban College of Arts and Science for Women, Tiruvannamalai-606603

[#2] Assistant professor, Department of Computer Science, Kamban College of Arts and Science for Women, Tiruvannamalai-606603

ABSTRACT

Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access, and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute-based encryption (CP_ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability, and efficiency of our proposed scheme.

keywords:PHR,cp-ABE, ACCUARCY

1.INTRODUCTION:

Loud storage [1] is an emerging model of storage to provide scalable, elastic and pay-as-you-use service to cloud computing users. For individual usage, the subscribers enjoy the freedom to access to their data anywhere, anytime with any device. When cloud storage [2] is utilized by a group of users, it allows team members to synchronize and manage all shared documents. Moreover, it also saves the user a lot of capital investment of expensive storage equipments [3]. Cloud delivers convenience to the customers and at the same time arouses many security and privacy problems [4], [5]. The customers prefer to adopt the encryption technology to protect the data confidentiality, which meanwhile arouses another problem: how to execute data retrieval on the large volume of ciphertext. It is almost Y. Yang is with College of Mathematics and Computer Science, Fuzhou University, Fuzhou, China; Fujian Provincial Key Laboratory of Network Computing and Intelligent Information Processing, Fuzhou University, China; Key Laboratory of Spatial Data Mining & Information Sharing, Ministry of Education, Fuzhou, China; University Key Laboratory of Information Security of Network Systems (Fuzhou University), Fujian Province, China; Fujian Provincial Key Laboratory of Information Processing and Intelligent Control (Minjiang University), Fuzhou, China. E-mail: yang.yang.research@gmail.com. X. Zheng and W. Guo are with College of Mathematics and Computer Science, Fuzhou University, Fuzhou, China; Fujian Provincial Key Laboratory of Network Computing and Intelligent Information Processing, Fuzhou University, China; Key Laboratory of Spatial Data Mining & Information Sharing, Ministry of Education, Fuzhou, China. E-mail: xianghan.zheng@fzu.edu.cn, guowenzhong@fzu.edu.cn. C. Rong is with Department of Electronic Engineering and Computer Science, University of Stavanger, Norway. E-mail: chunming.rong@uis.no. Corresponding authors: XianghanZheng, WenzhongGuo. unimaginable to ask the cloud subscriber to download all of their stored information and then decrypt and search on the recovered plaintext documents.The data user generates a token of the content that he wants to search using his private key. Receiving the token, the cloud server searches on the encrypted data without decrypting the ciphertext. The most important point is that the server learns nothing about the plaintext of the encrypted data nor the searched content during the data retrieval procedure. However, most of the available searchable encryption schemes only support some basic search patterns, such as single keyword search, conjunctive keyword search and boolean search. Since the cloud computing is a fierce competition industry, it is of vital importance to provide good user experience. It is urgent to design novel searchable encryption schemes with expressive search pattern for cloud storage.While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide

adoption. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust.

On the one hand, although there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates. cloud providers are usually not covered entities .On the other hand, due to the high value of the sensitive PHI, the third-party storage servers are often the targets of various malicious behaviours which may lead to exposure of the PHI. As a famous incident, a Department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who took the data home without authorization.

To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi trusted servers.

A feasible and promising approach would be to encrypt the data before out sourcing. Basically the PHR owner herself should decide how to encrypt there files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to theirs to fusers. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary. However, the goal of patient-centric privacy is often in conflict with scalability in a PHR system.

The latter has potentially large scale; should each owner herself be directly responsible for managing all the professional users, she will easily be over whelmed by the key management overhead. In addition, since those users' access requests are generally unpredictable, it is difficult for an owner to determine a list of them. On the other hand, different from the single data owner scenario considered in most of the existing works

The complexities per encryption, key generation, and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are nontrivial to solve, and remain largely open up-to-date. To this end, we make the following main contributions.

1.We propose a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multiowner settings. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains (PSDs). In particular, the majority professional users are managed distributive by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain. In this way, our framework can simultaneously handle different types of PHR sharing applications' requirements, while incurring minimal key management overhead for both owners and users in the system. In addition, the framework enforces write access control, handles dynamic policy updates, and provides break-glass access to PHRs under emergence scenarios.

2. In the public domain, we use multi authority ABE (MA-ABE) to improve the security and avoid eyes crow problem. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system. We propose mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes.

3. We provide a thorough analysis of the complexity and scalability of our proposed secure PHR sharing solution, in terms of multiple metrics in computation, communication, storage, and key management. We also compare our scheme to several previous ones in complexity, scalability and security. Furthermore, we demonstrate the efficiency of our scheme by implementing it on a modern workstation and performing experiments/simulations.

2. LITERATURE SURVEY

[1] 2016,**Joseph K. Liu, Kaitai Liang, Willy Susilo,**In this paper, we propose a two-factor data security protection mechanism with factor revocability for cloud storage system. Our system allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). The receiver needs to possess two things in order to decrypt the ciphertext. The first thing is his/her secret key stored in the computer. The second thing is a unique personal security device which connects to the computer. It is impossible to decrypt the ciphertext without either piece. More importantly, once the security device is stolen or lost, this device is revoked. It cannot be used to decrypt any ciphertext. This can be done by the cloud server which will immediately execute some algorithms to change the existing ciphertext to be un-decryptable by this device. This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any ciphertext at any time. The security and efficiency analysis show that our system is not only secure but also practical.

[2] 2017**, Joseph K. Liu, Kaitai Liang, Willy Susilo,** As one important technique of fuzzy clustering in data mining and pattern recognition, the possibilistic c-means algorithm (PCM) has been widely used in image analysis and knowledge discovery. However, it is difficult for PCM to produce a good result for clustering big data, especially for heterogenous data, since it is initially designed for only small structured dataset. To tackle this problem, the paper proposes a high-order PCM algorithm (HOPCM) for big data clustering by optimizing the objective function in the tensor space. Further, we design a distributed HOPCM method based on MapReduce for very large amounts of heterogeneous data. Finally, we devise a privacy-

preserving HOPCM algorithm (PPHOPCM) to protect the private data on cloud by applying the BGV encryption scheme to HOPCM, In PPHOPCM, the functions for updating the membership matrix and clustering centers are approximated as polynomial functions to support the secure computing of the BGV scheme. Experimental results indicate that PPHOPCM can effectively cluster a large number of heterogeneous data using cloud computing without disclosure of private data..

[3] 2014, QingjiZheng† ShouhuaiXu† Giuseppe Ateniese, It is common nowadays for data owners to outsource their data to the cloud. Since the cloud cannot be fully trusted, the outsourced data should be encrypted. This however brings a range of problems, such as: How should a data owner grant search capabilities to the data users? How can the authorized data users search over a data owner's outsourced encrypted data? How can the data users be assured that the cloud faithfully executed the search operations on their behalf? Motivated by these questions, we propose a novel cryptographic solution, called verifiable attribute-based keyword search (VABKS). The solution allows a data user, whose credentials satisfy a data owner's access control policy, to (i) search over the data owner's outsourced encrypted data, (ii) outsource the tedious search operations to the cloud, and (iii) verify whether the cloud has faithfully executed the search operations. We formally define the security requirements of VABKS and describe a construction that satisfies them. Performance evaluation shows that the proposed schemes are practical and deployable.

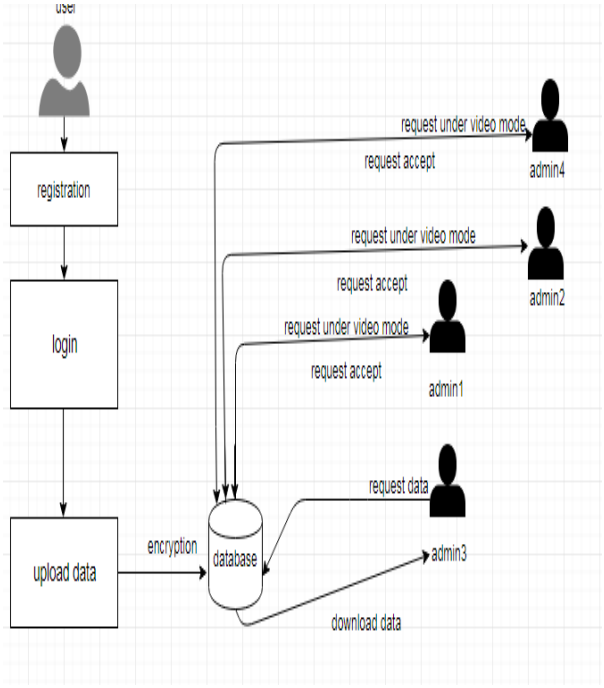
[4] 2015, :**Victor Chang, Muthu Ramachandran,** Offering real-time data security for petabytes of data is important for Cloud Computing. A recent survey on cloud security states that the security of users' data has the highest priority as well as concern. We believe this can only be able to achieve with an approach that is systematic, adoptable and well-structured. Therefore, this paper has developed a framework known as Cloud Computing Adoption Framework (CCAF) which has been customized for securing cloud data. This paper explains the overview, rationale and components in the CCAF to protect data security. CCAF is illustrated by the system design based on the requirements and the implementation demonstrated by the CCAF multi-layered security. Since our Data Center has 10 petabytes of data, there is a huge task to provide real-time protection and quarantine. We use Business Process Modeling Notation (BPMN) to simulate how data is in use. The use of BPMN simulation allows us to evaluate the chosen security performances before actual implementation. Results show that the time to take control of security breach can take between 50 and 125 hours. This means that additional security is required to ensure all data is well-protected in the crucial 125 hours. This paper has also demonstrated that CCAF multi-layered security can protect data in real-time and it has three layers of security: 1) firewall and access control; 2) identity management and intrusion prevention and 3) convergent encryption. To validate CCAF, this paper has undertaken two sets of ethical-hacking experiments involved with penetration testing with 10,000 trojans and viruses. The CCAF multi-layered security can block 9,919 viruses and trojans which can be destroyed in seconds and the remaining ones can be quarantined or isolated. The experiments show although the percentage of blocking can decrease for continuous injection of viruses and trojans, 97.43% of them can be quarantined. Our CCAF multi-layered security has an average of 20% better performance than the single-layered approach which could only block 7,438 viruses and trojans. CCAF.

[5] 2014, **: G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,** Remote data integrity checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multi-cloud storage. The formal system model and security model are given. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie- Hellman) problem. In addition to the structural advantage of elimination of certificate management.

3. PROPOSED SYSTEM

In this project we have to secure the file is the main motivation. In this, there is two parts are there one is user side and another one is admin side.In user side ,only they will upload the data in the form of file.After that in an admin side,there are user wants the file they needs acknowledgements of the other then only they will use the file else they are not accepting the file in the user side they used to download file by using the key .The main motive is that,if the first user wants the file the other than acknowledgement system is very important then the process initisalised by using the fragmentation part.

4. SYSTEM ARCHITECTURE:



5. METHODOLOGY

5.1 USER INTERFACE DESIGN:

This is the first module of our project. Theimportant role for the user is to move login window to user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user id and valid password). If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user. It well improves the security and preventing from unauthorized user enters into the network. In our project we are using JSP for creating design. Here we validate the login user and server authentication.

5.2 FILE UPLOAD:

User will login their account and upload a file or image, and that files/image are encrypt and store in admin side. Even uploaded user also doesn't access ,before admin can accept.

cloud computing also brings very serious security problems, especially for users' data stored in the cloud

In order to protect users' privacy, when the legal cloud users access cloud service resources, users need to verify the cloud server, and cloud server needs to identify the users' login requests to ensure that the users are legal users.

5.3 SECURITY PROVIDING FOR FILE:

In this part Admin will maintain the file,if the one admin from the admin team wants file they wants an acknowledgement of the other admins.The main motive is that secure the file.

5.4 ADMIN MONITORING THE FILE:

In this part admins will maintain the file, after that the admin will monitor the files in the way of video mode.If anyone of the admin from the admins team are going to request a file,the request will go by video mode.

5.5 VIEW/READ FILE:

For reading each file which have been uploaded and split into 4 parts we should be owner of the file otherwise we should know the four different key which have been combined by random algorithm after reading the file you can also download the file otherwise with wrong key you can't open content.

6. CONCLUSION:

In this paper, we introduce a large universe searchable encryption scheme to protect the security of cloud storage system, which realizes regular language encryption The cloud service provider could test whether the encrypted regular language in the encrypted cipher text is acceptable by the DFA embedded in the submitted search token. In the test procedure, no plaintext of the regular language or will be leaked to the cloud server. We also put

forth a concrete construction with lightweight encryption and token generation algorithms. An example is given to show how the system works. The proposed scheme is privacy-preserving and indistinguishable against, fragmentation which are proved in standard model. The comparison and experiment result confirm the low transmission and computation overhead of the scheme

The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works.

7.FUTURE ENHANCEMENT:

An accumulation is often needed to gather the partial results from these parallel executions in different servers. The runtime system captures new events and run corresponding actions to analyze the page and store more URLs into the URL set to generate new events.

8.output

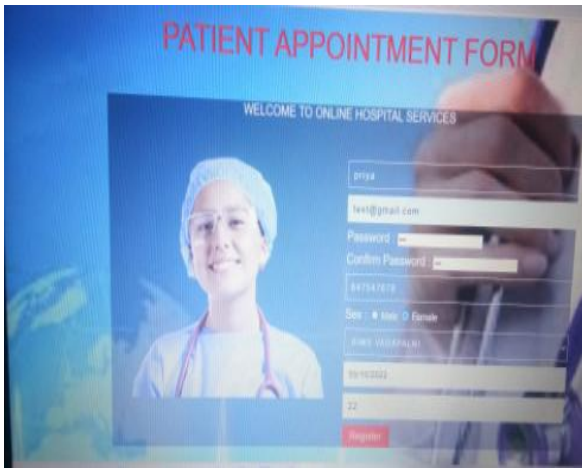


Fig 1: Data Transferring -Patient

Fig 1: Application Transferring –Doctor

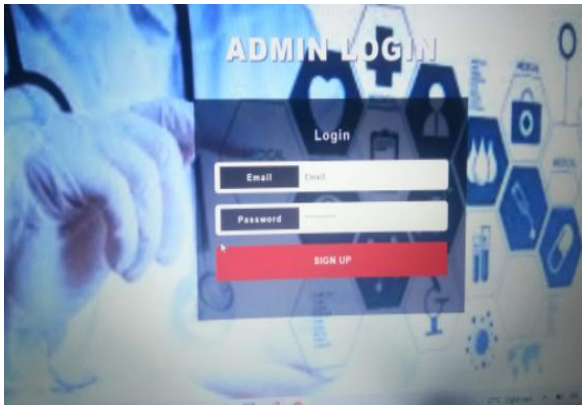


Fig 1: Access Authentication–Admin

REFERENCES

[1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010

[2] H. Lo¨hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2011.

[4] "The Health Insurance Portability and Accountability Act," http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp, 2012.

[5] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6] "At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded," http://articles.latimes.com/2006/jun/26/health/ he-privacy26, 2006.

[7] K.D. Mandl, P. Szolovits, and I.S. Kohane, "Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private," BMJ, vol. 322, no. 7281, pp. 283-287, Feb. 2001.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM '10, 2010.

[10] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[12] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 1, pp. 51-58, Feb. 2010.

[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.

[14] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-Policy Attribute-Based Threshold Decryption with Flexible Delegation and Revocation of User Attributes," 2009.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.