Volume 5, Issue 2, April 2018 ISSN: 2348-8565 (Online)
International Journal of Modern Engineering and Research Technology
Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

Enhancing the Security of Medical Data Transmission in Cloud Using Reversible Storage Identity Based Encryption Technique-A Review

Dr. Mukta Bhatele
Professor
Department of Computer Science & Engineering
Gyan Ganga Institute of Technology and Sciences
Jabalpur, (M.P.) [INDIA]
Email: mukta_bhatele@rediffmail.com

Samradhi Sharma
M.Tech. Research Scholar
Gyan Ganga Institute of Technology and Sciences
Jabalpur, (M.P.) [INDIA]
Email: samradhi_sharma@yahoo.com

ABSTRACT

Cloud computing becomes new computing standard for users. It provides services like software as a service, infrastructure as a services and platform as a service. In Cloud computing instead of using some hardware and software components in the computer, users can store the data, programs and accessing them easily through an internet. Cloud computing has both the broad network access and resource pooling to support big data from electronic health records. In calculation, analyze and control resource usage are measured service that has ability in regards to the type of service provided e.g., reserve and sharing. Necessarily it is important to put cryptographically augmented access control on such data. So, an encouraging crypto graphical primitive is needed to build a practical data sharing system, i.e., Identity-based encryption. The access control in this Identity-based encryption is not permanent. It should be implemented For the security purpose, a mechanism must be like where a user is removed from the system as soon as his/her permission is terminated. Consequently, the user cannot access the shared data anymore because he/she is removed. For this reason, the backward/forward secrecy of the cipher text should be provided which is known as revocable-storage identity-based encryption (RS_IBE). This approach acquaints the utilities of user repudiation and ciphertext update at the same time. Furthermore, we provide a detailed structure of Reversible storage-IBE, which certifies its secrecy in the described security model. By this RS-IBE scheme the realistic and cost-effective system of data sharing is achieved which has wonderful benefits of operability and potential. Certainly, To determine its practicability we provide implementation outcome of this suggested scheme.

Keywords:—*cloud computing, medical data, Reversible storage, identity based encryption , data security.*

I. INTRODUCTION

Present era is the era of Cloud Computing. privacy, reliability, ease of use, accuracy, and isolation are essential concerns for both Cloud providers and cloud user. cloud computing is a paradigm that provides very big computation capacity and huge memory space at a low cost. It enables users can access the services irrespective of time and location across numerous platforms it can be mobile devices, personal computers etc, and thus brings great ease to cloud users .

Medical information sharing is one of the most eye-catching applications of cloud computing, where searchable encryption is a interesting

solution for securely and easily sharing medical data among different medical organizers. For the sharing of personal medical records medical data information exchange model is used which allows a person to create, manage and control his medical information in cloud at centralized place. A Person can now share his medical records successfully with a wide variety of users such as family members, friends, consultants, doctors and insurance agencies. The main concern is about the confidentiality of patients' medical data . As patients lose full control to their own medical data, directly placing those responsive data under the control of the untrusted servers cannot provide strong privacy assurance at all.

Cloud Computing plays an important role by providing a capability of storage as service and software as service, by which software service providers can enjoy the almost infinite and expandable storage and computing resources. While going for cloud storage, the data owner and cloud servers are in two different domains. On one hand, these untrusted servers are not free to access the outsourced data content for data secrecy, on the other hand, the data resources are not physically under the full control of data owner. Storing medical data on the untrusted server leads to need of encryption mechanism to protect the medical data, before outsourcing to the cloud. To this end, the health records should be encrypted in addition to conventional access control mechanisms provided by the server.

As a result of the fast development in the technology and telecommunications, a lot of digital applications such as the telemedicine start to appear. This application facilitates the transmission and sharing of the patient's medical data by the healthcare professionals for further judgment works. Cloud computing, the environment that offers resources encapsulation on the Internet in the form of dynamic, scalable, and virtualized services, presents a variety of on demand services to the public such as the telemedicine services. Over this environment, the user can enjoy a lot of benefits offered by this computing paradigm like transmission, storage, and further processing needs on the user data. In spite of the cloud computing reward, it has a number of disadvantages such as the data security which considered a major problem that face the users of this technology since they outsource their data to distributed storage systems and not a local ones . Therefore, when transferring user's data over the cloud environment, especially the medical data, this kind of data which contains vital information about the patients, a high level of protection of the reliability and privacy of these data have to be guaranteed to overcome any attacking attempts that may face these transmitted data.

Cloud security: Furthermore to over come the above security problem .identity based access control placed on shared data should meet the following measures of security:

Data confidential: Confidentiality, in the context of computer systems, allows authorized users to access sensitive and protected data. Specific mechanisms ensure confidentiality and safeguard data from harmful intruders.

Best practices used to ensure confidentiality are as follows:

- An authentication process, which ensures that authorized users are assigned confidential user identification and passwords. Another type of authentication is biometrics.
- Role-based security methods may be employed to ensure user or viewer authorization. For example, data access levels may be assigned to specified department staff.
- Access controls ensure that user actions remain within their roles. For example, if

a user is authorized to read but not write data, defined system controls may be integrated.

Access controllability

Access controllability means that a data owner can perform the selective restriction of access to others can not right to use it without permissions. Further, it is desirable to enforce fine-grained access control to the outsourced data, i.e., different users should be granted different access rights with regard to different data pieces. The access authorization must be controlled only by the owner in untrusted cloud environments.

Integrity

Data integrity demands maintaining and assuring the accuracy and completeness of data. A data owner always expects that her or his data in a cloud can be stored correctly and trustworthily. It means that the data should not be illegally tampered, improperly modified, deliberately deleted, or maliciously fabricated. If any undesirable operations corrupt or delete the data, the owner should be able to detect the corruption or loss. Further, when a portion of the outsourced data is corrupted or lost, it can still be retrieved by the data users.

Medical Image Sharing is a term for the electronic exchange of medical images between hospitals, physicians and patients. Rather than using traditional media, such as a CD or DVD, and either shipping it out or having patients carry it with them, technology now allows for the sharing of these images using the cloud. The primary format for images is DICOM (Digital Imaging and Communications in Medicine). Typically, non-image data such as reports may be attached in standard formats like PDF (Portable Document Format) during the sending process. Additionally, there are standards in the industry, such as IHE Cross Enterprise Document Sharing for Imaging (XDS-I), for managing the sharing of documents between healthcare enterprises. A typical architecture involved in setup is a locally installed server, which sits behind the firewall, allowing secure transmissions with outside facilities.

Benefits: Improved access to patients' medical imaging histories, Ability to view images instant, Real-time collaboration by specialists, Avoiding duplicate care reduces costs, Decreased radiation exposure for patients Expertise and specialized opinion is remotely accessible to patients.

Additional Requirements: For access control of stored medical data , third party untrusted servers are considered. With cryptographic techniques, the aim is trying to find out who has access to which parts of a patient's medical data/ documents in a fine-grained manner.

A. In Symmetric Key Cryptography: They are a class of algorithms for cryptography for both encryption of plaintext and decryption of ciphertext which same cryptographic keys are used .The keys may be identical or may be somewhat different. The keys, in practice represent a shared secret between two or more users that can be used to maintain a private information. Proposed a solution for securing outsourced data on semi-trusted servers based on symmetric key derivation methods, which can achieve fine-grained access control. But the involvement of file creation and user grant operations is linear to the number of certified users, which is not much scalable.

B. In Public Key Cryptography: PKC based solutions were proposed because of its ability to separate read and write privileges. To realize fine-grained access control, the traditional public key encryption (PKE) based schemes proposed by J. Benaloh, M. Chase, E. Horvitz, and K. Lauter in their work "Patient controlled encryption: ensuring privacy of electronic medical records", they put forward how public and symmetric based encryption is used , disadvantage of their solution is either a key

administration is an overhead, or require encrypting multiple copies of a file using different users' keys.

C. Attribute Based Encryption based solutions: The ABE technique is implemented to realize finegrained access control for outsourced data; it is also used to secure electronic healthcare records (EHRs). Narayan et al. proposed an attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of Cipher Text-ABE (CP-ABE) .

But the ciphertext length increases gradually with the number of unrevoked users. In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs. Ibraimi et.al. applied ciphertext policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains but they do not use multi-authority ABE . In, Akinyele et al. investigated using ABE to generate self protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline. The drawback here is device dependency and user revocation is not supported. Also another drawback of all above solutions is problem of key-security as they consider single trusted authority.

D. Non Revocable Data Sharing System : The non-revocable data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. Note that the process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, the use of secret key should be limited to only usual decryption, and it is unwise to update the ciphertext periodically by using secret key. Another challenge comes from efficiency. To update the cipher text of the shared data, the data provider has to frequently carry out the procedure of download -decrypt-re-encrypt-upload. This process brings great communication and computation cost , and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage.

II . Proposed Solution

Identity Based Encryption

Identity-Based Encryption takes a effective approach to the crisis of encryption key management. IBE can use public key as any string, without the need of certificate it protects the data . key server provides the protection n which controls the generation of private decryption keys. By separating authentication and authorization from private key generation through the key server, dynamically it controlled the permission to generate key on a granular policy driven basis ,facilitating grainy control over access to information in actual time.

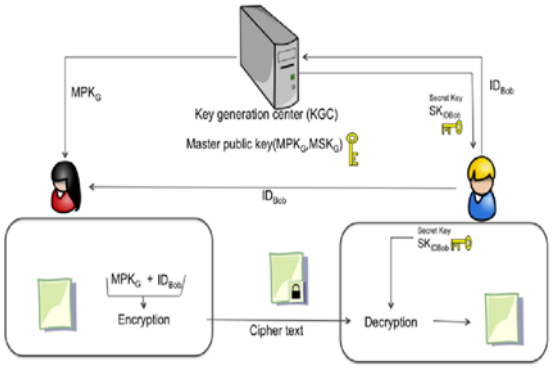

Figure 1. Identity Based Encryption

III. Reversible Storage Identity Based Encryption

Reversible storage identity based encryption One method to avoid those problem is directly re-encrypt the cipher text of the shared data to the cloud server. However, cipher text extension may introduce namely, cipher text size of the shared data is linear in the number of times the shared data have been updated. In addition, the technique of substitute re-

encryption can also be used to overcome the problem of efficiency.

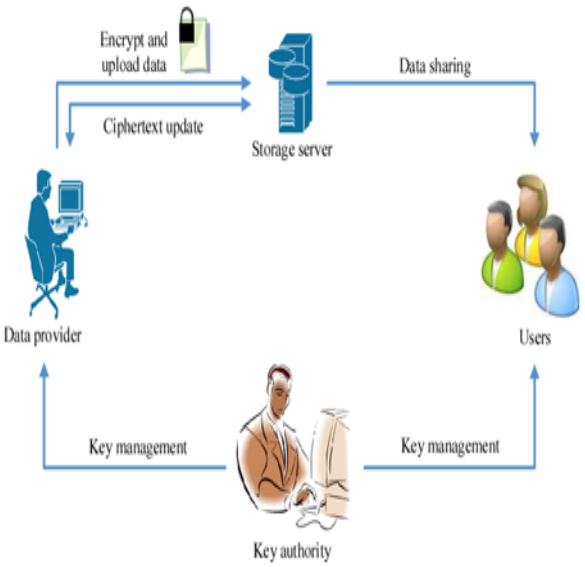

Figure 2. Working of Reversible Identity Based Encryption

This system of data sharing will work as follows:

Step 1: Firstly, the data provider A first decide the users X, Y with whom he/she can be shared data. Using their identities, A encrypts and uploads this ciphertext to the essential server in the cloud for X and Y.

Step 2: By downloading the ciphertext and decrypting it, X as well as Y can get the data that is shared. Nevertheless, for the unauthenticated user and the server, the data which is in the form of plaintext will not be available.

Step 3: In certain cases, when X's authorization is terminated, the shared data ciphertext is downloaded by the data provider A. A will decrypt the ciphertext and then re-encrypts the data so that X is forbidden from being able to access it and then the re-encrypted data is uploaded to the cloud once more. Now the user X is made available with the data. And the user can download the cipher text and by decrypting it, the plaintext will be made available.

IV. CONCLUSION

The records of personal data are now considered as an up-and-coming trend in the personal health information exchange field. Here user highly utilized cloud storage and transmission service. The main privacy issue is security of data ,the reversible storage identity based encryptions and its related techniques which are applied in order to enforce for the security function. The medical sharing will use more secure encryption methods in the future for minimizing the key management problems and complexity and for providing more secure storage and sharing facility to the data's stored in the clouds servers.

REFERENCES:

[1] Aiello, W., Lodha, S., Ostrovsky, R.: Fast Digital Identity Revocation (Extended Abstract). In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 137–152. Springer, Heidelberg (1998).

[2] Baek, J., Zheng, Y.: Identity-Based Threshold Decryption. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 262–276. Springer, Heidelberg (2004)

[3] Boldyreva, A., Goyal, V., Kumar, V.: Identity-based encryption with efficient revocation. In: ACM CCS 2008, pp. 417–426 (2008)

[4] Boneh, D., Boyen, X.: Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)

[5] Boneh, D., Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption.

SIAM J. Comput. 36(5), 1301132 (2007)MathSciNet

[6] Boneh, D., Ding, X., Tsudik, G., Wong, C.-M.: A method for fast revocation of public key certificates and security capabilities. In: USENIX Security Symposium 2001. USENIX (2001)

[7] Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. SIAM J. Comput. 32(3), 586 –615 (2003) MathSciNet.

[8] Andersen, K. Y. Yigzaw, and R. Karlsen, "Privacy Preserving health data processing," in e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on. IEEE, 2014, pp. 225-230.

* * * * *