IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10513

AN EFFICIENT ENCRYPTED MEDICAL DATA STORAGE USING TWO CLOUDS WITH DUPLICATE DATA GENERATION TECHNIQUES

Ms.S.Jayapratha , M.E[1], S.Shanmathi[2], M.Vinodhini[3], A.Hemalatha[4]

Assistant Professor, Department of Computer Science and Engineering, Sri Bharathi Engineering College for Women, Kaikkurichi, Pudukkottai-622303, Tamil Nadu, India[1]

B.Tech ,Information Technology,Sri Bharathi Engineering College for Women, Kaikkurichi, Pudukkottai, 622303,Tamil Nadu, India[2-4]

Abstract- In cloud secure personal data sharing is the important issues because it creates several securities and data confidentiality problem while accessing the cloud services. Many challenges present in personal data sharing such as data privacy protection, flexible data sharing, efficient authority delegation, computation efficiency optimization, are remaining toward achieving practical fine-grained access control in the Personal Information Sharing system. Personal records must be encrypted to protect privacy before outsourcing to the cloud. Aiming at solving the above challenges, here propose an efficient data sharing mechanism for Personal Data Sharing, which not only achieves data privacy, fine-grained access control and authority delegation simultaneously. Proposed system is used to secure patients' MHR (Medical Health Record) in the healthcare cloud using the duplicate generation technique with a two server based computing facility. Duplicate server serves as a second gallery to contain duplicate MHR that appear to the attacker as if it is the original MHR. When user uploading a file on original server, corresponding duplicate file will be stored on another server. In this method, the decoy files are called when an attacker is detected as accessing the system, in our proposed methodology the duplicate files are retrieved from the beginning to ensure better security. In proposed approach RSA algorithm is implement to encrypt the medical records.

Index Terms – Data sharing mechanism, attribute based encryption, secure outsourced computation, cloud computing, Electronic Medical Record.

I . INTRODUCTION

Cloud computing is definitely a promising model for business computing. It's describes important infrastructure to have an up-and coming type of service provision which includes the benefit of reducing expense by sharing computing and storage sources. Currently, Cloud Computing is really a huge technology that is exceeding all of the earlier technologies of computing of this competitive and demanding Information technology industry.

Cloud computing is consistently growing and there are many main cloud computing providers including Amazon, Google, Microsoft, Yahoo and many others who are offering solutions including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Storage-as-a- Service and Infrastructure-as-a-Service (IaaS). In addition, considering the possibility to substantially minimizing expenses by optimization and also maximizing operating as well as economic effectiveness, cloud computing is an excellent technology. Furthermore, cloud computing can tremendously boost its cooperation, speed, and also range, thus empowering a totally worldwide computing model on the internet infrastructure. On top of that, the cloud computing has advantages in delivering additional scalable, fault tolerant services.

Cloud computing handles resource management in a better way since the user no longer needs to be responsible for identifying resources for storage. If a user wants to store more data they request it from the cloud provider and once they are finished they can either release the storage by simply stopping the use of it, or move the data to a long-term lower-cost storage resource. This further allows the user to effectively use more dynamic resources because they no

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10513

longer need to concern themselves with storage and cost that accompany new and old resources.

The cloud services can be implemented in four deployment models:

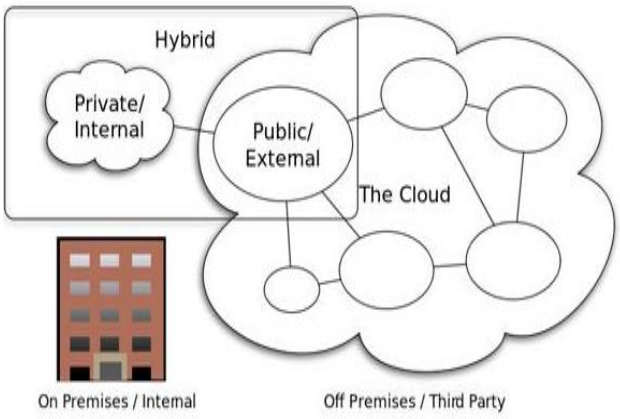

Fig.1 Types of Cloud Computing

• Public Cloud:

The cloud infrastructure is made available to the general public or large industry group and is owned by an organization selling cloud services.

• Private Cloud:

The cloud infrastructure is operated entirely for a single organization. It may be managed by the organization or a third party, and may exist on-premises or off-premises.

• Community Cloud:

The cloud infrastructure is shared by several organizations and supports a specific community. It may be managed by the organizations or a third party, and may exist on-premises or off-premises.

• Hybrid Cloud:

The cloud infrastructure is a composition of two or more clouds (private, community or public) shown in the fig.1 that are bound together by standardized or proprietary technology that enables portability of data and application.

II . RELATED STUDY

[1] Title: SecCloudSharing: Secure data sharing in public cloud using ciphertext-policy attribute-based proxy re-encryption with revocation - Tiwari, Deepnarayan, and G. R. Gangadharan. .Propose a cipertext-policy attribute-based proxy re-encryption scheme. In the proposed scheme, we design an efficient fine-grained revocation mechanism, which enables not only efficient attribute-level revocation but also efficient policy-level revocation to achieve backward secrecy and forward secrecy. The SecCloudSharing protocol develops a ciphertext-policy attribute-based proxy re-encryption (CP-AB-PRE) scheme to delegate a data owner controlled policy revocation process to a cloud server. The cloud server transforms a ciphertext associated with an access policy to another ciphertext under a new access policy without revealing the secret key of the data owner and the message. A KGC is a global central entity that initializes the system by publishing the public parameters. The KGC initializes the attribute revocation process by generating a random number corresponding to the revoked attribute on the request of the cloud server and sends it to the A-KACs. Each A-KAC updates the revoked attribute of the user by combining with the random number generated by the The KGC initializes the system functionality by publishing the public parameters and also controls the functionality of the cloud server and A-KACs. A cloud server is configured as a data storage server and a proxy mediator server to provide data services to the users

[2]Title:Online/offline unbounded multi-authority attribute-based encryption for data sharing in mobile cloud computing - Zhang, Y., Zheng, D., Li, Q., Li, J., & Li, H.Propose an online/offline MA-ABE scheme, which realizes both the online/offline secret key generation and the online/offline encryption while supporting a fully large attribute universe. In the offline phase, one global-identity authority and multiple attribute authorities doing the majority of the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 10, Issue 5, May 2021
DOI 10.17148/IJARCCE.2021.10513

work to issue attribute secret keys before knowing users' global identity and attributes. The data owner can perform most of the encryption computation tasks before knowing the actual message and access structure. Furthermore, the online phase can rapidly assemble the final decryption key and ciphertexts when related specifications become known. Particularly, global identity authority and attribute authorities need not to cooperate in the whole process. In the proposed system, the computation required for the generation of user global-identity secret keys, the generation of user attribute secret keys and the encryptions of messages are split into an offline phase and an online phase. In the offline phase, GA and AAs do the majority of the work to issue attribute secret keys before knowing users' global identity and attributes. The data owner can perform most of the encryption computation tasks before knowing the actual message and the access structure. Furthermore, the online phase can rapidly assemble the final decryption key and ciphertexts when related specifications become known. The technique of online/offline digital signature (OOS) is used by AAs to efficiently generate a signature on users' attribute secret keys. GA further generates users' global-identity secret keys, and hence, the decryption key for users only when the online signature is valid. Theoretical analysis and performance comparisons indicate that the proposed OO-MAABDS system is extremely suitable for resource constrained users in mobile cloud computing.

III . PROPOSED WORK

Proposed system adopt two different public cloud servers to achieve secure outsourced computation, such as outsourced key generation/encryption/re-encryption key generation/ decryption. Actually, one public cloud server (e.g., public cloud 2) is sufficient for outsourced decryption, but not enough for other operations, because all the secret will be exposed to the unique cloud server. The access control model consists of five entities: private key generator (PKG), public cloud 1, public cloud 2, data owners and data consumers. Proxy Re-encryption is used to re-encrypt the data before sending it to the data consumer. Here propose an efficient data sharing mechanism for Personal Data Sharing, which not only achieves data privacy, fine-grained access control and authority delegation simultaneously, but also optimizes the computation efficiency and is suitable for resource constrained servers.

Most of the data consumers are honest, while few of them are corrupt and will leakage their secret keys in the collusion. On the contrary, PKG and data owner are assumed to be fully trusted. Besides, public cloud 1 and public cloud 2 cannot collude with each other. The non-collusive assumption is reasonable, because the client can demand that two cloud servers cannot reveal users' information by contract. In proposed work, PR-ABE (Attribute Based Encryption with Proxy Re-encryption) technique implements to provide secure encryption of medical data. To improve the access control, here partial key sharing scheme will be implement. Using this, data owner can send partial secret key for the requested user. This approach overcomes the key guessing attack in data retrieval process. Proposed system will be implementing using PHP as front end and SQL is for back end process. This approach has modules like Framework Creation, Medical files uploading, Data Encryption, duplicate Storage, File access and alert system.

Input process has file storage and output was provide secure to medical files using two cloud. System architecture involves the high level structure of software system abstraction, by using decomposition and composition, with architectural style and quality attributes. A software architecture design must conform to the major functionality and performance requirements of the system, as well as satisfy the non-functional requirements such as reliability, scalability, portability, and availability.

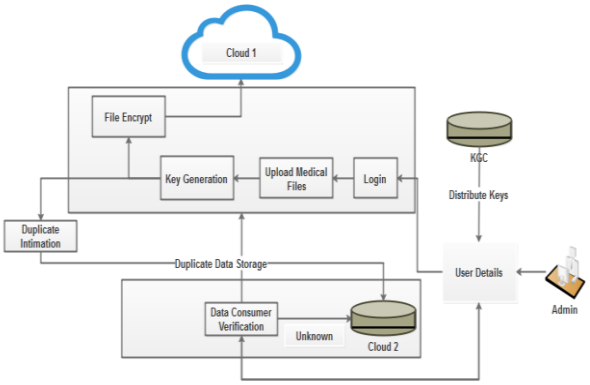

Fig.2 Proposed System Architecture

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10513

A .MEDICAL CLOUD FRAMEWORK

There is a significant volume of healthcare data generated daily. The data are important and vital for decision making and delivering the best care for patients. Cloud computing is a cost effective method that facilitates real-time data collection, data storage and exchange between healthcare organizations.

B.UPLOAD MEDICAL FILES

Cloud computing allows data collection and transfer to healthcare organizations. Data are collected from hospitals in the form of patient details, doctor details, medical reports and prescription details and then transmitted wirelessly to healthcare external processing units where patient's physician monitor and analyse those data.

C. DATA ENCRYPTION

In this module, in order to make health data's more secure use multi party in cloud computing system. The data's are then
encrypted with identity policy can be decrypted only if the identity policy is satisfied. Where the health data is encrypted using attributes and key policy.

D. DUPLICATE STORAGE

This technique can be considered as an illusion technique, as it makes the attacker believe that he/she has accessed the user's original medical files while in fact it is just a duplicate file.Fig.2 illustrates that both authorized and unauthorized users will be referred to the Duplicate Storage as the first step, while authorized legitimate users, as a second step, will be referred to the Original Cloud after being verified.

E. FILE ACCESS

This method of behavior-based security is commonly used in fraud detection application. In our proposed system, once the user accesses his/her account, by default the duplicate storage is shown.

F.ALERT INTIMATION

One of the key issues is to effectively detect any unauthorized data access in cloud. Besides, in the distributed case when such inconsistencies are successfully detected, to find which server the data access occurs. Finally provide SMS alert to data owner regarding the file access in duplicate storage. The intimation will be send to the form of mobile SMS.

IV .RESULTS AND DISCUSSIONS

In this section, a clear logic of the proposed strategy is described with practical proofs. The following fig.3 ,fig.5,fig.6 illustrates the clear view of login process by admin ,doctor ,patient respectively and the fig.4 shows the key generation of authorized persons.

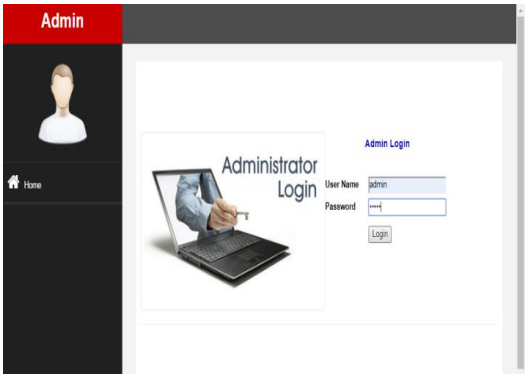

Fig.3 Login Process

Fig.4 Key Generati

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10513

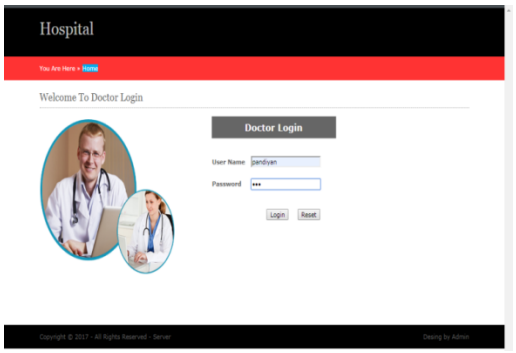

Fig 5.Login Process by Doctor

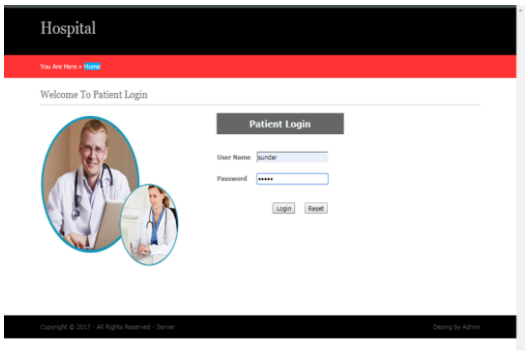

Fig 6.Login Process by Patient

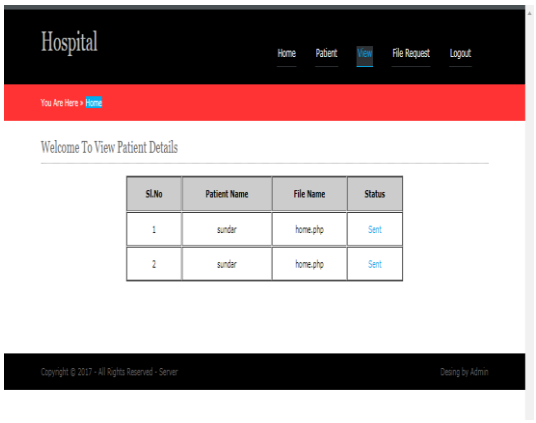

Fig.7 Uploading Medical Data

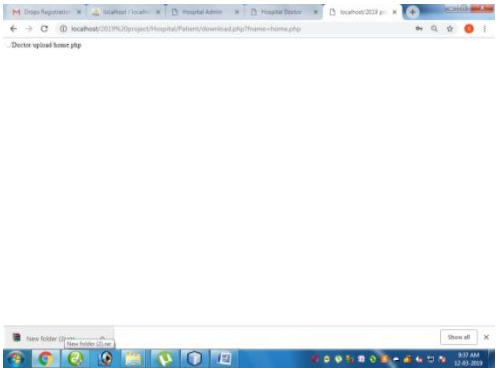

Fig.8 Retrieving Medical Data

The above fig.7 shows uploading medical data by doctor and the fig.8 shows the process of retrieving medical data by patient.

V.CONCLUSION AND FUTURE SCOPE

In this project proposed a new mechanism is proposed to protect the healthcare data in the cloud. This system has a double layer protection in which the EHRs are stored in the cloud. Encryption/ Decryption will be done in one layer and in the other layer, duplicate files will be created and stored. To this end, two cloud storages are generated for different purpose. The original medical files are kept secretly in the cloud and the duplicate cloud is used as duplicate file storage. Therefore, instead of retrieving the duplicate medical files only when any unauthorized access is discovered, the user, by default, accesses the duplicate files in cloud 2. The original server is only accessible by a user after verifying the authenticity of the user. Thus, the original multimedia data become more secure by setting the default value of the duplicate storage, while the original medical files are kept in a secure hidden cloud.

In future work, we can extend the framework to implement the system with various encryption algorithms and also other cryptographic approaches in real time images and medical videos. Implement Stenography based approach to hide the Medical Data inside the Medical Image or other Images to provide secure sharing.

REFERENCES

[1] D. F. Ferraiolo, R. S. Sandhu, S. I. Gavrila, D. R. Kuhn, and R. Chandramouli, “Proposed NIST standard for role-based access control,” ACM Transactions on Information and System Security,vol. 4, no. 3, pp. 224–274, 2001.

[2] E. Bertino, P. A. Bonatti, and E. Ferrari, “TRBAC: A temporal rolebased access control model,” ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 191–233, 2001.

[3] J. Joshi, E. Bertino, U. Latif, and A. Ghafoor, “A generalized temporal role-based access control model,” IEEE Transactions on Knowledge and Data Engineering, vol. 17, no. 1, pp. 4–23, 2005.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10513

[4] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca, "Geo-rbac: a spatially aware rbac," in 10th ACM Symposium on Access Control Models and Technologies, SACMAT 2005, Stockholm, Sweden, June 1-3,2005, pp. 29–37.

[5] S. G. Akl and P. D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," ACM Transactions on Computer Systems, vol. 1, no. 3, pp. 239–248, 1983.

[6] J. Alderman, N. Farley, and J. Crampton, "Tree-based cryptographic access control," in Computer Security - ESORICS 2017 - 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15, 2017, pp. 47–64.

[7] A.Castiglione, A. D. Santis, B. Masucci, F. Palmieri, A. Castiglione, and X. Huang, "Cryptographic hierarchical access control for dynamic structures," IEEE Transactions Information Forensics and Security, vol. 11, no. 10, pp. 2349–2364, 2016.

[8] Castiglione, A. D. Santis, and B. Masucci, "Key indistinguishability versus strong key indistinguishability for hierarchical key assignment schemes," IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 4, pp. 451–460, 2016.

[9] J. Alderman, J. Crampton, and N. Farley, "A framework for the cryptographic enforcement of information flow policies," in 22nd ACM on Symposium on Access Control Models and Technologies,SACMAT 2017, Indianapolis, IN, USA, June 21-23, 2017, pp. 143–154.

[10] A.Castiglione, A. D. Santis, B. Masucci, F. Palmieri, A. Castiglione,J. Li, and X. Huang, "Hierarchical and shared access control," IEEE Transactions Information Forensics and Security, vol. 11, no. 4, pp.850–865, 2016.