International Journal of Future Generation Communication and Networking
Vol. 13, No.2s, (2020), pp. 1678–1683

"Enabling authentication and Access Control-Based Data Sharing with personal Information Hiding for Secure Cloud Storage"

Supriya Raywade , Ayushi Dixit, Shruti Jain, Deepali Jain
Dept. of Computer Engg. NBN Pune, India

Abstract

Unfortunately, the e-healthcare cloud system has shown its potential to improve health care and the quality of life of the individual, privacy and security slows its general deployment and application There are a number of researches on the protective privacy of electric healthcare high (EHR). Information. However, all of these have two major limitations, they only work on the 'black or white' access regulator policy. Additionally, they suffer from mutual attack. In this paper, for the first time, we find that inferential attack-resistance

We first recommend a two-layer encryption scheme with an e-healthcare cloud company with a fine-grained access regulator. To ensure an effective and fine-grained controller over EHR data, we employ first-layer encryption, where we advance a specific threshold for each data feature in the EHR and independently encrypt it with high efficiency. To reserve an understanding of the role features and access strategies in first-layer encryption, we build second-layer encryption fully to the benefit of cloud server revenue. In order to protect the appearance of accessibility to, we will build an additional blind data retrieval protocol. We also show that we can easily extend our scheme to support search functionality. Finally, we perform extensive security analyzes and performance assessments.

Keyword:*Advanced Encryption Standards, Personal Data Extraction, Anonymous Authentication, Rotating Group Signature, Elliptic Curve Cryptography, Smart Health Applications.*

Introduction:

Cloud computing provides a user-oriented way to store and compute data. We can use cloud computing to manage data privacy and privacy in the cloud. We need to pay for usage and it requires an internet connection to work. Lack of Data Security Cloud provides an effective way to store data in encrypted form in the cloud. Its purpose is to prevent misuse of patient's documents and to search for the data they need to meet the patient's need. Extremely secure and protective concerns are the form of problems that stand in the way of widespread adoption of the framework. IT application plays an important role in health and patient care. Cloud users upload personal or confidential data to the cloud's data center. Many users cannot handle dynamic changes in previous electronic health record systems. Our main purpose is to protect data from unauthorized access. File uploading operation in the previous system was not carried out safely and the lack of security increased the misuse of data. Cloud file strength has some complex issues, and when the cloud file is aggregated, search information should not be uncovered by others and scrutinizing the entire shared file can detect hidden evidence. In some religious cloud storage classifications, such as Electronic Health Records (EHRs) system, cloud file capacity Materials There will be Ligi. In cloud storage facilities, users can store their data a little bit in the cloud and separate data sharing with others. Remote data honest auditing is proposed to guarantee the integrity of data deposited in the cloud. In selected general cloud storage systems such as the Electronic Health Accounts (EHRs) classification. In this project, a sanitizer is used for cleaning or mining data blocks that correspond to the file's sensitive information and makes the signatures of these data blocks valid for a clean file In remote data integrity auditing schemes, the data owner must first create the required data blocks before uploading them to the cloud. These signatures can be used to prove that the cloud really has these data blocks in the integrity auditing phase.

Related work:

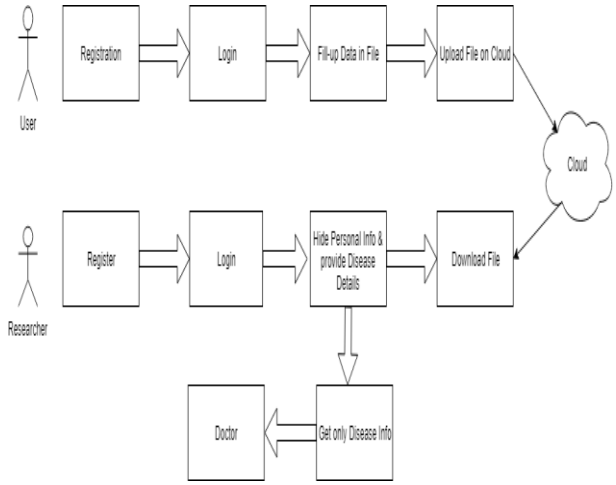
To verify the truthfulness of the facts placed in the cloud, many discrete data examining structures are honestly predictable.

ISSN: 2233-7857 IJFGCN

In this project, we are developing 3 modules:
Patient: -
In this module, a user is registered and followed by OTP authentication and so on
Completing the OTP verification involves login. Fill out the user form. In this project, we
Developing a model for the health care system and we can integrate this module with other systems. Here we are considering the user that a patient uploads a disease report and the patient receives a prescription and advises on the disease.
• Researcher:
The investigator is nothing more than an Admin (Owner) who will hide the patients' personal information and send this disease report to the appropriate doctor (doctor) for their diagnostic findings.
• Doctor:
In this module the physician is a third-party user, looking only at information related to the disease by hiding someone
Details and submissions of a doctor related to the patient's disease report and also provides advice related to the disease.

System modules:
Our system mainly consists of three modules one of which is Doctor and the other is patient and research.

System Building:
In the process, we design and develop a system to protect data and confidential information. Our primary purpose of the System is to protect information from unauthorized access. Writing an entire shared file may see private encryption information, but it will prevent the shared file from being used by others. Signatures are used to verify the integrity of the purification file in the reliability audit section.



Mathematical Model:

- Input: input as a patient report. A report in nothing but text, doc file.
- S = {I, F, O}
- Where, S = Proposed system.
- I = Input of system (text file).
- F = Functions of the system.

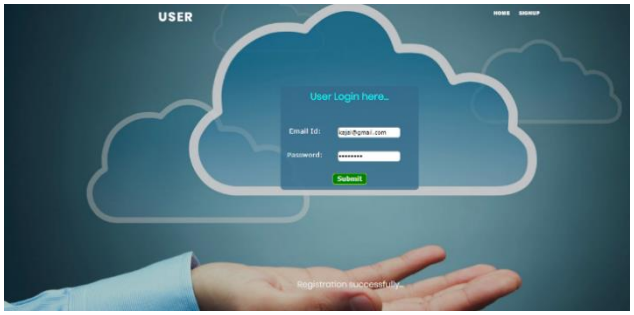
ISSN: 2233-7857 IJFGCN

- O = Output of the system (Final secure data send).
- F = {f1, f2, f3}
- f1= encryption
- f2=decryption.
- f3=digital key generation
- The proposed system uses AES algorithm for encryption and decryption purpose for secure file transfer from one layer to another layer.
- Output: Complete file sends in a group of people securely.

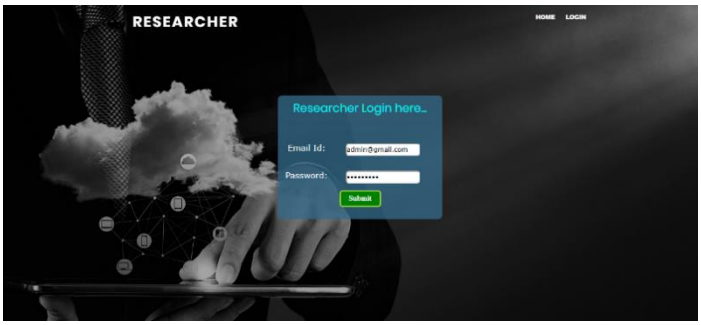
Conclusion:

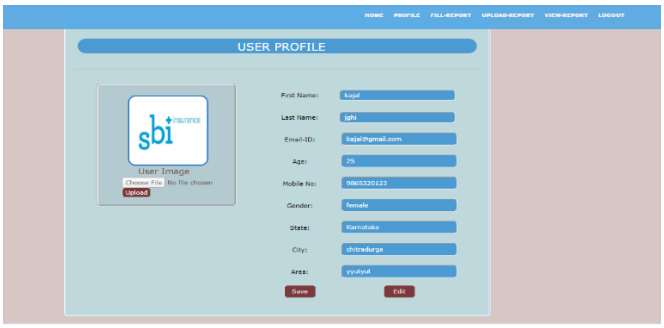
In the project, we realized the moment that privacy-protection keyword indexes were allowed in the search process for the EHD Reasoning Storage space that could support automatic delete. The security and security analysis here shows that our scheme provides reasonable overhead computation in cloud storage applications compared to traditional systems. This is the first security plan that can be retrieved with specific professionals for the EHD Reasoning Record Storage space, which protects the encryption function and confidentiality of the moment. The solution can ensure the comfort of EHD and its ability to withstand keyword attacks. In our scheme, the file stored in the cloud can be shared and used by others on the condition that the sensitive information of the file is protected. In addition, remote data integrity auditing can still be performed effectively. Safety proof and experimental analysis proves that the proposed scheme achieves the desired safety and efficiency. In this paper, the user uploads a file with a signature and sends it to the sanitizer. The sanitizer now encrypts this received file and uploads it to the cloud server. If a third party auditor wants to access this file, he must ask the user for permission to proceed. Also, he has to provide the user-generated signature when uploading the file.

Output/screenshots:



ISSN: 2233-7857 IJFGCN





Reference:

[1] K. Ren, C. Wang, and Q. Wang, “Security challenges for the public cloud,” *IEEE Internet Comput.*, vol. 16, no. 1, pp. 69–73, Jan. 2012.
[2] G. Ateniese *et al.*, “Provable data possession at untrusted stores,” in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 598–609.
[3] A. Juels and B. S. Kaliski, Jr., “Pors: Proofs of retrievability for large files,” in *Proc. 14th ACM Conf. Comput. Commun. Secur.*, 2007, pp. 584–597.
[4] H. Shacham and B. Waters, “Compact proofs of retrievability,” *J. Cryptol.*, vol. 26, no. 3, pp. 442–483, Jul. 2013.
[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362–375, Feb. 2013.
[6] S. G. Worku, C. Xu, J. Zhao, and X. He, “Secure and efficient privacy-preserving public auditing scheme for cloud storage," *Comput. Electr. Eng.*, vol. 40, no. 5, pp. 1703–1713, 2014.
[7] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, “Symmetrickey based proofs of retrievability supporting public verification,” in *Computer Security—ESORICS*. Cham, Switzerland: Springer, 2015, pp. 203–223.
[8] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, “Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium,” *J. Netw. Comput. Appl.*, vol. 82, pp. 56–64, Mar. 2017.
[9] J. Sun and Y. Fang, “Cross-domain data sharing in distributed electronic health record systems,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 6, pp. 754–764, Jun. 2010.
[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.

ISSN: 2233-7857 IJFGCN

[11] C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, 2009, pp. 213–222.
[12] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, May 2011.
[13] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling cloud storage auditing with key-exposure resistance," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1167–1179, Jun. 2015.
[14] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1362–1375, Jun. 2016.
[15] J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1931–1940, Aug. 2017.
[16] J. Yu, R. Hao, H. Xia, H. Zhang, X. Cheng, and F. Kong, "Intrusionresilient identity-based signatures: Concrete scheme in the standard model and generic construction," *Inf. Sci.*, vols. 442–443, pp. 158–172, May 2018.
[17] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in *Proc. IEEE 5th Int. Conf. Cloud Comput. (CLOUD)*, Jun. 2012, pp. 295–302.
[18] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," *J. Syst. Softw.*, vol. 113, pp. 130–139, Mar. 2016.
[19] A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, "NPP: A new privacy-aware public auditing scheme for cloud data sharing with group users," *IEEE Trans. Big Data*, to be published, doi: 10.1109/TBDATA.2017.2701347.
[20] B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared data with efficient user revocation in the cloud," *IEEE Trans. Serv. Comput.*,n vol. 8, no. 1, pp. 92–106, Jan./Feb. 2015.
[21] Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, "Efficient integrity auditing for shared data in the cloud with secure user revocation," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, Aug. 2015, pp. 434–44

ISSN: 2233-7857 IJFGCN

ISSN: 2233-7857 IJFGCN