Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# A Cloud Based System for Patient Health Records Using Symmetric Encryption

**K.S.Sureh, Mrs. SaritaChowdary, T. Balachary**
Dept of CSE, MLRIT,
Dundigal, Hyderabad, India

***Abstract- This paper presents implementation of cloud based system for patient health records as it is a sharing patient heath record in third party system such as cloud so security is important concern in this paper we providing security using symmetric Encryption. This system is helpful to hospitals as well as patients to share their health records in a third party server so they can access their records from anywhere as it is a shared system security is important we encrypting the patient records using symmetric Encryption also known as private-key cryptography, and is called so because the key used to encrypt and decrypt the message must remain secure, because anyone with access to it can decrypt the data. Using this method, a sender encrypts the data with one key, sends the data (cipher text) and then the receiver uses the key to decrypt the data.***

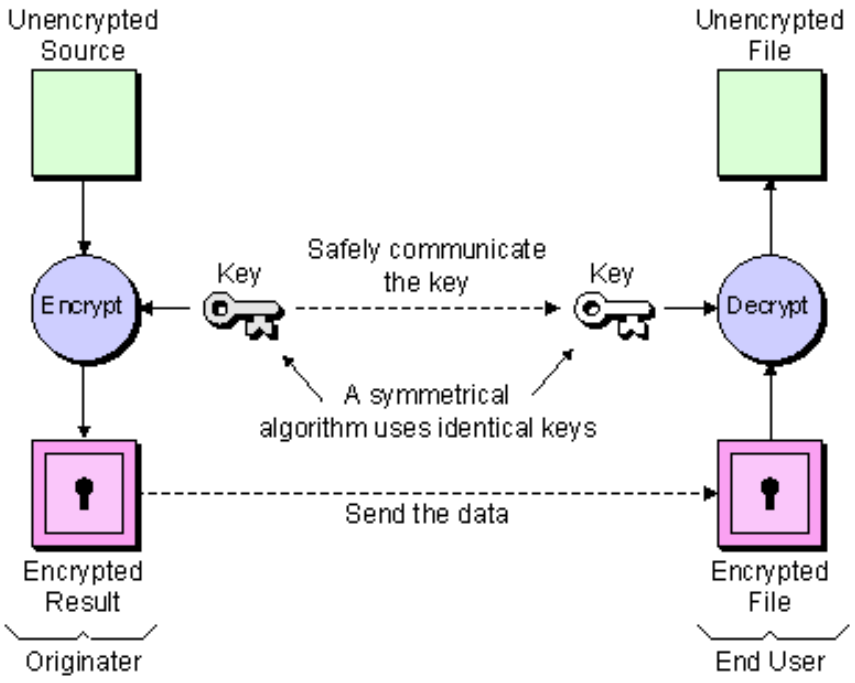
***Keywords – Patient Health Records, Cloud based system, Symmetric Encryption, Cipher text.***

## I. INTRODUCTION

In Recent years sharing of patient health records emerged as a central model to exchange information. Because it is difficult to patients to maintain server to store their health records centrally they approach the third party services to share their health records centrally so as it is a third party system we are providing security using symmetric encryption also known as private-key cryptography, and is called so because the key used to encrypt and decrypt the message must remain secure, because anyone with access to it can decrypt the data. Using this method, a sender encrypts the data with one key, sends the data (cipher text) and then the receiver uses the key to decrypt the data.

## II. RELATED WORK

This paper is mostly related to work in cryptographically enforced access control for outsourced data and attribute based encryption. To improve upon the scalability of the above solutions, private-key cryptography, a key is used to encrypt and decrypt the message must remain secure, because anyone with access to it can decrypt the data. Using this method, a sender encrypts the data with one key, sends the data (cipher text) and then the receiver uses the key to decrypt the data.

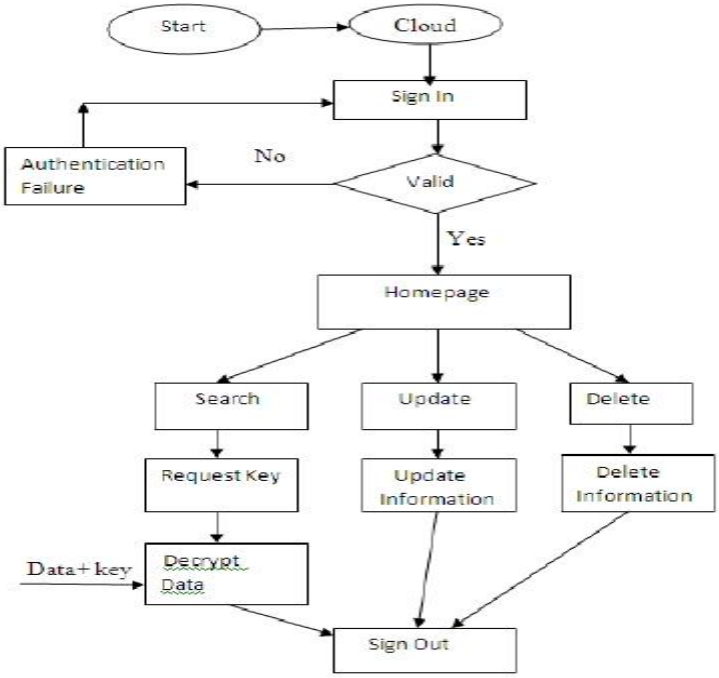


## III. PROPOSED SYSTEM

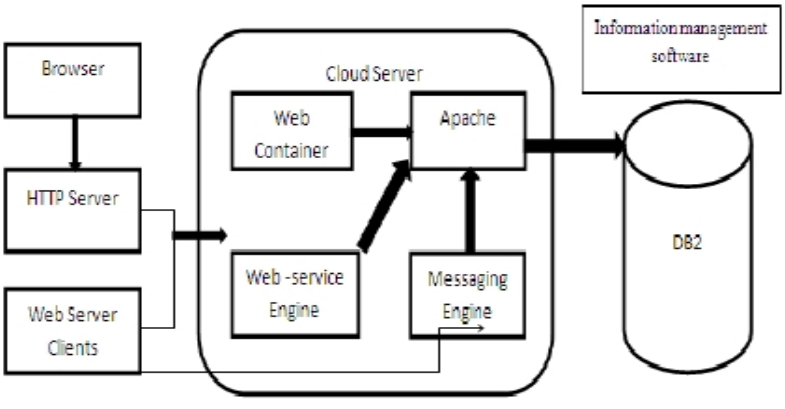
In this system number of PHR owners and users are involved. The owners refer to patients whose medical related data are being controlled and the users are those who try to access them. There exists a central server where owners place their sensitive medical data, and attempted by users to gain access. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data. This leads to the need of Symmetric Encryption. An important requirement of efficient PHR access is to enable "patient-centric" sharing. This means that the patient should have the ultimate control over their personal health record. They determine which users shall have access to their medical record. User controlled read/write access and the main goal of our system is to provide secure patient-centric PHR access and efficient key management at the same time.

## IV SYSTEMDIAGRAM




In this system a user can login with third Party server such as cloud then the system checks for authentication if he is a valid user he connects to the his PHR and then he can update, delete or search for his records and he has decrypt his data by using key.

## IV SYSTEM ARCHITECTURE




This architecture will tells how the patient health record syatem works here between the database and the web there is a third party system which will connets the application server with the database.

## V USERS of PATIENT HEALTH RECORDS

The system is designed to manage Patient Health Records (PHR) with different user access environment. The data values are maintained under a third party cloud provider system. The data privacy and security is assured by the system. The privacy attributes are selected by the patients. The data can be accessed by different parties. The key values are maintained and distributed to the authorities. The system is enhanced to support Symmetric Encryption model. The user identity based access mechanism is also provided in the system. The system is divided into six major modules.

They are data owner, cloud provider, key management, security process and client.

Data Owner - The data owner module is designed to maintain the patient details. The used to select sensitive attributes. Patient Health Records (PHR) is maintained with different attribute collections. Data owner assigns access permissions to various authorities.

Cloud Provider -The cloud provider module is used to store the PHR values. The PHR values are stored in databases. Data owner uploads the encrypted PHR to the cloud providers. User access information's are also maintained under the cloud provider. Key Management -The key management module is designed to manage key values for different authorities. Key values are uploaded by the data owners. Key management process includes key insert and key revocation tasks. Dynamic policy based key management scheme is used in the system. Security Process - The security process handles the Attribute Based Encryption operations. Different encryption tasks are carried out for each authority. Attribute groups are used to allow role based access. Data Decryption is performed under the user environment. Client -The client module is used to access the patients. Personal and professional access models are used in the system. Access category is used to provide different attributes. The client access log maintains the user request information for auditing process.

## VI CONCLUSION

The personal health record system needs security against attackers and hackers. Scalable and Secure sharing includes basic securities to protect the information from unauthorized access and loss. This paper proposed the new approach for existing PHR system for providing more security using symmetric encryption which plays an important role because these are unique and not easily hackable. We are reducing key management problem and also we enhance privacy guarantee.

## 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," in SecureComm¨10, Sept.2010, pp. 89-106.
2. H. L¨ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI ¨10, 2010, pp. 220-229.
3. M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *CCS '09*, 2009, pp.121-130.
4. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASSIACCS¨10, 2010.
5. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM¨10, 2010.
6. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in ACM CCS, ser. CCS ¨08, 2008, pp.417-426.
7. J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. PrePrints, 2010.
8. S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.
9. M. Vijayapriya Dr. A. Malathi , M. Phil. Research scholar PG & Research Department of Computer Science" Multi Authority Attribute Based Encryption for Personal Health Record". International Journal of Computer Trends and Technology (IJCTT) - volume 4 Issue 8- August 2013
10. Priyanka Korde, Vijay Panwar, Sneha Kalse "Securing Personal Health Records in Cloud using Attribute Based Encryption" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 - 8958, Volume-2, Issue-4, April 2013