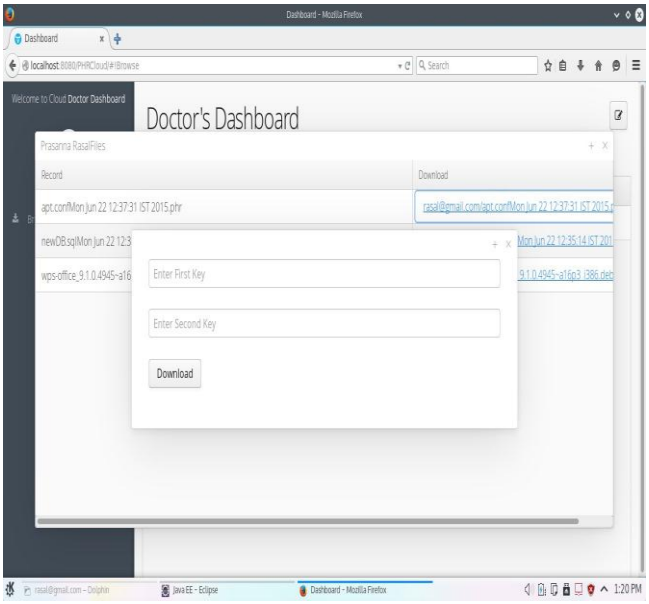


**Figure 14:** Doctor accessing patient's record

## 7. Comparison Of Developed System And Existing System

There have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. The existing systems usually assume the use of a single trusted authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem since the TA can access all the encrypted files, opening the door for potential privacy exposure. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys[1].

The developed system assures the patients' control over access to their own PHRs; and it provides promising method to encrypt the PHRs before outsourcing. The system ensures 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. In order to protect the personal health data stored on a semi-trusted server, system enabled a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users

The system focuses on the multiple data owner scenario, and divides the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. It bridges the above gaps by proposing a unified security framework for patient-centric sharing of PHRs in a multi-domain, multi-authority PHR system with many users. The framework captures application level requirements of both public and personal use of a patient's PHRs, and distributes users' trust to multiple authorities that better reflects reality.

## 8. Conclusion

1) The project discusses platform for sharing of personal health records in the secure and scalable manner by using Cloud computing. To enhance the fully patient centric concept and its privacy each PHR file is encrypted which also allows fine grained data access.
2) The user doesn't need to locally store their data. So there is burden of managing data at local site. User can rely on cloud service provider for the storage of their data.
3) The framework efficiently handles the prime challenge of key management brought by introduction of multiple PHR users and owners.
4) Homomorphic Encryption is used for security purpose and for key management.
5) The key idea is to divide the system into multiple security domains (namely public domains and personal domains) according to the different user's data access requirements.

## References

[1] Ming Li, Member, IEEE, Shucheng Yu, Scalable and secure sharing of personal health record in cloud computing using attribute based encryption [1], IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013
[2] L. Ibraimi, M. Asim, and M. Petkovic, Secure Management of Personal Health Records by Applying Attribute-Based Encryption, technical report, Univ. of Twente, 2009.
[3] 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.
[4] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Intl Conf. Distributed Computing Systems (ICDCS 11), June 2011.
[5] A. Boldyreva, V. Goyal, and V. Kumar, Identity-Based Encryption with Efficient Revocation[5], Proc. 15th ACM Conf. Computer and Comm. Security (CCS), pp. 417-426, 2008.


Licensed Under Creative Commons Attribution CC BY