having a minimum number of attributes only can decrypt the data.

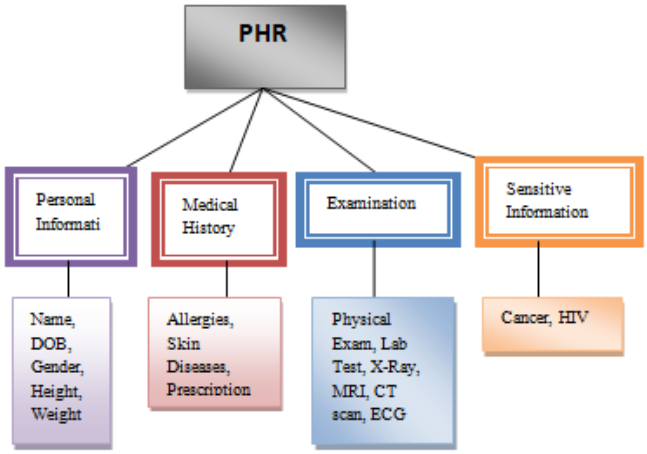


**Figure 3:** Attribute Hierarchy of health records

Public key encryption was the most traditional method applied to the PHR for the security of the data. But it made the high key-management problems and also this method was very less scalable. Cipher text Policy Attribute based Encryption (CP-ABE): technique is used to keep encrypted data confidential The key-idea of the CP-ABE is: the user secret key is associated with a set of attributes and each cipher text will embedded with an access structure. The user can decrypt the message only if the user's attribute satisfied with the access structure of the cipher text [22].

Key-Policy Attribute-based Encryption (KP-ABE) is a crypto system for fine grained sharing of encrypted data. In KP-ABE cipher text are label with attributes and private key are associated with access structures that control which cipher text a user is able to decrypt. It is used for securing sensitive information stored by third parties on the internet. The KP-ABE is useful for providing the fine-grained access control to the data system where it can efficiently specify that which part of data system can be accessed by which user and what are the operations they can execute over there. Multi-Authority Attribute-Based Encryption (MA-ABE) is an advanced attribute based encryption in which it concerned with multiple attribute authority for handling the different set of users from different domains. [23] In the PHR system the users will be from different domain like the doctors from health care organizations, the friends and family from personal relations and other users from insurance domain too. Thus the MA-ABE scheme will highly reduce the key-management issues and it will provide fine-grained access control to the system.

### 4.2 Proposed PHR System

Traditional clinical settings concerned with paper-based medical records and prescriptions have also advanced to the Personal Health Records (PHRs) and the Electronic Health Records (EHRs).From the clinical point of view, it is important to access the up-to-date integrated patient health information. E-health cloud can be considered as a platform that, besides storing huge volumes of the health data, also serves as a structured management of the health data across multiple healthcare providers. In the existing system the data owner is uploading the data to the cloud server, after encrypting the data according to the access control policy [29] defined with the set of attributes. This encrypted data can be decrypted by the user only if the attributes of that user satisfies the access control policy. The problem addressed here is the confidentiality of PHRs. Patients records contains sensitive information such as details of a patient's disease, drug usage, sexual preferences, etc. Inappropriate disclosure of a record can change patient's life, and there may be no way to repair such harm financially or technically. Therefore, it needs protection for patient's health records when they are uploaded and stored in commercial Web-based systems. Consider following scenario where a patient, has some sensitive personal health records which she wants to store securely in a Web-based PHR, and share them with other users who belong to two different security domains: (1) professional domain (PD) - a healthcare provider group such as doctors, nurses, or (2) social domain (SD) - her family, friends, or patients.

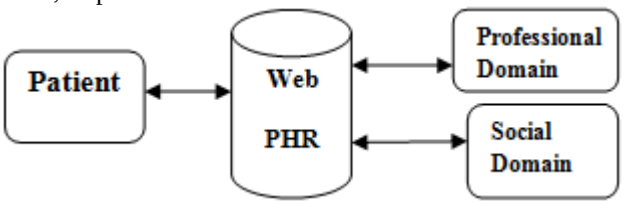


**Figure 4:** Proposed PHR System Architecture

The scenario gives the idea about the need for a system which fulfills the following security requirements:

a. Protect health records from network attacker. So, data is to be encrypted before it is sent to the web PHR.
b. Health records protected from third parties who store PHRs. The third party manages web PHRs which are not accessible to the plain data.
c. The access policy concerned with the encrypted data, such that only those users having a secret key associated with set of attributes which satisfies the policy might be capable of decrypting it.
d. Users from the professional domain and users from the social domain both need to be properly authenticated and authorized to access the data.

Solution of the problem in the existing system is overcome by the Personal health record is maintain in the centralize server to maintain patient's personal and diagnosis information. A high degree of patient's privacy is maintained simultaneously with the help of multi-authority ABE. Proposed system enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation a under emergency scenarios. Analytical and experimental results are presented which show the security, scalability and efficiency and privacy of our proposed scheme. Use case diagram of proposed system is shown in the fig:

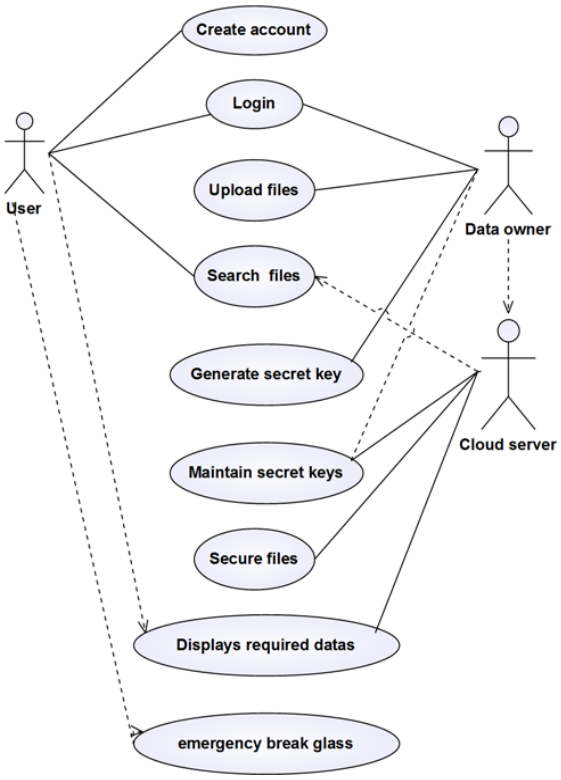


**Figure 5:** Use Case flow of PHR System

To achieve fine-grained and scalable data access control for PHRs, we adopted attribute based encryption (ABE) techniques to encrypt each patient's health record file We focused on multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users with the help of MA-ABE technique. In this system, we fulfill the mentioned gaps by proposing a security framework model for patient-centric sharing of PHRs in a multi-domain, multi-authority PHR system with many users.

## 5. Conclusion

In this paper, we have proposed privacy preserving and secure sharing patient centric framework for maintaining personal health records in cloud computing. With the help of partially used cloud servers, patients shall full control through encrypting their PHR files to allow fine grained access. This framework concerned with the unique challenges by multiple PHR owners and users, in that we greatly reduce the time, security and complexity of key management. We used ABE technique to encrypt the PHR data, so that patients can allow access as the private users, but not accessible by the public users.

## 6. Acknowledgement

My sincere thanks to Dr. Arati M. Dixit madam for her helpful opinion and suggestion for the paper.

## References

[1] Connecting for Health. The personal health working group final report, 2003 July 1.
[2] AbuKhousa, E.Najati, H.A. UAE-IHC Steps towards Integrated E-Health Environment in UAE. In Proceedings of the 4th e-Health and Environment Conference in the Middle East, Dubai, UAE, 30 January 2012–2 February 2012.
[3] Lohr, H. Sadeghi, A. Winandy, M. Securing the E-Health Cloud. In "Proceedings of the 1st ACM International Health Informatics Symposium (IHI 2010)", Arlington, VA, USA, 11–12 November 2010; pp. 220–229.
[4] Commonwealth Secretariat. Progress report. Available online: http://www.thecommonwealth.org/ files/189921/File Name/HealthProgressReports-E-Health.pdf (accessed on 28 June 2012).
[5] Momtahan, L.Lloyd, S. Simpson, A. Switched Lightpaths for E-Health Applications: Issues and Challenges. In Proceedings of the Twentieth IEEE International Symposium Computer-Based Medical Systems (CBMS'07), Maribor, Slovenia, 20–22 June 2007; pp. 459–464.
[6] Agrawal, D. Abbadi, A. Antony, S.Das, S. Data Management Challenges in Cloud Computing Infrastructures. In Proceedings of the 6th International Workshop on Databases in Networked Information Systems (DNIS 2010), Aizu-Wakamatsu, Japan, 29–31 March 2010.
[7] Hasan, J. Effective telemedicine project in Bangladesh: Special focus on diabetes health care delivery in a tertiary care in Bangladesh. Telemat. Inform. **2012**, 29, 211–218.
[8] Rayport, J.F. Heyward, A. Envisioning the Cloud. The Next Computing Paradigm. A Market space Next Point of View. Available online: http://marketspacenext.com/inthemedia/ envisioning-the-cloud/ (accessed on 28 June 2012).
[9] Introduction to Cloud Computing Architecture. Sun Microsystems, Santa Clara, CA, USA, 2009.
[10] Varia, J. Cloud Architectures. Available online: http://aws.amazon.com/articles/ 1632 encoding UTF8 & jiveRedirect 1 (accessed on 28 June 2012).
[11] Hosseini, A.; Sommerville, I.; Sriram, I. Research Challenges for Enterprise Cloud Computing. Available online: http://arxiv.org/abs/1001.3257 (accessed on 28 June 2012).
[12] Mei, L.; Chan, W.K.; Tse, T.H. A Tale of Clouds: Paradigm Comparisons and Some Thoughts on Research Issues. In Proceedings of the Asia-Pacific Services Computing Conference (APSCC'08), Yilan, Taiwan, 9–12 December 2008; pp. 464–469.
[13] Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.Rabkin, A.; Stoica, I. Zaharia, M. Above the Clouds: A Berkeley View of Cloud Computing. Available online: http://inst.cs.berkeley.edu/~cs10/fa10/lec/20/2010-11-10-CS10-L20-AF-Cloud-Computing.pdf (accessed on 29 June).
[14] Sriram, I.; Khajeh-Hosseini, A. Research Agenda in Cloud Technologies. In Proceedings of the 1st ACM Symposium on Cloud Computing, SOCC 2010, Indianapolis, IN, USA, 10–11 June 2010.
[15] Youseff, L.; Butrico, M.; da Silva, D. Toward a Unified Ontology of Cloud Computing. In Proceedings of the

Grid Computing Environments Workshop (GCE'08). Austin, TX, USA, 12–16 November 2008; pp. 1–10.
[16] Leavitt, N. Is cloud computing really ready for prime time? Computer 2009, 42, 15–20.
[17] Al-Jaroodi, J.Mohamed, N. Service-oriented middleware: A survey. J. Netw. Comput. Appl. 2012, 35, 211–220.
[18] Nguyen, D.K..Lelli, F. Papazoglou, M.P. van den Heuvel, W.-J. Blueprinting Approach in Support of Cloud Computing. Future Internet 2012, 4, 322–346.
[19] Kelly, E.P.; Unsal, F. Health information privacy and e-healthcare. Int. J. Healthc. Technol. Manag. 2002, 4, 41–52.
[20] Cote, R.A. Architecture of SNOMED Its Contribution to Medical Language Processing. In Proceedings of the Annual Symposium on Computer Applied Medical Care, Washington, DC, USA, 25–26 October 1986; pp. 74–80.
[21] A. Sahai and B. Waters, "Fuzzy Identity-Based encryption," in LectureNotes in Computer Science, vol. 3494, 2005, pp. 457–473
[22] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM International Journal of Communication and Computer Technologies Volume 01 – No.72 Is Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.
[23] S. Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure," Proc. ACM Cloud Computing Security Workshop (CCSW'10), pp. 47-52, 2010.
[24] X. Liang, R. Lu, X. Lin, and X. Shen. "Patient self-controllable access policy on phi in healthcare systems", AHIC 2010, Kitchener, Ontario, Canada, pp.1–5
[25] S. Yu, C. Wang, K. Ren and W. Lou, (2010), "Achieving secure, scalable, And fine-grained data access control in cloud computing", INFOCOM, 2010 Proceedings IEEE, San Diego, CA, USA, pp.1–9.
[26] 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,‖ Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm '10), pp. 89-106, Sept. 2010.
[27] e-Health Cloud: Opportunities and Challenges by Eman AbuKhousa, Nader Mohamed and Jameela Al-Jaroodi Future Internet **2012**, 4, 621-645; doi:10.3390/fi4030621
[28] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, January 2013, pp. 131-143.
[29] M. Chase and S.S. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 121-130, 2009.
[30] L. Ibraimi, M. Asim, and M. Petkovic, "Secure Management of Personal Health Records by Applying Attribute-Based Encryption," technical report, Univ. of Twente, 2009.
[31] J. Sun, X. Zhu, C. Zhang, andY. Fang, "HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare," in Proc. IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2011, pp. 373–382.