# Scalable and Secure Sharing of Personal Health Records in Web Using Attribute-Based Encryption

[1]Reshma S. Sapakal,[2]Pankaj R. Chandre
[1] Student ME(Computer),[2]Prof. ME(Computer)
[1]Department of Computer Engineering
[1]Flora Institute of Technology, Khopi, Pune, India

***Abstract*– Traditional paper-based health records may result in wastage of paper. Now days internet has grown very rapidly. There are more advances in medical and information technology. So using benefits of both traditional health record can be transfer to electronics health record (EHR) and allow medical people to do their activities in numerous ways. Existing centralized Personal Health Record (PHR) systems has efficiency and security problems. To overcome this problem Personal Health Records are outsourced to third party semi trusted data servers over the web to provide distributed environment. However there is major risk of privacy of personal health information exposed to third party server and to unauthorized users. To assure privacy and security one efficient way is to encrypt PHR before outsourcing it to the internet. There are other issues like scalable key management, efficient user revocation and fine grained access. To achieve scalable and fine-grained access Attribute-Based Encryption is used to encrypt PHR. PHR system is consider as multiple owner, multiple user system. For reducing key management complexity, users are divide into multiple user domains like public and personal. While providing high degree of privacy proposed system shows security, scalability and efficiency from its result analysis.**

***IndexTerms*– Electronic Health Record, Personal Health Record, Attribute Based Encryption, Third party Servers, Privacy and Security**

## I. INTRODUCTION

In field of communication, communication is fastest growing area. Using advantage of it allow user to achieve “any time, anything and anywhere” access to required medical information. The traditional paper-based health records generate an extensive paper waste. So there is great interest of moving from paper-based health records to electronic health records (EHRs). With the growth of information and medical technology, health records are transformed from traditional paper records to electronic medical records which are widely used. It leads to the development of a new exchange system of medical information which was named PHRs[1]. PHRs is a new patient-centric health information system. For storing information conveniently and efficiently, medical information is outsourced the third-party semi trusted servers over the internet. So PHR systems are widely deployed and hence improve people’s daily life compared with traditional paper-based systems for its interesting advantages like high efficiency, better accuracy, and broader availability.

According to a recent report [4], there are more than 77% patients and 70% physicians who want to get involved with PHR systems. The Health Insurance Portability and Accountability Act (HIPAA) has been established for years to regulate PHR related operations [5]. In patients’ sensitive Personal Health Information (PHI) contains highly-private information like social security number, address, and date of birth, all of which can be easily used by attackers for malpractice [6], [7]. Several medical records theft and stolen incidents [8] have been reported recently where attackers steal and publish patient health information to a third party over the Internet. According to a recent survey [9], researchers estimate the economic impact of medical identity theft in the United States at 41.3 billion dollars per annum. More than 78% of participants in [10] worry about the leakage and misuse of their personal information and health condition, so that they fear to use of PHR systems.

For providing privacy and security to the health information, information is encrypted before outsourcing it over internet. Basically, the PHR owner i.e. patient herself should decide how to encrypt her PHR and to allow which set of users will access the information. A PHR will be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary [11].

Traditional public key encryption PKE[1] is not useful here as it has disadvantages like key management complexity, fine-grained access, and scalability. To overcome these problems Attribute Based Encryption (ABE)[2] is good solution. Chase and Chow[3] proposed a MA-ABE solution referred to as CC MA-ABE program. Generally, PHR service allows a user to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. As PHR is multi owner system that encrypts their PHR according to their own way. Here each user obtains keys from every owner whose PHR she wants to read would limit the accessibility since patients are not always online. An alternative is to use a central authority (CA) to do the key management on behalf of all PHR owners.

## II. Related Work

In PHR system data is outsourced on data server over internet. For privacy and security of information, encryption techniques are. Cryptography is used to provide privileges. For smoother access privileges, the traditional public key encryption (PKE) [12], [13] may costs excess key management overhead and scalability issue. For more scalable PKE, ABE can be used. In Goyal et al.s seminar papers on ABE [14], data encryption is done using set of attributes so that multiple users that have proper keys can decrypt. Attribute-based encryption (ABE) is a new technique that uses the concept of public-key cryptography. ABE defines the identity as set of attributes not limited to single atomic key as in PKE. There are different versions of ABE as MA-ABE (Multi-authority ABE), CP-ABE (Cipher-text Policy ABE) and KP-ABE (key-policy ABE). The traditional public key encryption (PKE) [15], [16] can be used to achieve fine-grained access. KP-ABE algorithm used for access control in PHRs [17]. But KP-ABE lacks the efficiency and security of the scheme. Because of the data owner is also the TA (rusted Authority) and the program didn't changes the random parameter of ABE it has efficiency problem. To solve the efficiency problem of KP-ABE, a MA-ABE access control strategy is used. However, there are several common drawbacks of the above works. First, they 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.

.

## III. Implementation Details

Proposed PHR system has multiple owners and multiple users. Owner is nothing but patient. Owner has full control over his PHR data. PHR system stores data on central server that stores all the owners' information. Users are divided into multiple security domains as personal and professional. Personal domain contains users like close friends and relatives. Professional domain also called as public domain contains users like doctors, pharmacist, researchers, insurance company etc. The PHR documents accessed by users through the server for read or update to someone's PHR. The main aim is to provide efficient, secure data access controlled by patient and efficient key management simultaneously.

The framework of PHR is as shown in Figure1 [18].

For supporting interoperability, the PHR support identical encoding, communications and messaging standards. As the medical professionals also called public users use PHRs, proposed system develop abstract representations and explanations of the encoded data. In addition PHRs contains authentication vexing problem. A stand-alone PHR is safe until it is under owner's control. But if its data are unencrypted and the device is lost then what happen? The PHR interacts with other health care system, so authentication is very necessary.

As shown in the Fig 1. , step ((3)) shows upload of ABE-encrypted PHR files to the server by user. Set of data attributes is selected for data access for users in the PSD. The User retrieves PHR data from the server and they can decrypt it only if they have proper attribute based decryption keys ((5)). The user can write to PHRM, if they have proper write keys ((4)).

### *A. User Revocation*

Revocation of users is done for following situations: 1) For public domain users revocation of one or more role attributes; ; 2) revoking public domain user is as same as to revoking all of that user's attributes. AA does all these operations for the user belongs to it. ((8)). 3)Revoking personal domain user's access privileges; 4)revoking personal domain user. PHR owner's client application initiates this.

### *B. Policy Updates*

Policy can be made by owner of information by using set of attributes. Policy can be modified by a PHR owner by updating the attributes in the cipher text.

### *C. Break-glass*

In emergency the regular access policies cannot be applied. So break-glass access is used to access the patient's PHR by giving access rights to an emergency department (ED), (6)). To prevent the misuse of break-glass service, the emergency staff must be authorized by the ED and the emergency situation, and obtain temporary read keys ((7)). After the emergency, the patient can revoke them.

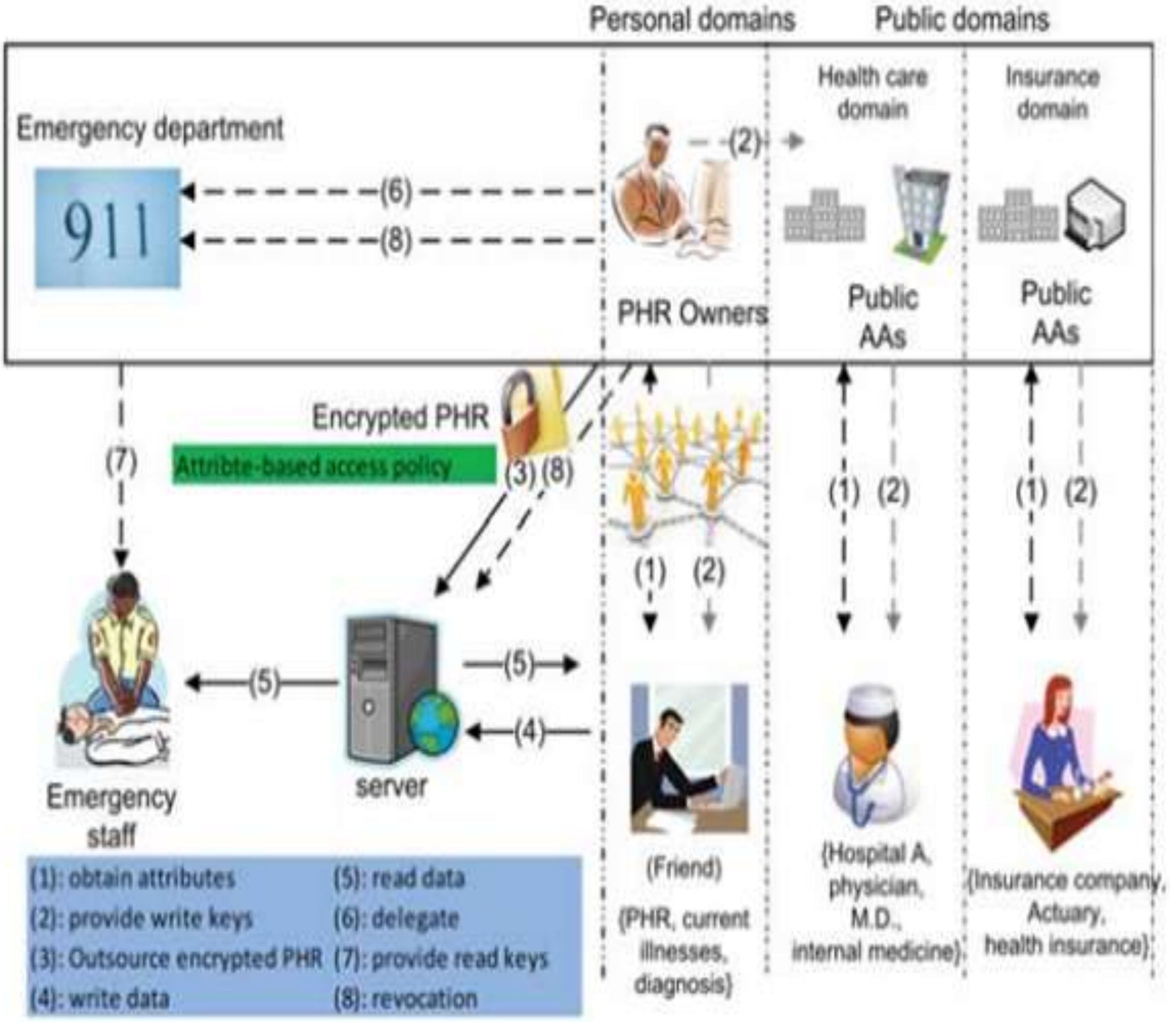

Figure 1. The Proposed Framework for patient centric, Secure & Scalable PHR sharing on semi trusted storage under multi-owner settings

Following are the modules of the project

- PHR Owner Module
- Server Module
- Attribute based Access Policy Module
- Data confidentiality Module

The PHR Owner module provides secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, *public domains* (PUDs) and *personal domains* (PSDs)) according to the different users' data access requirements. The server is semi-trusted. The system assumes each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols. In the framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users. In addition, two ABE systems are involved. The proposed system term the users having read and write access as data readers and contributors, respectively. The owners upload ABE-encrypted PHR files to the server. For encryption of PHR Attribute Based Encryption technique is used for key generation and Blowfish encryption technique is used for Encryption. The system is Defect Tracking System is of P Class because: Problem can be solved in polynomial time.

## IV. Evaluation Result

Figures shows storage cost, execution time and performance analysis of encryption algorithms. As compare to other encryption algorithm, ABE and Blowfish has equal storage cost, lowest execution cost and highest performance. So ABE and Blowfish is best option for providing security in PHR system.

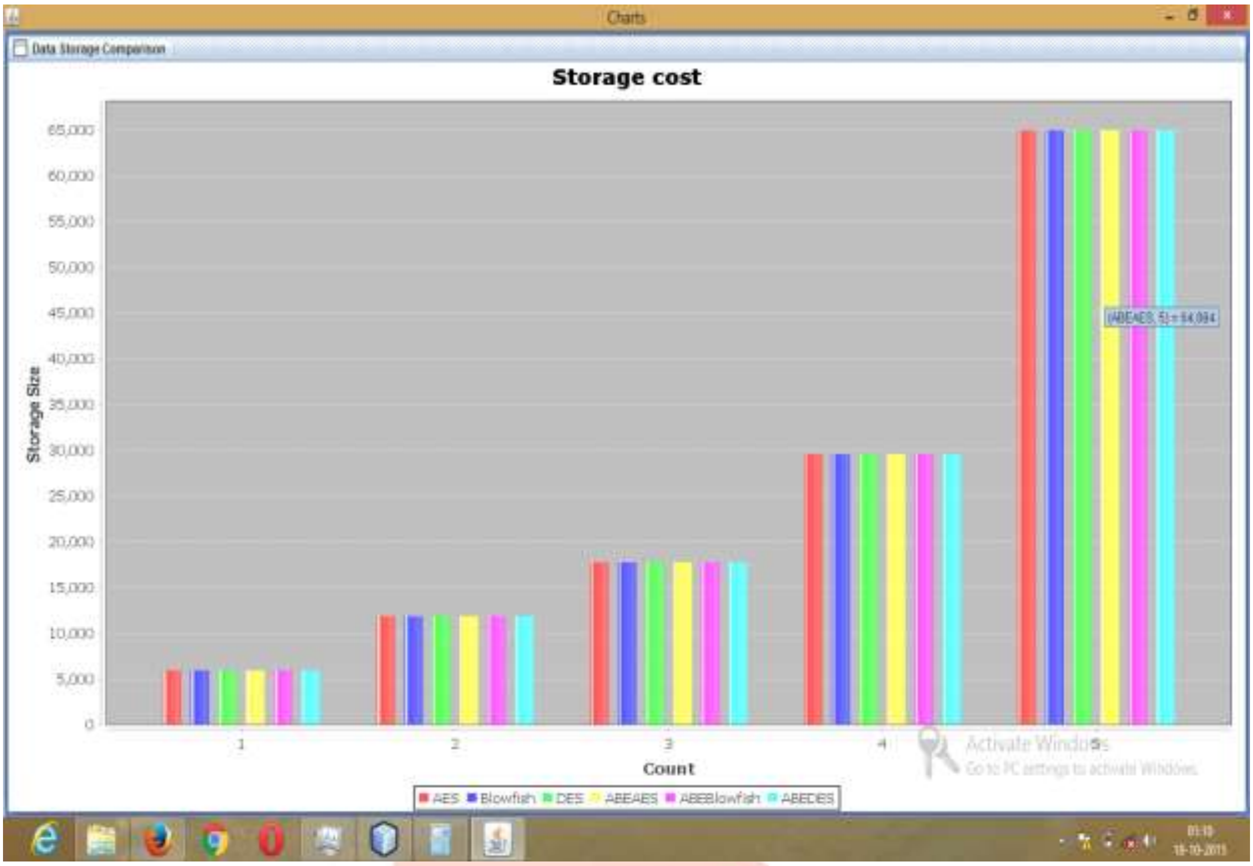

Figure 2 Storage Cost Analysis

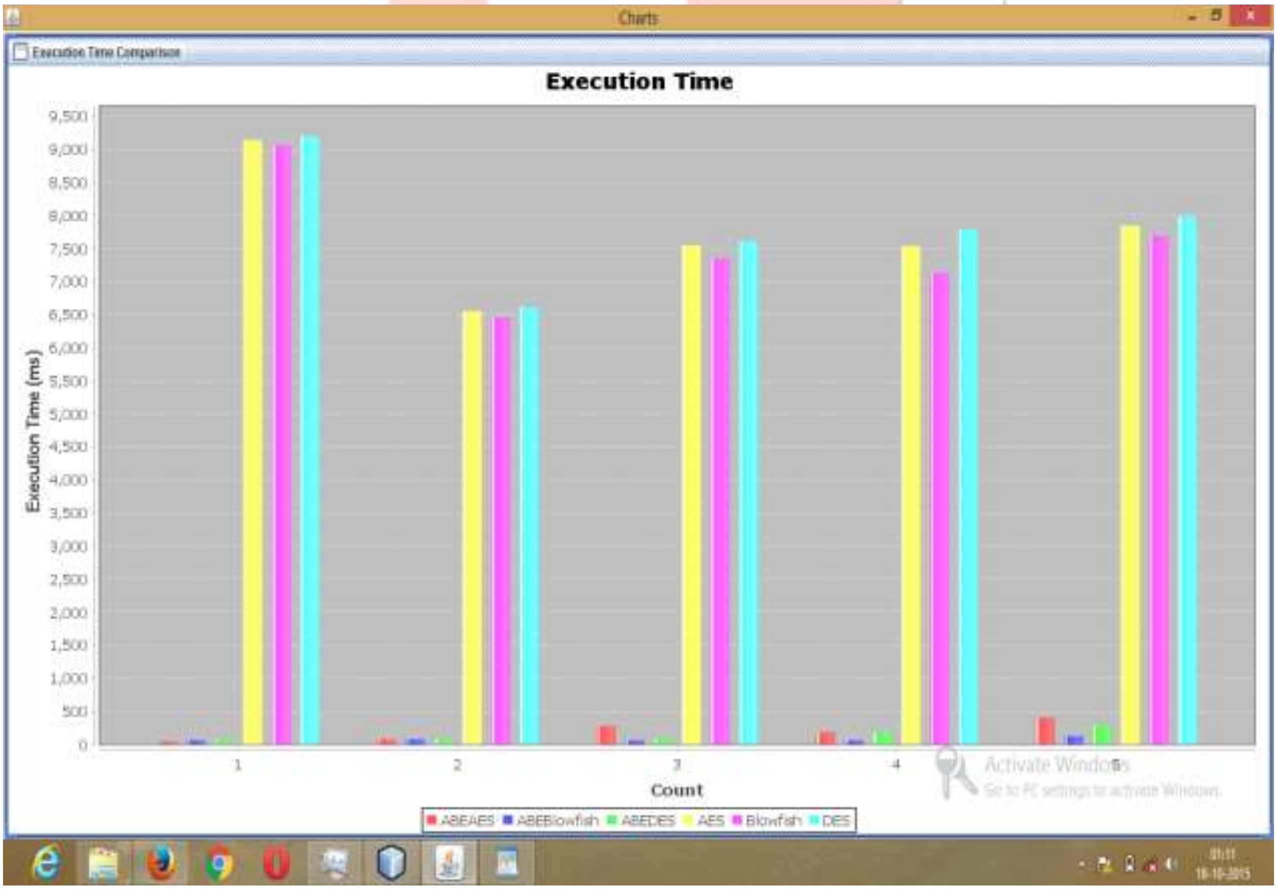

Figure 3 Execution Time Analysis

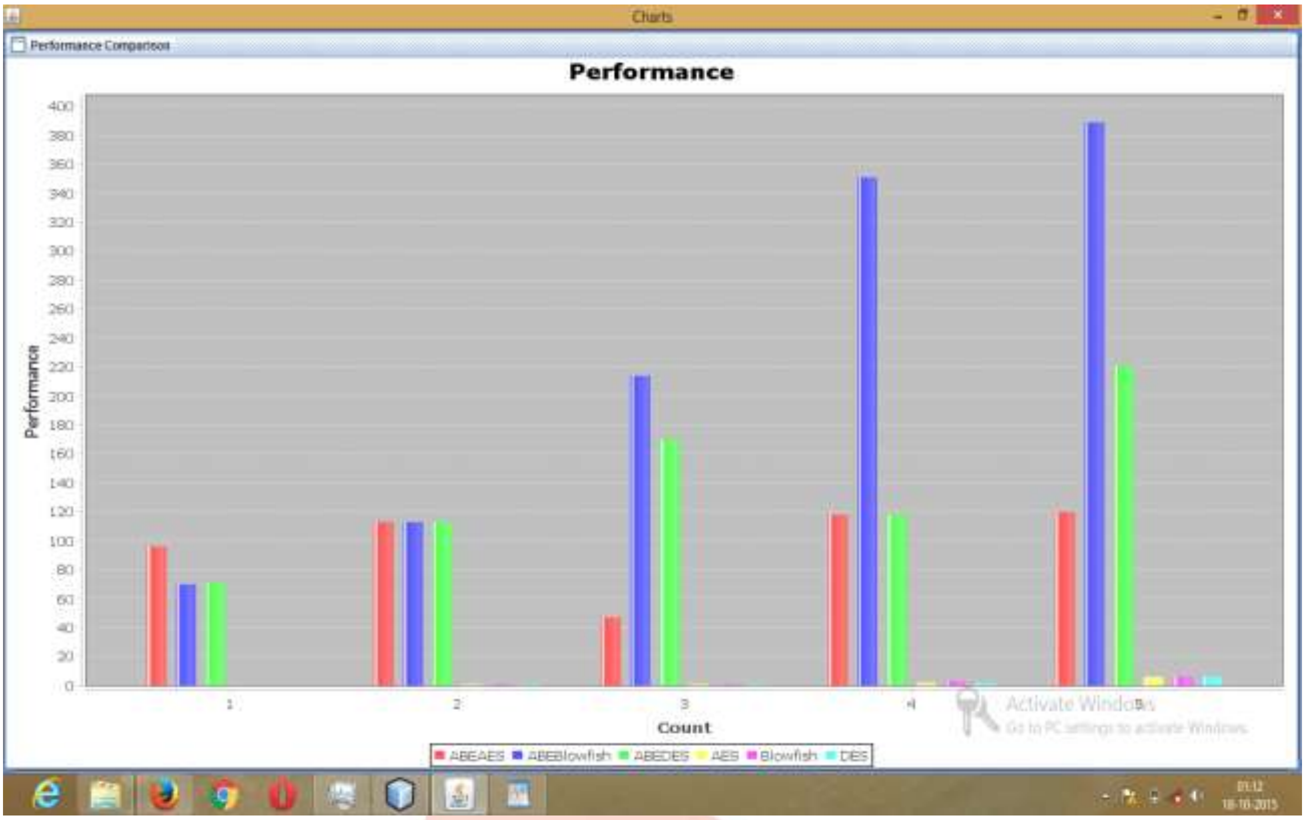

Figure 4 Performance Analysis

## V. CONCLUSION

There was widespread consensus at the College's symposium about the potential value of PHR systems. Participants elucidated the potential of PHR systems to transform patient–provider relationships, especially when integrated with EHR systems. They also identified many challenges—technical, social, organizational, legal, and financial—that warrant further study.
PHRM systems plus points are described by users that transform patient provider relationships. Especially when it is integrated with EHR systems. PHRM has many that must be considered for further study like technical, social, organizational, legal, and financial. Users and organizations related to medical field fast adopt PHRMs. Many challenges to deployment of PHRMs are similar to those for EHRs. More PHRM-related research is required. In PHRM every entity such as employers, patients, payers, governments, and research institutions must play key roles in developing PHRM to overcome the problems to widespread adoption. With a better understanding of the needs and benefits of PHRMs, we can develop better solution. The opportunity costs for PHR deployment are measured in medical errors, dollars, and lives. If the potential benefits are to realize for both routine health care and for responding to catastrophic disasters like Hurricane Katrina, these important PHR-related issues must be addressed.

## VI. ACKNOWLEDGEMENT

I want to thank all the people who helped me in different way. Especially I am thankful to my guide Prof. Pankaj R. Chandre for his continuous support and guidance in my work. Also, I would like thank our HOD Prof. S. A. Joshi , and Principal Dr. A. S. Padalkar.

## REFERENCES

[1] J. Benallie, M. Chase, et al. "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records", CCSW '09 Proceedings of the 2009 ACM workshop on Cloud computing security New York: ACM Press,( 2009).

[2] V. Goyal, O. Pandey, et al. "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", CCS '06 Proceedings of the 13th ACM conference on Computer and communications security, New York: ACM Press,( 2006).

[3] M. Chase, S. S. Chow. "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", CCS '09 Proceedings of the 16th ACM conference on Computer and communications security, New York:ACM Press,( 2009).

[4] [Online]. Available: http://www.research2guidance.com/us-1.3-billion-the-market-for-mhealth-applications-in-2012/

[5] Employee Benefit Research Institute. (2008). *Retirement Confidence Survey* [Online]. Available:

http://www.ebri.org/surveys/hcs/

[6] L. Sweeney, “K-Anonymity: A model for protecting privacy,” *Int. J. Uncertain. Fuzz.*, vol. 10, no. 5, pp. 557–570, 2002.

[7] [Online]. Available: http://www.healthegift.com/page/50

[8] [Online]. Available: http://www.nytimes.com/2011/11/05/us/ucla-health-system-warns-about-stolen- records.html

[9] Ponemon Institute. (2012). *Third Annual Survey on Medical IdentityTheft* [Online]. Available: http://www.ponemon.org/

[10] [Online]. Available: http://healthcaremgt.net/blog/2011/08/areyou-educating-patients-on-ehr/

[11] K.D. Mandl, P. Szolovits, and I.S. Kohane, “Public Standards and Patients’ Control: How to Keep Electronic Medical Records Accessible but Private,” BMJ, vol. 322, no. 7281, pp. 283-287, Feb. 2001.

[12] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,” Proc. ACM Workshop Cloud Computing Security (CCSW 09), pp. 103-114, 2009.

[13] C. Dong, G. Russello, and N. Dulay, “Shared and Searchable Encrypted Data for Untrusted Servers,” J. Computer Security, vol. 19, pp. 367-397, 2010.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proc. 13th ACM Conf. Computer and Comm. Security (CCS 06), pp. 89-98, 2006.

[15] D. Zismer, J. McCullough, and P. Person, “Integrated health care economics. Part 2: Understanding the revenue drivers in fully integrated community health systems,” Physician Exec., vol. 35, no. 4, pp. 26-28, 2011.

[16] M. Li, S. Yu, K. Ren, and W. Lou, “Securing personal health records in cloud computing: Patient-centric and finegrained data access control in multi-owner settings,” in Proc. SECURECOMM, Singapore, 2010, pp. 89106.

[17] D. Zismer, J. McCullough, and P. Person, “Integrated health care economics. Part 2: Understanding the revenue drivers in fully integrated community health systems,” Physician Exec., vol. 35, no. 4, pp. 26-28, 2011

[18] S. E. Wang, B. G. Lin, “ College of Mathematics and Computer Science,F uzhou Un A Scheme Of Attribute-Based encryption Access Policy Used In Mobile Cloud Storage For Personal Health Records”.

[19] Reshma S. Sapakal, et.al, “Secure Patient Health Record Manager Using Attribute-Based Encryption”, International Journal of Computer Science and Mobile Computing vol. 3 December 2014.