Innovative Science and Technology Publications

International Journal of Future Innovative Science and Technology,
ISSN: 2454- 194X Volume-3, Issue-2, Jun - 2017

A SURVEY ON SECURE SHARING ALGORITHMS USED ON PERSONAL HEALTH RECORDS

G.Priyanka[1]
PG Scholar
Computer Science and Engineering Department,
Vivekanandha College of Engineering for Women,
Namakkal, India.
priyankariya1094@gmail.com

D.Radhika [2]
Assistant Professor
Computer Science and Engineering Department,
Vivekanandha College of Engineering for Women,
Namakkal, India.
radhikadeva6@gmail.com

Jun – 2017

www.istpublications.com

A SURVEY ON SECURE SHARING ALGORITHMS USED ON PERSONAL HEALTH RECORDS

G.Priyanka[1]
PG Scholar
Computer Science and Engineering Department,
Vivekanandha College of Engineering for Women,
Namakkal, India.
priyankariya1094@gmail.com

D.Radhika [2]
Assistant Professor
Computer Science and Engineering Department,
Vivekanandha College of Engineering for Women,
Namakkal, India.
radhikadeva6@gmail.com

Abstract: Personal Health Records or PHR is the medical information of a person, stored and managed by the patient himself, in third party servers like clouds, so as to make it available for global data sharing. As the usage of such servers for storage purposes become more complex, they give rise to various security issues. Privacy, scalability and flexibility are some general issues concerning third party servers. Attribute Based Encryption (ABE), one of the earliest methods used for outsourced data encryption, has been utilized in several schemes as a solution, but such designs suffer from inflexibility, when the access control policies used are complex. This work focuses on the multi-data owner/sspatient scenario, where the PHR system users are divided into two security domains- the private domain and public domain, each of which is encrypted using its own set of mechanisms.Based on the analysis result we propose a solution to secure symmetrically encrypted cipher text that has efficiency higher than the existing solutions.

Index Terms: *Flexibility, Access Policy, Scalability, Attribute Revocation*.

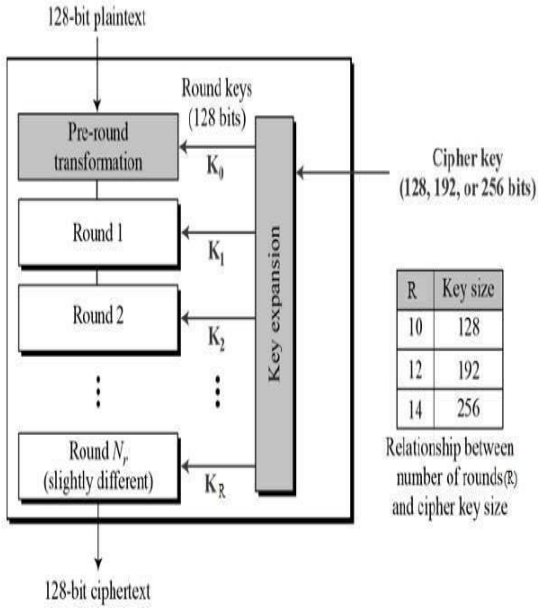
I.INTRODUCTION

A PHR is information about the health of a patient, compiled and maintain by the patient himself. This can be used to path and share an individual's past and current health information. PHR is also a tool for global medical data sharing. Thus an authorized medical care provider can have access to a patient's health related information and thereby gains more insight into the health history of the patient under his care. To overcome the obstacles arising as a result of scalability problems, many PHR services are outsourced to third party servers like the clouds. Cloud Computing, one of the most powerful paradigms in the IT sector, is a way to increase capacity on the fly without investing in new infrastructure, training new personnel, or licensing new software. However cloud computing means storage of data on the internet Central Authority can lead to a single point of failure. A better suggestion, which has also been effectively implemented, is the Attribute Based Encryption (ABE) scheme.

Operation of AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and rounds for 256-bit keys. Each of these rounds uses a different

128-bit round key,



R	Key size
10	128
12	192
14	256

Relationship between number of rounds(R) and cipher key size

Users of the PHR service are given access to a PHR file only if they have been authorized by the PHR owner/patient, i.e., the patient. A patient's PHR file can be accessed by his relatives, friends, doctors, nurses etc. If the owner/patient is responsible for managing all details of each user key, In this Internet era data grows rapidly. Storing huge amount of data locally using Pcs, pen drive, CD (or) DVD is highly impossible. So the users tend to use the cloud for storage purpose. Cloud is a virtual environment where the user can use remote servers through internet for storing, managing or for processing the data. Cloud storage is one of the services offered by cloud. It provides high security of data, reduce the cost of storage, easy sharing of huge data, data recovery etc. So, using the cloud storage space efficiently is essential for every user. For that purpose data deduplication technique is used.

II.LITERATURE REVIEW

While reviewing a scheme we listed the algorithms and techniques used in that scheme and the merit and demerit of that scheme are also specified. The following papers are survived in this section

In [1] authors Maheswari S, upendra gudla **"Secure sharing of personal health records in Jelastic cloud by Attribute based encryption"** describe about patient health records in Jelastic cloud provides the more profit to the data owner and end users. We know that building a specialized data center's is very difficult task and maintenance charge also very high. Jelastic Cloud is exactly given that the high security, scalability and easy maintenance to the PHR application in cloud. To supply the security to our PHR information, we use the Attribute based encryption algorithm we can encrypt the patient health information before storing into third party server (Servint).

Data, its only become visible in the form of encrypted data. For decrypting the information we must key, only allowed persons having the key and they can easily access the PHR data based on the attributes (friends, family members and doctors) given by the user though uploading their personal health records. Identity based encryption [IBE], is proposed by Alexandra Boldyreva for providing the security to the Information or data stored in third party servers.the merits of this Jelastic Cloud provides the Scalability, Load balancing and easy maintenance to our PHR .But demerits of reduces the Maintenance cost. idea about that Compared to the previous works our algorithm and PHR is operational successfully in cloud environment with the great features.

In [2] authors John Bethencourt, Amit Sahai, Brent Waters **"Ciphertext-Policy Attribute-Based Encryption"** propose scheme only method for enforce such policy is to employ a trusted server to store the data and act as a go-between access control. we current a system for realize difficult access control on encrypted data by means of the purpose of we call Ciphertext-Policy Attribute-Based Encryption. our methods are secure against collusion attacks. before Attribute- Based Encryption systems used attributes to explain the encrypted data and build policies into user's keys. traditional access control methods such as Role-Based Access Control (RBAC). user encrypts sensitive data, it is necessary that she create a specific access control policy on who can decrypt this data. For example, expect that the FBI public corruption offices in Knoxville

and San Francisco are investigate an contention of bribery involving a San Francisco lobbyist and a Tennessee congressman. we would like to need that sensitive data is store in an encrypted form so so as to it will remain private even if a server is compromise. Merit of this our system is that it is proved secure under the generic group heuristic .demerits of system secure under a more standard and non-interactive assumption. resulted in a reasonable loss of efficiency.

In [3] authors Shucheng Yu, Cong Wan, Kui Ren , and Wenjing Lou **"Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing"**proposed a emerging compute paradigm in which resources of the computing infrastructure are provided as services over the Internet. To keep sensitive user data private against untrusted servers, existing solutions usually apply cryptographic methods by disclose data decryption keys only to allowed users. We realize this goal by exploiting and exclusively combining technique of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. promising computing paradigm which newly has drawn general attention from both academia with industry. various business models are developed, which can be described by terms of "X as a service (XaaS)" [1] where X could be software, hardware, data storage, and etc. Successful examples are Amazon's EC2 and S3 [2], Google App Engine [3], and Microsoft Azure [4] which provide users with scalable resources in the pay-as-you use fashion at comparatively low prices. the merits of the scheme security proofs show that is secure under standard cryptographic models. But it has a demerit too that is One challenge in this context is to achieve fine.

In [4] authors Melissa Chase, Sherman S.M. Chow **"Improving Privacy and Security in Multi-Authority Attribute-Based Encryption"** determine decryption ability based on a user's attributes encryptors can require that a user obtain keys for suitable attributes from each authority before decrypting a message. influence, and protects the users' privacy by prevent the authorities from pool their information on particular

users, thus making ABE more in working condition in practice. sender can encrypt a message specifying an attribute set and a numberd, such that only a recipient with at least d of the given attribute can decrypt the message. The solution in that effort is to require that each user have a unique global identifier (GID), which they must present to each power. We also present an anonymous key issue protocol which allows multi-authority ABE with improved user privacy. more recent terminology,it would be describe as a key-policy (KP) ABE plan that allows for threshold policies. the authority specify an attribute set for the user, and the user is allowed to decrypt when the overlap between this set and the set associated with a exacting ciphertext is above a threshold. the merits of the supports a tree access structure.
But it has a demerit too. But it has a demerit too capacity want to divide control of the various attribute over many different authorities.

In [5] authors Karthik.S. R, Bhavya B M **"Scalable and Secure Sharing of E-health Records using Encrypt Technique in Cloud Computing"** it determines a Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud provider exposed to those third party servers and to unauthorized parties. novel patient-centric framework and a suite of mechanism for data access control to PHRs stored in semi-trusted servers.

Toward achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) technique to encrypt each patient's PHR file. high degree of patient privacy is certain simultaneously by exploiting multi-authority ABE. Our scheme also enable dynamic correction of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenario. PHR service allows a patient to create, manage, and manage her personal health data in one place all through the web, which has made the storage, retrieval, and sharing of the medical information more

efficient. system into two types of domains, namely public and personal domains. popular professional users are manage distributively by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain. the merits of the privacy guarantees compared with previous works. But it has a demerit too capacity various users from public domains with different professional roles, qualifications and affiliations.

In [6] authors Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou, **"Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption"** describe a Personal health record (PHR) is an emerging patient-centric model of health in order exchange, which is often outsourced to be stored at a third party, such as cloud provider. there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To achieve fine-grained and scalable data way in control for PHRs, we power attribute-based encryption (ABE) technique to encrypt each patient's PHR file. A high degree of patient privacy is guaranteed simultaneously by exploit multiauthority ABE.

Every patient is promise the full control of her medical records and can share her health data with a extensive range of users, including healthcare providers, family members or friends. semitrusted servers, and focus on addressing the complicated and challenging key management issues. the merits of the practicality of using them in building PHRsystems. But it has a demerit data access right could be given based on users' identities rather than their attributes, while ABE does not handle that efficiently.

In [7] authors Iniya Shree, K. Narmatha, Vijesh Joe. C **"An Multi-Authority Attribute Based Encryption For Personal Health Record In Cloud Computing"** the cloud is to manage or to secure the data's from the unauthorized persons. Here in medical field, Patient – centric model describes about the patients Personal Health Record (PHR), anywhere the health information is to be secluded from the third party servers. The security scheme Multi Authority Attribute Based Encryption (MA-ABE) is used to keep the patient's record**.** planned results are compare with the existing CP-ABE and the results that MA-ABE model is more safe with less delay**.** storage space as a service, cloud storage provider allow you to safely upload your files to the internet, which will be store on the third party services. Patients can control their health information and with the help of Internet way in they can get their information wherever at any time. It make easy to collect and keep their medical information in one accessible and secure location. To make sure patient-centric privacy control more than their own PHRs, it is required to encrypt the data before storing patient's information. the merits of the terms of specifying policies and managing user attributes CP-ABE. But it has a demerit makes easy to gather and maintain their medical information in one accessible and secure location Carrying paper records.

In [8] authors Y.B. Gurav, Manjiri Deshmukh **"Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption**" the centralize server to maintain patient's personal and diagnosis information. Personal health record (PHR) is an promising patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. novel patient-centric framework and suite of mechanism for data access control to PHR's stored in semi-trusted servers Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remain the most main challenges toward achieve fine-grained, cryptographically enforced data access control .

A high degree of patient privacy is sure concurrently by exploit multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute Revocation and break-glass access under emergency scenarios. To ensure patient-centric privacy control over their own PHRs, it is essential to

have fine-grained data access control mechanism that work with semi-trusted servers. A possible and promising approach would be to en- crypt the data before outsourcing. the merits of the homomorphic encryption with data auditing is used to verify the trustworthiness of third party auditor. But it has a demerit MA-ABE in real time with the property of Disjunctive as well as it had the little bit problem while revocation.

In [9] authors Yeong-Tae Song, Sungchul Hon, Jinie Pak **"Empowering Patients Using Cloud Based Personal Health Record System"** proposed empower patients to access to their own medical decisions. though, medical data is largely coming from clinical institution so there is no way for them to manage and maintain their own medical record. it is necessary to have an effective and efficient personal health record system (PHRS) that allows patients orguardians to continually monitor and control the personal health record.. A possible and promising approach would be to en- crypt the data before outsourcing.. monitoring capability by using easy uploading module and decision support system medical coding standards such as ICD-9-CM, SNOMED CT, etc. to achieve interoperability between different electronic health record systems. personal health record (PHR) system that allow an individual to monitor and share the data with the clinicians.

In terms of the important use, both EHR and PHR must be interoperable with each other via the observance to all applicable medical standards such as ICD-9-CM, SNOMED CT, LOINC, and HL7. the merits of the mobile application to collect medical data and stored in HL7 CDA format for interoperability. But it has a demerit general public in many ways – the transition from clinician centered to patient centered.

In [10] authors V.Indhumathi V.Prakasham, **"On Demand Security For Personal Health Record In Cloud Computing"** determines several services that maintain Personal Health Record (PHR). It is a patient health-centric replica for data exchange in cloud Personal Health Record (PHR) is often keep in a third party server i.e. cloud server. A high degree of patient privacy is enrich at the same time by developing Multi- Authority Attribute based mostly cryptography (MAABE). We include to improve the security of Personal Health information and set access privileges for every PHR data.

We propose a cloud based personal health record system that allows constant monitor capability by behind dynamic creation of clinical document architecture (CDA) document from a mobile device. Before taking a key to decipher the PHR record in multiple owner scenarios it must raise some security queries on PHR owner. We can say that it is a patient centric model as in general control of patient's data is with patient. Patient can create, delete, modify and split own PHR information through the public cloud and we made to storage, retrieval, then more efficient sfor sharing of the medical information. Attribute Authorities (AA) plays an important position to check the each user roles and attributes. And any other unauthorized users can't be access the whole system. Encrypted text are joint with the groups of attributes and using exact key only decrypt the cipher text. the merits of the PHR information is highly secured function for using Multi Authority-Attribute Based Encryption. But it has a demerit we significantly reduce the Key complexity.

III.ANALYSIS

This section presents the study on cipher text schemes which we reviewed in previous section. Based on this study results we can find the finest scheme used for cipher text.

Table 1: COMPARITIVE STUDY ON DEDUPLICATION SCHEMES

SI. NO	TITLE	Type of Secure ABE and cipher text policy	Algorithms Used	Merits	Demerits
1.	Secure sharing of personal health records in Jelastic cloud by Attribute based encryption	PHR secure	Attribute based encryption algorithm Identity based encryption algorithm	Scalability, Load balancing and easy maintenance to our PHR	reduces the Maintenance cost
2.	Ciphertext-Policy Attribute-Based Encryption	Role based Access control	Encryption algorithm, Decryption algorithm, Identity based encryption algorithm	our system is that it is proved secure, the generic group heuristic.	system secure under a more standard and non-interactive assumption.
3.	Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing	Health Insurance Portability and Accountability Act (HIPAA)	Attribute based encryption algorithm Decryption algorithm,	use fashion at comparatively low prices.	Cannot implemented directly in cloud
4.	Improving Privacy and Security in Multi-Authority Attribute-Based Encryption	Global identifier	Attribute based encryption algorithm. Key policy Attribute based encryption Decryption algorithm.	the supports a tree access structure.	the various attribute over many different authorities.
5.	Scalable and Secure Sharing of E-health Records using Encrypt Technique in Cloud Computing	Health Insurance Portability and Accountability Act (HIPAA)	Attribute based encryption algorithm Identity based encryption algorithm	privacy guarantees compared with previous works.	manage the keys of a small number of users in her personal domain.

6.	Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption	Health Insurance Portability and Accountability Act (HIPAA)	Attribute based encryption algorithm Identity based encryption algorithm	them building PHR systems.	ABE does not handle that efficiently.
7.	An Multi-Authority Attribute Based Encryption For Personal Health Record In Cloud Computing	CP-ABE	Multi Authority Attribute Based Encryption (MA-ABE) Key-Policy Attribute-Based Encryption (KP-ABE).	specifying policies and managing user attributes CP-ABE.	Cannot implemented directly in cloud
8.	Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-Based Encryption	Personal Health Center	Attribute based encryption algorithm Multi Authority Attribute Based Encryption (MA-ABE)	MA-ABE in real time with the property	the little bit problem while revocation.
9.	Empowering Patients Using Cloud Based Personal Health Record System	Health Information Exchange	Attribute based encryption algorithm Decryption algorithm.	the mobile application to collect medical data	High cost
10.	On Demand Security For Personal Health Record In Cloud Computing	Health Insurance Portability and Accountability Act (HIPAA)	Multi-Authority Attribute based mostly cryptography (MAABE) Attribute Authorities (AA)	the PHR information is highly secured	the Key complexity.

IV.POSSIBLE SOLUTION

"Medical Care Goes Home" become a clear healthcare trend in future. It indicates provision of health services to homes with new innovative services such as personal health monitoring and support systems and user-friendly information systems for supporting health education and awareness. The trend is towards more involvement of patient in receiving information, in decision-making and in responsibility for own health. The prime feature of this trend is to shift from healthcare-institution-centered care to the patient centered care and from prevention to rehabilitation. PHR that enables patients to record and maintain their own health records plays a significant role in this trend. PHR will continue to flourish as the related technologies evolve. Standardization will play a more and more important role in PHR development. The main challenges from the technological point of view refer to the storage, maintenance, communication and retrieval of multimedia information in different technological platforms and heterogeneous database systems that may be geographically distributed. Integration and interface of multi-vendor platforms and the development of health sector specific middleware and applications have recently received lot of effort by research and development projects. This integration effort is critical since the number of systems of different purposes (administrative, insurance, clinical, nursing, etc) is rising. The standardization issues among all types of electronic health records, including PHR, EMR, etc. become more and more important.With the expansion of electronic health records, EHR developers have developed their own Personal Health Records or patient portal systems, which allow patients to have direct access to much of their clinical data, including such items as diagnoses, procedures, allergies, medications, surgeries, lab results, and other data and to manage on-line such activities as scheduling of visits and prescriptions and refills. This type of PHR is referred to as a "tethered" PHR, since it is typically limited to a single health system. While these tethered systems have become popular, many patients get their care from numerous providers, so their tethered PHR record may be incomplete. Thus, there has been growing interest in developing non-tethered, crossorganization PHRs, including those sponsored by Health Information Exchange (HIE) organizations. These untethered systems may have the advantage of providing comprehensive longitudinal information across the numerous providers where the patient has received care.

V.CONCLUSION

Further research needs to be done to evaluate the lack of internet access as a barrier to patients accessing their PHR. While this research showed that a lack of internet access

was not a barrier to PHR, this was an emailed online survey, which excluded patients that did not have functional email or Internet access from participating in the survey. The success of PHRs will hinge on whether PHRs benefits outweigh the barriers which rests on the success of the healthcare organizations, providers and information technology being able to engage patients. Low engagement population groups need to be targeted to establish a confidence level guaranteeing confidentiality, information control and collaborative information sharing.

REFERENCES

[1] Kabilan N, "Scalable and secure sharing of Health record maintenance using advanced encryption standard", SRResearch paper vol. 1, no. 4 may, 2016.

[2] Ming Li, Shucheng yu, Yao Zheng, Kui Ren and Wenjing Lou, "Scalable and secure sharing of personal health records in cloud using Attribute based encryption algorithm ", IEEE Transanction on Parallel and Distributed systems vol. 3, no.7, july 2015.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in s*Proc. Of CCS'06*, 2016.

[4] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over encryption: Management of access control evolution on outsourced data," in *Proc. of VLDB'07*, 2007.

[5] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2015.

[6] Mira Belenkiy, Jan Camenisch, Melissa Chase, Markulf Kohlweiss, Anna Lysyanskaya, and Hovav Shacham. Randomizable Proofs and Delegatable Anonymous Credentials. In CRYPTO, LNCS. Springer, 2016.

[7] Jan Camenisch and Anna Lysyanskaya. E_cient Non-transferable Anonymous Multi-show Credential System with Optional Anonymity Revocation. In EUROCRYPT 2001, volume 2045 of LNCS, pages 93{118. Springer Verlag, 2015.

[7] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, "Securing the E-Health Cloud," Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2016.

[8] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), June 2015.

[9] "The Health Insurance Portability and Accountability Act,"http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp, 2015.

[10] Akinyele .J.A, Sahai .A ,Lehmann .C.H, and Rubin .A.D, "Self-protecting electronic medical records using attribute-based encryption," Cryptology ePrint Archive, Report 2010/565, 2016, http://eprint.iacr.org/

[11] Attrapadung .N and Imai .H, "Conjunctive Broadcast and Attribute-Based Encryption," Proc. Third Int'l Conf. Palo Alto on Pairing-Based Cryptography-Pairing, pp. 248- 265, 2009.

[12] Benaloh .J, Chase .M, Horvitz .E, and Lauter .K, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security CCSW '09), pp. 103-114, 2016.

[13] Ming LiShucheng Yu, Yao Zheng,Kui Ren, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE transactions on parallel and distributed systems, vol. 24, no. 1, january 2015.

[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, 2015.

[15] McDaniel. P, Pirretti. M, Traynor. P,and Waters. B,"Secure Attribute-Based Systems," J.Computer Security, vol. 18, no. 5, pp. 799-837, 2015.

[16] Liang. X, Lu. R, Lin. X, and Shen. X.S, "Cipher text Policy Attribute Based Encryption with Efficient Revocation", technical report, Univ. of Waterloo, 2016.

[17] Li. Ming ,Shucheng Yu, Yao Zheng,Kui Ren, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", IEEE transactions on parallel and distributed systems, vol. 24, no. 1, january 2016.
[18] Yu. S, Wang. C, Ren. K and Lou. W, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2015.
[19] Sun. Jin, Hu. Yupu, and Zhang. Leyou,"A Key- Policy Attribute-Based Broadcast Encryption", The International Arab Journal of information Technology, Vol. 10, No. 5, September 2015.