Survey On Secured Health Care Data Sharing On Cloud Using Revocable Attribute Based Encryption Schemes

Somireddy Pavani [a], Dr. Arun Sahayadhas [b]

[a] Research Scholar of Computer Science and Engineering, VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai
[b] Professor of Computer Science and Engineering, VELS Institute of Science, Technology & Advanced Studies, Pallavaram, Chennai
[a]somi.phd@velsuniv.ac.in, [b]arun.se@velsuniv.ac.in.

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 4 June 2021

Abstract: The applications on generating, collecting and processing of a vast amount of sensitive or personal information have made easier by the latest advancements in the information technologies. In recent period, a problem arises in privacy module and storage module over the health care systems in storing and retrieving the large amount of data bases regarding to the medical history of every patient over a public cloud environment day by day. An additional security and privacy protection concern solutions are introduced by the cloud computing environment when it comes to data being outsourced to the cloud. Revocable Attribute Based Encryption (ABE) with data deduplication is the best way to avoid the privacy problems. In this paper, survey on secured health care data sharing on cloud using Revocable Attribute Based Encryption (ABE) schemes is studied that provides measures to meet any specific application requirements also for strong security to the system. In the results all different studies are evaluated and compared with each other to obtain a best out of it in terms security and performance.

Keywords: Attribute Based Encryption (ABE), Revocable-storage, health Care Systems, Data Sharing, security and data.

1. Introduction:

In addition to the public government organizations, private organizations also focused on eHealth as a first priority for the development from the past few decades to encourage this eHealth. At this point of view, for providing eHealth services in a reliable and cost-effective way, a constant increase in research focus on modern eHealth and founds aims to update the existed healthcare systems have been seen. A potential improvement of efficiency is provided by adopting of advances in eHealth solutions for managing of the medical healthrecords. New computational paradigms like cloud computing is of such adopted advances that helps in reducing the cost and supporting the collaboration among various organizations. The data of users stored in remote areas about health data records of patients however faces many challenges in privacy point of view. The designing of secured systems against to the variety of attacks and malicious behaviours is the main focus in investigation for the many of researches in addition to creating of flexible and efficient cloud based services [1]. On the other hand, sharing of health data records securely over the cloud can be allowed by various organizations like hospitals to host the data of patients with the clear set of existed mechanisms. As it is easy to transfer the medical records of patients with such type of mechanisms, the health practitioner's productivity can be increased. Also, research with a better support and enhanced collaboration among the various scientists and specialists around the world can be achieve due to such functionality of sharing**.** At First work on Revocable-Storage Hierarchical Attribute Based Encryption (RS-HABE) scheme considered as a fundamental structure in developing a framework for sharing the Electronic Health Records (EHR) securely over public cloud is studied which includes the revocation of user, updating of cipher text update and secret key delegation functionalities. The forward and backward security features are provided simultaneously by this RS-HABE scheme [2]. Secondly, a work that introduced a Privacy preserving, Revocable-Cipher text Policy-Attribute Based Encryption (PR-CP-ABE) scheme considered as a main structure of the frame work called integrated, privacy preserving user centric attribute based access control is studied which provide a privacy and security to the outsourced data of users which is stored throgh a Cloud Service Provider (CSP). The privacy preserving and protecting of data and CSPs efficiency in data storage are improved in this work by using the Extended Path-ORAM access protocol and integrated secure deduplication approach [3]. Then at last, a work of Revocable Cloud assisted Signature-Attribute Based Signcryption (RCS-ABS) Scheme depending on the attribute based signcryption technology is studied in this survey which provides a reliable and secured protection of data by preventing the users from accessing of data with knowledge of attributes. Then the revocation function of user is realized with such attributes that use the broadcast encryption and key segmentation technologies [4].

2. Structure Of Secured E-Health System:

The process of making a secure E-Health system is the proposed system of this paper, with the influence of Deduplication in attributes Based Encryption model. In E-Health system a lot of databases have been stored frequently. The purpose of using data Deduplication is the way to handle large amount of databases [5]. While talk about privacy in E-Health systems, Data access control technique is used to overcome the drawback of this system. The implementation of this technique was mainly depending upon on the encrypted data. Once the encryption was complete, data Deduplication process is come to fill the remaining part of the Attribute Based Encryption technique. The function of general ABE algorithm with de-duplication process applied one to protect data from the attackers [6]. The experimental structure of ABE algorithm with E-health system has shown in the figure (1).

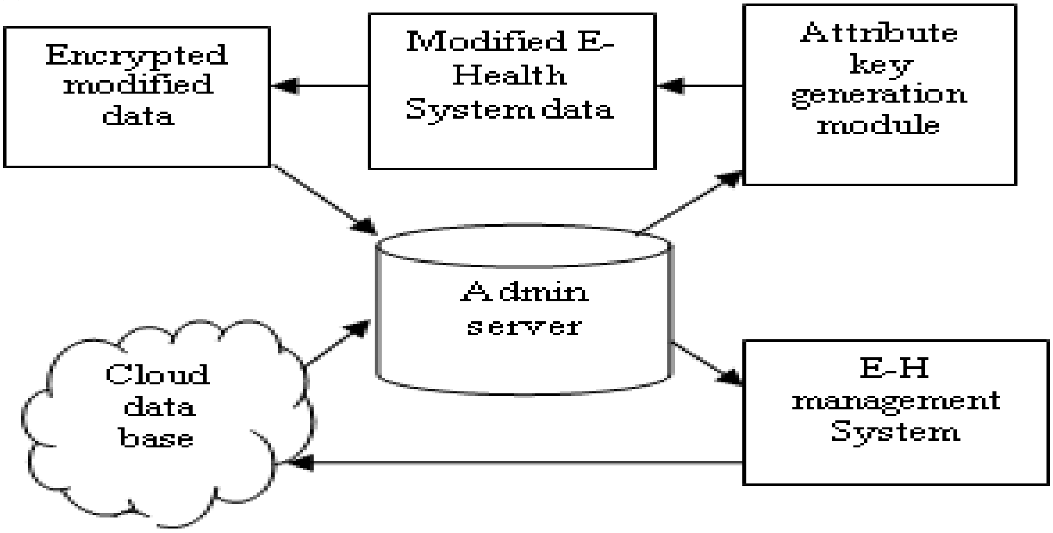

Fig. 1: STRUCTURE OF SECURE E-HEALTH SYSTEM

Some of the important modules of E-Health Systems are

2.1 Log in

It is the first module of the E-Health System. In this module, it is used to register a patient log in form. After the procedure of complete the registration, that module admin provide a admit card for the E-Health System [7]. That admit card is used to move the way of doctor's appointment fixing module. It includes all the databases of patient registration.

2.2 Appointment

It is the second module of E-Health System. The process of this module was fixing the appointment of doctor's based on health problems [8]. For instance a patient register a disease as eye problem, that module admin fix the appointment of eye doctor.

2.3 Doctor

This module gathers information about doctor's period of time that available in that hospital. It denotes how many doctor's worked in that hospital and how many specialist doctors currently available in that hospital also mentioned in that module.

2.4 Patient

After visiting the doctor's that admin module stores the information about patient details. It contains several number of databases can be stored and retrieved day by day [9].

2.5 Report

At the end of all the check up in hospital and consulting with doctor, that admin module provide a patient medical report and stored in a report databases in that module . In case patient misses a medical report, that time with the use of this module, retrieved their medical report immediately. It also contains large amount of databases [10].

3. Survey On Secured Revocabl Abe Schemes In Health Care Data Sharing

3.1 RS-HABE Based Scheme

This work focused on advancements in sharing of EHR data outsourced to the cloud securely with ABE. The challenging problems such as revocation of users, updating the cipher text and secrete-key delegation that are not handled by the existed methods had mostly focused in this work. For this, with the addition of important functionalities a new cipher text-policy ABE has developed first and then most widely used attribute based access scheme is build by combining it with a symmetric encryption scheme to share the data of HER securely over the public cloud. The major contribution of works in this study is particularly described further. Requirements of securely sharing the EHR data over a cloud were met and formalized it with a notion of revocable-storage hierarchical ABE by extending the new cipher text policy ABE. This scheme simultaneously captured the dynamic revocation of user, updating of public cipher text and scalable secret key delegation. This work provides a forward security and backward security perfectly that overcome afore mentioned problems. Then a general frame work called attribute based access is developed depending on the symmetric encryption and RS-HABE such as cipher text policy. This frame work supported secure and efficient sharing of private data to the every host even over the semi-trusted cloud servers because of the advantages of RS-HABE.

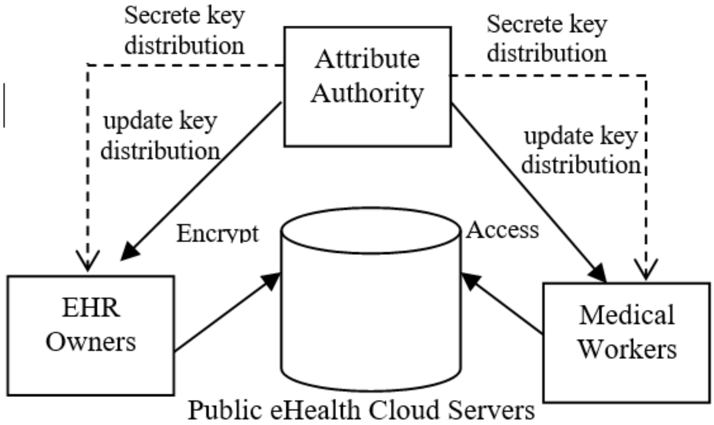

Fig. 2: Secured Ehr Data Sharing Framework Using A Rs-Habe Scheme

The following frame work shown in figure (2) instantiated under the bi-linear groups by introducing the structure of existing RS-HABE scheme. This RS-HABE's security notation has defined and its selective security has proved in exclusive of random oracles based on assumption of q-type complexity in the bilinear groups. Then the performance of this work relating to the system functionality and security were evaluated theoretically. Finally this work was illustrated from the experiments that it was a frame work that achieved a preferable practicality and security of sharing HER data over the cloud.

3.2 Integrated PRCP-ABE Scheme

In this a framework called an integrated, privacy preserving organization or user centric attribute based access control is developed with the ability of revocation, updated privacy preserved access policy, secured de-duplication of data and privacy protected access patterns. Fine grained access controls which has read or write access over the encrypted data was supported in this frame work.

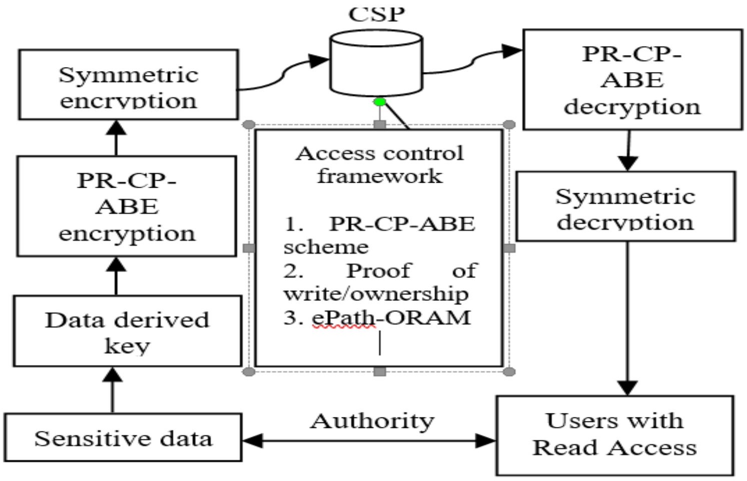

Fig. 3: STRUCTURE OF PRCP-ABE SCHEME FRAMEWORK

The PRCP-ABE scheme is the main structure of the framework as shown in figure (3) that used with a new access control approach. It was possible with this used structure of access control framework to support the dynamic attribute revocation and to prevent the loss of privacy for sensitive data. This structure of access control framework used the Linear Secret Sharing Scheme (LSSS) matrix. It was proved that LSSS is an efficient and significant policy structure. From their knowledge, this work may the first structure which combines both the structure of privacy preserving LSSS access policy and immediate attribute revocation.The prevention of access pattern disclosures and provision of advanced access control features are supported in this frame work by the extended Path (ePath)-Oblivious RAM (O RAM) access protocol that weren't supported by the existed ABE schemes. In the cloud storage application, this protocol allowed hiding of a client's access patterns from a strange server. Moreover, existed schemes not supporting the update of encrypted data as well as access polices were also supported with this ePath-ORAM-Access protocol to update read/write data and issues of policy operations. In addition, secure de-duplication solution also introduced according to the used access control scheme in order to meet the CSP's storage requirements. To this end, one proof and two proofs of write and ownership mechanisms respectively along with a scheme for achieving secure de-duplication are used. Then, in terms of performance guarantees and security an evaluation of this framework was presented compared with the other existed schemes. Moreover, this PR-CP-ABE scheme framework efficiency is evaluated by implementing a prototype of this work along with the secured de-duplication mechanism performance in terms of encryption and decryption computation time. Confidentiality and unforgeability and feasibility of the scheme also shown by using the further analysis of communication and computational overhead. Figure (4) shows the schematic of this specific system.

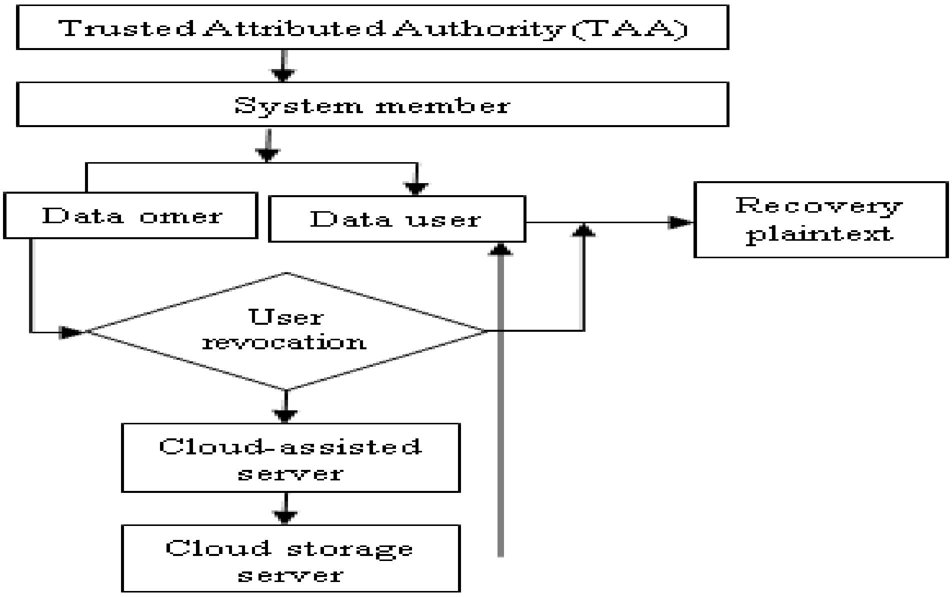

Fig. 4: SCHEMATIC OF SYSTEM

This work studied and analyzed various researches relative to the user revocation mechanism in the existed attribute-based cryptosystem schemes to meet the requirements of different application areas by adding them with this attribute-based signcryption system. The broadcast encryption scheme along with key splitting technology was used firstly to realize the cloud-based EHR system by presenting a novel RCS-ABSC scheme. This means, the messages are neither signed nor decrypted in the system by the revoked users. The first scheme used in attribute-based signcryption scheme that implemented a revocation function was a RCS-ABSC scheme. This scheme with the function of user revocation demonstrated that it was a feasible particularly in terms of the communication and computing costs. Moreover, the computation overhead of signcryption is reduced at user side to support the authentication by using a trusted third party server to assist signature. In addition to the gunteeing the authentication, confidentiality and privaacy protection for data, public varification also provides by this method.

4. Results:

Development of Encrypting datas with the use of cloud computing has done a remarkable job of store and secure data's from vulnerable attacks. In E-health system before the arrival of encrypting technique, lot of problems had raised in that period. The theoretical analysis of the discussed studies indicates the functionality and security at the suitable cost of computation overhead. The performances of works studied in this survey are evaluated and compared regarding to the security and functional properties as shown in table (1).

Table 1: COMPARISONS OF SECURITY PROPERTIES

Properties	**RS-HABE Based Scheme**	**Integrated PRCP-ABE Scheme**	**RCS-ABSC Scheme**
Access policy	LSSS	LSS matrix	MSP
Revocation level	User	Attribute	User
Security method	Backward and Forward Security	Privacy preserving-Cipher Policy	Attribute based Signcrypt-ion
Hierarchical key delegation	yes	Yes	No

The security properties of studied works focused on the revocable ABE scheme for the secure health data sharing over the cloud are summarized in the above table (1). The significant access polices are supported in all the RS-HABE and integrated PRCP-ABE schemes in a LSSS form. It can be seen that the attribute based revocation is supported by the integrated PRCP-ABE scheme where as user based revocation is supported by the remaining of RS-HABE and RCS-ABSC schemes. Backward and Forward Security is provided in the RS-HABE scheme with the help of dynamic revocation of user and updating of public cipher text policy. The privacy protection and secured HER data sharing is provided in PRCP-ABE scheme with the Privacy preserving-Cipher Policy method. Then reliable and secured protection against the data is provided in the RCS-ABSC scheme using the attribute based Signcryption method. Moreover, RS-HABE and PRCP-ABE schemes only utilized the hierarchical key delegation enjoy the functionality.

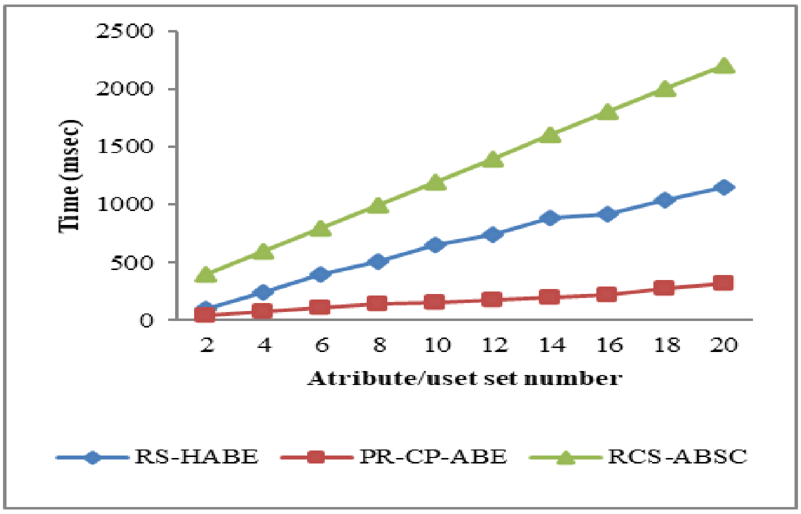

Fig. 5: Comparision Of Computational Time For Encryption

The computational time on both the encryption and the decryption of data using three schemes are computed and compared as shown by the figure (5) and figure (6). It can be seen that relatively a linear characteristics are there for the both encryption and decryption computational times with the number of attributes or user sets. The computational time is much higher for the encryption than the decryption. From the figure (5), it can be illustrated that the PRCP-ABE scheme acquires a less computational time for the encryption compare to the other two schemes since it support the privacy preserving access policy structure. The RCS-ABSC has lower computation time than RS-HABE scheme because of its signature generated partially using a trusted third cloud server.

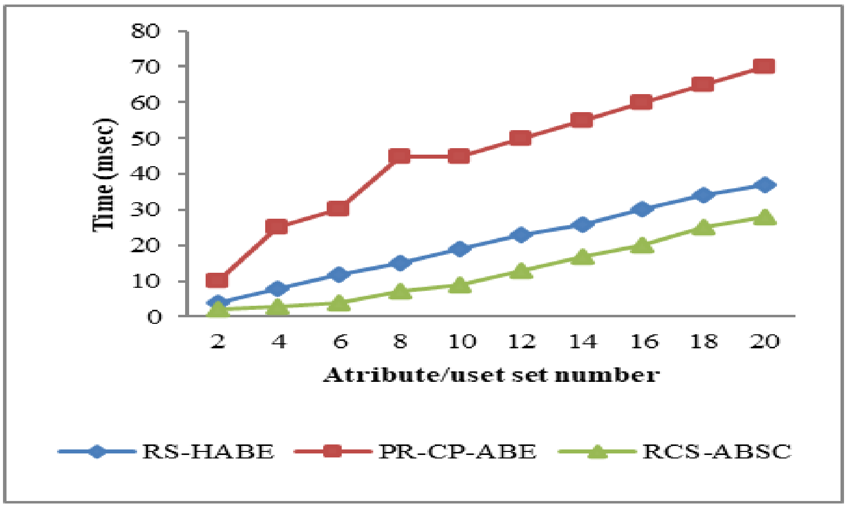

Fig. 6: Comparision Of Computational Time For Decryption

From figure (6) it can be shown that the computation time for decryption is low for the RCS-ABSC scheme because of the direct revocation and signature based attribute than other two ones. The RS-HABE has acquired less computation than the PR-CP-ABE scheme.

5. Conclusion:

Since E-Health system contains patient medical reports, patient databases, doctor's details etc., it will be a bigger problem of this society right now once the information's are hacked. So security and storage module is very important one to develop an E-Health organization System. This survey paper studied on Revocable Attribute-Encryption schemes supported the progress of E-Health System environment with privacy and storage modules.

This survey paper presented some significant works focused on privacy preserved sharing and secured storage of health data records over a cloud. This survey will provide a helpful insight to the designers in order to suggest the designing and development mechanisms for the cloud based eHealth services which would be support sharing of data over a different cloud environments.

References

1. Jianting Ning, Haijiang Wang, Geong Sen, Ximeng Liu, Poh Xinyi Huang and Guiyi Wei, "Secure Fine-grained Encrypted Keyword Search for e-Healthcare Cloud", IEEE Transactions on Dependable and Secure Computing, 2019
2. Jianghong Wei, Xiaofeng Chen, Xinyi Huang, Xuexian Hu, and Willy Susilo, "RS-HABE: Revocable-storage and Hierarchical Attribute-based Access Scheme for Secure Sharing of e-Health Records in Public Cloud", IEEE Transactions on Dependable and Secure Computing, 2019.
3. Runhua Xu, James Joshi and Prashant Krishnamurthy, "An Integrated Privacy Preserving Attribute Based Access Control Framework Supporting Secure De-duplication ", IEEE Trans., on Dependable and Secure Computing, 2019
4. Li Peng, Yali Wang, Ji Geng, Miao Lai, and Fuhu Deng, "Revocable Cloud-Assisted Attribute-Based Signcryption In Personal Health System", IEEE Access, 2019.
5. Xiaozhu Meng, Kun He, Pan Zhou, Zhizhou Pan and Ling Yuan, "A Novel Task-Duplication Based Clustering Algorithm for Heterogeneous Computing EnvironmentS", IEEE Transactions on Parallel and Distributed Systems, 2018
6. Yarkın Doröz, Wei Dai, Kurt Rohloff, Yuriy Polyakov, Erkay Savaş, Berk Sunar and Hadi Sajjadpour "Implementation and Evaluation of a Lattice-Based Key-Policy ABE Scheme", IEEE Trans., on Info., Fore., & Secu., Volume: 13, Issue: 5, 2018
7. Yixin Zhang, He Luo, Liping Zhang, and Shanyu Tang, "Privacy Protection for E- health Systems by Means of Dynamic Authentication and Three-Factor Key Agreement", IEEE Trans., on Indu., Electr., Vol: 65, Issue: 3, 2018
8. Jianyong Sun, Liehang Shi, Jianguo Zhang, Tonghui Ling, Yuanyuan Yang, Yiping Gu, Zhiming Yang, Yanqing Hua and Mingqing Wang, , "Three-Dimensional Visual Patient Based on Electronic Medical Diagnostic Records", IEEE Jour., of Biomedical and Health Informatics, Vol: 22, Issue: 1, 2018
9. Daphney-Stavroula Zois, Tolga Soyata and Omid Rajabi Shishvan, "achine Intelligence in Healthcare and Medical Cyber Physical Systems: A Survey", IEEE Access, Volume: 6, 2018
10. Guangzhe Zhao, Zhi Liu, Yankun Cao, Jiahua Song and Lizhen Cui, "A Benchmark Database and Baseline Evaluation for Fall Detection Based on Wearable Sensors for the Internet of medical Things Platform", IEEE Access, Vol: 6, 2018
11. Zhixin Sun, Hanshu Hong and Guofeng Lin, "A Collaborative Key Management Protocol in Ciphertext Policy Attribute-Based Encryption for Cloud Data Sharing", IEEE Access, Volume: 5, 2017
12. Kaiping Xue, David S. L. Wei, Peilin Hong Yingjie Xue, Hao Yue, Wei Li and Jianan Hong,, "RAAC: Robust and Auditable Access Control With Multiple Attribute Authorities for Public Cloud Storage", IEEE Trans., on Infor., Forensics and Security, Vol: 12, Issue: 4, 2017
13. Xiaohua Jia, Xuemin Sherman Shen, Kan Yang and Zhen Liu,, "Time-Domain Attribute-Based Access Control for Cloud-Based Video Content Sharing: A Cryptographic Approach", IEEE Transactions on Multimedia, Volume: 18, Issue: 5, 2016
14. Yoga chandran Rahul amathavan, Rongxing Lu, Fei Li, Jinguang Han and Muttu krishnan Rajarajan Suresh Veluru, "User Collusion Avoidance Scheme for Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption", IEEE Trans., on Computers, Vol: 65, Issue: 9, 2016.
15. S. Lin, R. Zhang, H. Ma and M. Wang, "Revisiting attribute-based encryption with verifiable outsourced decryption", IEEE Trans. Inf. Forensics Secur., vol. 10, no. 10, pp. 2119-2130, Oct. 2015.