In 2005, Amit et al. [5] developed Fuzzy IBE that allows one private key for an identity x to decrypt a cipher text encrypted under x', if both identities are close to each other in a certain metric space. Due to error tolerant property of a Fuzzy IBE scheme it is possible to use biometric identities, which inherently have noise. This scheme is both error-tolerant and secure against collusion attack. Since it allows aggregation of identities in a certain metric space, it does not provide much flexibility for constant size key aggregation which provides constant size cipher text.

2.2 Attribute-Based Encryption (ABE)

ABE is an effective technique that provides fined-grained access control to data in the cloud. Initially Access Control Lists (ACL) was used but it was not scalable and provided only coarse-grained access to data. ABE was first proposed buy Goyal et al. [6] which is more scalable and provide fined-grained data access control. In Attribute-Based Encryption user or piece of data has attributes associated with it and user is granted if and only if the attributes satisfy the access control policy. There are two kinds of ABE

2.2.1 Key-Policy Attribute Based Encryption (KP-ABE)

Private key is associated with access control policy and the attributes are stored with data.

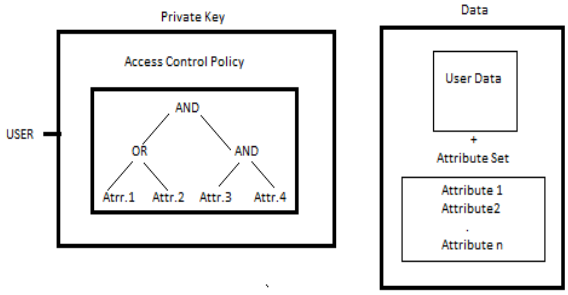

Figure 2: Key-Policy Attribute Based Encryption (KP-ABE)

2.2.2 Cipher text-Policy Attribute Based Encryption (CP-ABE)

It is converse of KP-ABE. Private key is associated with attributes and access control policies are stored with data**.**

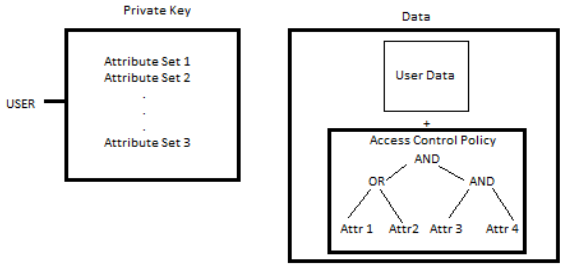

Figure 2: Ciphertext-Policy Attribute Based Encryption (KP-ABE)

In 2012, Tu et al. [7] developed system to establish access control for the encrypted data using Cipher text-Policy Attribute-Based Encryption. In this work a department distributes a secret key and revoking their access rights when they are no longer authorized to access the encrypted data. To ensure this, the data is re-encrypted in the cloud thus making revoked user's key useless. Main advantage of this scheme is that it is semantically secure against chosen cipher text attacks(CCA).However, this scheme places heavy computation overhead in case of user revocation due to updating of cipher texts.

In 2013, Li et al. [8] leverages Attribute-based Encryption techniques to enable secure sharing of personal health records (PHR) in the cloud. This work focuses on the multiple data owner scenario and divides the users based on their professional role. With respect to access control this scheme specifies role-based fine-grained access control policies for their Personal Health Records. This scheme is effective because it does not require data owner to be online at all times and greatly reduces key management complexity for owner and users as the owner do not have to manage keys for each individual user.

2.3 Proxy Re-encryption Scheme

It is a semi-trusted proxy with a re-encryption key which works as follows:-
Suppose there is Alice (data owner) who encrypts data m with her public key. When she wants to share her data with Bob, she sends encrypted data into another cipher text that can be decrypted by Bob's secret key. Main benefit of this scheme is, at no stage proxy will be able to access the plaintext.

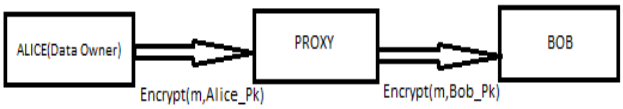

Figure 3: Proxy Re-encryption Scheme

In 2011, Tran at al. [9] developed a system based on Proxy Re-encryption scheme where the data owner's private key is divided into two parts; one half is stored on data owner's machine while the other is stored in the cloud proxy. The data is first encrypted with half of data owner's private key and again encrypted by the proxy using his other half of the key. The user who has been granted access rights will retrieve the data as proxy will decrypt the cipher text with half the user's private key and then complete plain text can be retrieved with decryption performed again at user's side. When data owner wishes to revoke user's access rights he informs the cloud proxy to remove user's key. The main strength is it does not require re-encryption every time when user's access rights are revoked and hence saves computation costs. Main drawback is this scheme suffers from collusion attacks i.e. if access rights of revoked user and proxy collude, then the revoked user has access to all other user's private key in the group. Proxy also suffers from too many encryption and decryption operations.

In 2013, Leng at al. [10] developed a system that allows patients to specify fine-grained access control policy. For enforcing sticky policies and to provide users with write privileges for PHRs it utilized Conditional Proxy Re-Encryption. Whenever users finished updating PHRs, they signed PHRs using signature key of the PHR owner and hence difficult to verify who signed the PHRs, thus creating

authentication problem.

In 2012, Chen et al. [11] proposed an EHR system based on smart cards and RSA.This system enables patients to store medical records on hybrid clouds. In this system two usage cases are discussed: first, medical records are accessed by doctors who created the records and second, medical records are accessed by other hospitals that have to seek permission from data owners. Authors also discuss solution for emergency situations. Main shortcoming of this approach is it places heavy computational overhead on data owners.

2.4 Hybrid ABE and PRE

ABE and PRE scheme can be used together to enhance security and privacy for data sharing and collaboration in cloud.

In 2010, Yu et al. [12] was first work which combined Attribute Based Encryption and Proxy Re-encryption for Cloud data security. In this scheme the data owner encrypts his data using a symmetric key and then again encrypts the symmetric key using Key Policy-Attribute Based Encryption scheme. When a new user joins the system data owner assigns secret key. When a user is revoked it updates access structure of that user so that it can no longer access the data and at the same time remaining users secret keys will also be updated. Main benefit of this scheme is use of proxy re-encryption that does not require data owner to be online to provide key updates and most of the computational burden is delegated to the cloud. In addition to this, data confidentiality is ensured since data is stored in encrypted form. Main drawback is that this scheme is slower.

In 2014, Kuo at al. [13] developed a patient-centric access control scheme that ensures confidentiality of personal health records (PHR), integrity of personal health records (PHR), authenticity of personal health records (PHR), fine grained access control and revocation of access control. To achieve these objectives this proposed scheme uses Conditional Proxy Re-Encryption, the Advanced Encryption Standard and the RSA algorithm. This scheme provides flexibility with respect to key management and an efficient encryption policy. Limitations of this scheme are proxy suffers from too many encryption and decryption operations hence it is slower. It also suffers from collusion attacks.

A Synopsis of above discussed Secure Data Sharing methods is done below:

Table 1: Gives synopsis of different approaches used for secure data sharing and collaboration with their benefits and limitations.

Author	*Method*	*Benefits*	*Limitations*
F. Guo, Y. Mu, and Z. Chen[4] (2007)	Identity Based Encryption (IBE) with key aggregation	Multiple cipher texts can be decrypted using a single private key	Key aggregation cost is O (n) sizes for both cipher texts and public parameter. This increases storage and transmission cost of cipher texts, which is not suitable for cloud.
A. Sahai and B. Waters [5] (2005)	Fuzzy Identity Based Encryption (IBE)	This scheme is both error-tolerant and secure against collusion attack	It does not provide much flexibility for constant size key aggregation which provides constant size cipher text.

Tu S, Niu S, Li H, Xiao-ming Y, Li M [7] (2012)	Attribute Based Encryption(ABE)	It is semantically secure against chosen cipher text attacks (CCA).	This scheme places heavy computation overhead in case of user revocation due to updating of cipher texts.
Li M, Yu S, Zheng Y, Ren K, Lou W [8] (2013)	Attribute Based Encryption (ABE) that focuses on the multiple data owner scenario.	It does not require data owner to be online at all times. Greatly reduces key management complexity since it is based on role based ABE	-
Tran DH, Nguyen HL, Zha W, Ng WK [9] (2011)	Proxy Re-encryption scheme	It does not require re-encryption every time when user's access rights are revoked and hence saves computation costs.	This scheme suffers from collusion attacks. Proxy also suffers from too many encryption and decryption operations.
Leng, C., Yu, H., Wang, J., & Huang, J.[10] (2013)	Conditional Proxy Re-Encryption scheme	Provides users with write privileges for PHRs	Authentication Problem: Whenever users finished updating PHRs,they signed PHRs using signature key of the PHR owner and hence difficult to verify who signed the PHRs
Chen, Y. Y., Lu, J. C., & Jan, J. K.[11] (2012)	Proxy Re-Encryption scheme.	Enables patients to store medical records on hybrid clouds Provides solution for emergency situations.	Places heavy computational overhead on data owners.

Yu S,Wang C, Ren K, LouW [12] (2010)	Hybrid ABE and PRE	It does not require data owner to be online to provide key updates Most of the computational burden is delegated to the cloud.	This scheme is slower
Kuo-Hsuan Huang,En-Chi Chang,Shao-Jui Wang [13] (2014)	Hybrid ABE and PRE	Provides efficient system to allows patients to control their personal health records (PHR) based on a patient centric access control scheme approach.	Proxy suffers from too many encryption and decryption operations hence it is slower. It suffers from collusion attacks. Large key size(total number of keys=total number of cipher texts)

Conclusion

The paper defines the approaches and the previous work regarding the secure sharing in Cloud Computing. Auditing and Accountability in the Cloud can be the future research area. Throughout this paper we have assumed that members of group will not carry out any malicious activities, so future direction would be to design model to prevent and handle this situation. Another future direction would be to associate data with its access control policy. This will prevent overhead of accountability and if any member tries to make illegal copies of data then access control will lock the data.

References

[1] HealeyM "Why IT needs to push data sharing efforts", InformationWeek. Source: http:// www.informationweek.com /services/integration/why-it-needs-to-push-data-sharing-effort/ 225700544. [Accessed on Oct 2012].
[2] Wu R, "Secure sharing of electronic medical records in cloud computing". Arizona State University, ProQuest Dissertations and Theses, 2012.
[3] Zhou M, Zhang R, XieW, QianW, Zhou "A Security and privacy in cloud computing: a survey". Sixth international conferences on semantics knowledge and grid (SKG) pp. 105–112, 2010.
[4] F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How to Decrypt Multiple Cipher texts Using a Single Decryption Key," in Proceedings of Pairing-Based Cryptography (Pairing '07), ser. LNCS, vol. 4575. Springer, pp. 392–406, 2007.
[5] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Proceedings of Advances in Cryptology - EUROCRYPT '05, ser. LNCS, vol. 3494. Springer, pp. 457–473, 2005.
[6] Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute-based encryption for fine-grained access control of encrypted data. 13th ACM conference on computer and communications security (CCS '06), pp 89–98, 2006.
[7] Tu S, Niu S, Li H, Xiao-ming Y, Li M " Fine-grained access control and revocation for Sharing data on clouds",IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW) 2012, pp. 2146–2155.
[8] Li M, Yu S, Zheng Y, Ren K, Lou W, " Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption". IEEE Trans Parallel Distributed System pp. 131–143, 2013.
[9] Tran DH, Nguyen HL, Zha W, Ng WK, "Towards security in sharing data on cloud based social networks. 8th International conference on information, communications and signal processing (ICICS), pp. 1–5, 2011.
[10] Leng, C., Yu, H., Wang, J., & Huang, J. "Securing Personal Health Records in the Cloud by Enforcing Sticky Policies," TELKOMNIKA Indonesian Journal of Electrical Engineering, 11(4), 2200-2208, 2013.
[11] Chen, Y. Y., Lu, J. C., & Jan, J. K. "A secure EHR system based on hybrid clouds," Journal of medical systems, 36(5), 3375-3384, 2012.
[12] Yu S, Wang C, Ren K, LouW "Achieving secure, scalable and fine-grained data access control in cloud

computing". In INFOCOM, 2010 proceedings IEEE, pp. 1–9, 2010.

[13] Kuo-Hsuan Huang, En-Chi Chang, Shao-Jui Wang,"A Patient-Centric Access Control Scheme for Personal Health Records in the Cloud", Fourth International Conference on Networking and Distributed Computing, 2014.

Author Profile

Prajakta Narayan Solapurkar is pursuing M.E in the Computer Department at Pune Institute of Computer Technology, Pune. She has done B.E from PES Modern College of Engineering, under Pune University, India.

Professor **Girish Potdar** is Vice Principal and HOD of Computer Department at Pune Institute of Computer Technology in Pune, India.