Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption

SHRUTI CHAUHAN[1], DR. S. DEEPAJOTHI[2], M. SREENU[3]
[1]PG Scholar, Dept of CSE, Ashoka Institute Of Engineering & Technology, India,
[2]HOD, Dept of CSE, Ashoka Institute Of Engineering & Technology, India
[3]Professor, Dept of CSE, Ashoka Institute Of Engineering & Technology, India,

Abstract: Distributed computing gives an adaptable and helpful path for information sharing, which brings different advantages for both the general public and people. In any case, there exists a characteristic protection for clients to straightforwardly outsource the common information to the cloud server since the information frequently contain significant data. Therefore, it is important to put cryptographically upgraded get to control on the mutual information. Character based encryption is a promising cryptographical primitive to fabricate a down to earth information sharing framework. In any case, get to control isn't static. That is, the point at which some client's approval is lapsed, there ought to be a component that can expel him/her from the framework. Thusly, the renounced client can't get to both the already and consequently shared information. To this end, we propose a thought called revocable-capacity personality based encryption (RS-IBE), which can give the forward/in reverse security of ciphertext by presenting the functionalities of client repudiation and ciphertext refresh at the same time. Besides, we show a solid development of RS-IBE, and demonstrate its security in the characterized security display. The execution examinations demonstrate that the proposed RS-IBE conspire has focal points regarding usefulness and proficiency, and hence is attainable for a handy and practical information sharing framework. At long last, we give execution after effects of the proposed plan to exhibit its practicability.

Keywords*:* Cloud Computing, Data Sharing, Revocation, Identity-Based Encryption, Ciphertext Update, Decryption Key Exposure.

I. INTRODUCTION

Cloud computing is a paradigm that provides massive computation capacity and huge memory space at a low cost [1]. It enables users to get intended services irrespective of time and location across multiple platforms (e.g., mobile devices, personal computers), and thus brings great convenience to cloud users. Among numerous services provided by cloud computing, cloud storage service, such as Apple'si Cloud [2], Microsoft's Azure [3] and Amazon's S3 [4], can offer a more flexible and easy way to share data over the Internet, which provides various benefits for our society [5],[6]. However, it also suffers from several security threats, which are the primary concerns of cloud users [7].Firstly, outsourcing data to cloud server implies that data is out control of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information. Secondly, data sharing is often implemented in an open and hostile environment, and cloud server would become a target of attacks. Even worse, cloud server itself may reveal users' data for illegal profit. Thirdly, data sharing is not static. That is, when a user's authorization gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data. A natural solution to conquer the aforementioned problem is to use cryptographically enforced access control such as identity-based encryption (IBE). Furthermore, to overcome the above security threats, such kind of identity-based access control placed on the shared data should meet the following security goals:

- **Data Confidentiality:** Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data.
- **Backward Secrecy:** Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.
- **Forward Secrecy:** Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her.

The specific problem addressed in this paper is how to construct a fundamental identity-based cryptographical tool to achieve the above security goals. We also note that there exist other security issues that are equally important for a practical system of data sharing, such as the authenticity and availability of the shared data [8], [9], [10], [11], [12].But the research on these issues is beyond the scope of this paper.

II. MOTIVATION

It seems that the concept of revocable identity-based encryption(RIBE) might be a promising approach that fulfills aforementioned security requirements for data sharing. RIBE features a mechanism that enables a sender to append the current

time period to the ciphertext such that the receiver can decrypt the ciphertext only under the condition that he/she is not revoked at that time period. As indicated in Fig.1, a RIBE-based data sharing system works as follows:

Step 1: The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the ciphertext of the shared data to the cloud server.

Step 2: When either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding ciphertext. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.

Step 3: In some cases, e.g., Alice's authorization gets expired, David can download the ciphertext of the shared data, and then decrypt-then-re-encrypt the shared data such that Alice is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

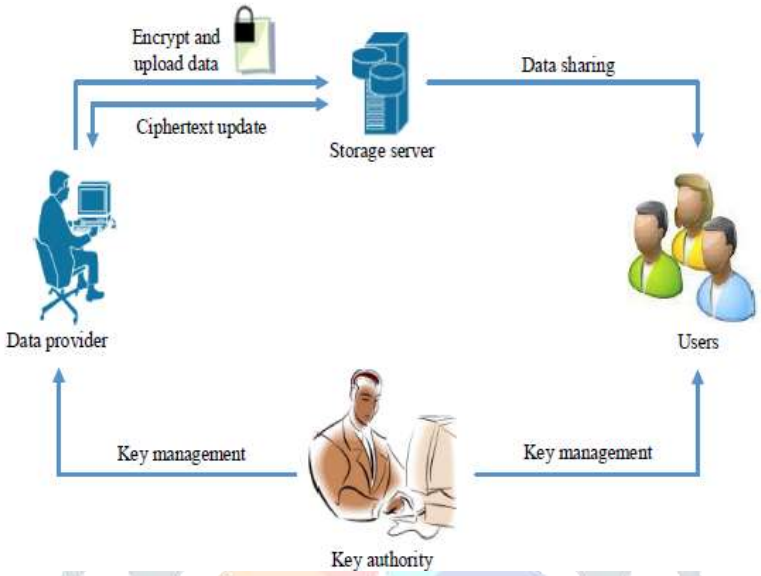

Fig.1. A natural RIBE-based data sharing system.

Obviously, such a data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new challenges. Note that the process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, the use of secret key should be limited to only usual decryption, and it is inadvisable to update the ciphertext periodically by using secret key. Another challenge comes from efficiency. To update the ciphertext of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-reencrypt-upload. This process brings great communication and computation cost, and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage. One method to avoid this problem is to require the cloud server to directly re-encrypt the ciphertext of the shared data. However, this may introduce ciphertext extension, namely, the size of the ciphertext of the shared data is linear in the number of times the shared data have been updated. In addition, the technique of proxy re-encryption can also be used to conquer the aforementioned problem of efficiency. Unfortunately, it also requires users to interact with the cloud server in order to update the ciphertext of the shared data.

III. RELATED WORK

A. Revocable Identity-Based Encryption

The concept of identity-based encryption was introduced by Shamir [13], and conveniently instantiated by Boneh and Franklin [14]. IBE eliminates the need for providing a public key infrastructure (PKI). Regardless of the setting of IBE or PKI, there must be an approach to revoke users from the system when necessary, e.g., the authority of some user is expired or the secret key of some user is disclosed. In the traditional PKI setting, the problem of revocation has been well studied [15], [16], [17], [18], [19], and several techniques are widely approved, such as certificate revocation list or appending validity periods to certificates. However, there are only a few studies on revocation in the setting of IBE. Boneh and Franklin [14] first proposed a natural revocation way for IBE. They appended the current time period to the cipher text, and non-revoked users periodically received private keys for each time period from the key authority. Unfortunately, such a solution is not scalable, since it requires the key authority to perform linear work in the number of non-revoked users. In addition, a secure channel is essential for the key authority and non-revoked users to transmit new keys. To conquer this problem, Boldyreva, Goyal and Kumar [20] introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users. However, this scheme only achieves selective security. Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud [21] proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme [22], Chenet al. [23] constructed a RIBE scheme from lattices. Recently, Seo and Emura [24] proposed an efficient RIBE scheme resistant to a realistic threat called

decryption key exposure, which means that the disclosure of decryption key for current time period has no effect on the security of decryption keys for other time periods. Inspired by the above work and [25], Liang et al. [26] introduced a cloud-based revocable identity-based proxy re-encryption that supports user revocation and ciphertext update. To reduce the complexity of revocation, they utilized a broadcast encryption scheme [27] to encrypt the ciphertext of the update key, which is independent of users, such that only non-revoked users can decrypt the update key. However, this kind of revocation method cannot resist the collusion of revoked users and malicious non-revoked users as malicious non revoked users can share the update key with those revoked users. Furthermore, to update the ciphertext, the key authority in their scheme needs to maintain a table for each user to produce the re-encryption key for each time period, which significantly increases the key authority's workload.

B. Forward-Secure Cryptosystems

In 1997, Anderson [28] introduced the notion of forward security in the setting of signature to limit the damage of key exposure. The core idea is dividing the whole lifetime of a private key into T discrete time periods, such that the compromise of the private key for current time period can not enable an adversary to produce valid signatures for previous time periods. Subsequently, Bell are and Miner provided formal definitions of forward-secure signature and presented practical solutions. Since then, a large number off or ward-secure signature schemes [29], [30], [31], [32], [33]has been proposed. In the context of encryption, Canetti, Halevi and Katz[34] proposed the first forward-secure public-key encryption scheme. Specifically, they firstly constructed a binary tree encryption, and then transformed it into a forward-secure encryption with provable security in the random oracle model. Based on Canetti et al's approach, Yao et al. [35]proposed a forward-secure hierarchical IBE by employing two hierarchical IBE schemes, and Nieto et al. [36] designed a forward-secure hierarchical predicate encryption. Particularly, by combining Boldyreva et al.'s [20] revocation technique and the aforementioned idea of forwardsecurity1, in CRYPTO 2012 Sahai, Seyalioglu and Waters[37] proposed a generic construction of so-called revocable storage attribute-based encryption, which supports user revocation and ciphertext update simultaneously. In other words, their construction provides both forward and backward secrecy. What must be pointed out is that the process of ciphertext update of this construction only needs public information. However, their construction cannot be resistant to decryption key exposure, since the decryption is a matching result of private key and update key.

C. Our Contributions

In this paper, we introduce a notion called revocable storage identity-based encryption (RS-IBE) for building a cost-effective data sharing system that fulfills the three security goals. More precisely, the following achievements are captured in this paper:

- We provide formal definitions for RS-IBE and its corresponding security model;
- We present a concrete construction of RS-IBE. The proposed scheme can provide confidentiality and backward/forward2 secrecy simultaneously;
- We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure;
- The proposed scheme is efficient in the following ways:
  - The procedure of ciphertext update only needs public information. Note that no previous identity-based encryption schemes in the literature can provide this feature;
  - The additional computation and storage complexity, which are brought in by the forward secrecy, is all upper bounded by O(log(T)2),where T is the total number of time periods.

D. KUNodes algorithm

Our RS-IBE scheme uses the same binary tree structure introduced by Boldyreva, Goyal and Kumar [20] to achieve efficient revocation. To describe the revocation mechanism, we first present several notations. Denote by ε the root node of the binary tree BT , and Path(η) the set of nodes on the path from ε to the leaf node η (including ε and η). For anon-leaf node θ, we let θ_l and θ_r stand for its left and right child, respectively. Given a time period t and revocations list RL, which is comprised of the tuples (η_i, ti) indicating that the node ηi was revoked at time period t_i, the algorithm KUNodes(BT ,RL, t) outputs the smallest subset Y of nodes of BT such that Y contains an ancestor for each node that is not revoked before the time period t.

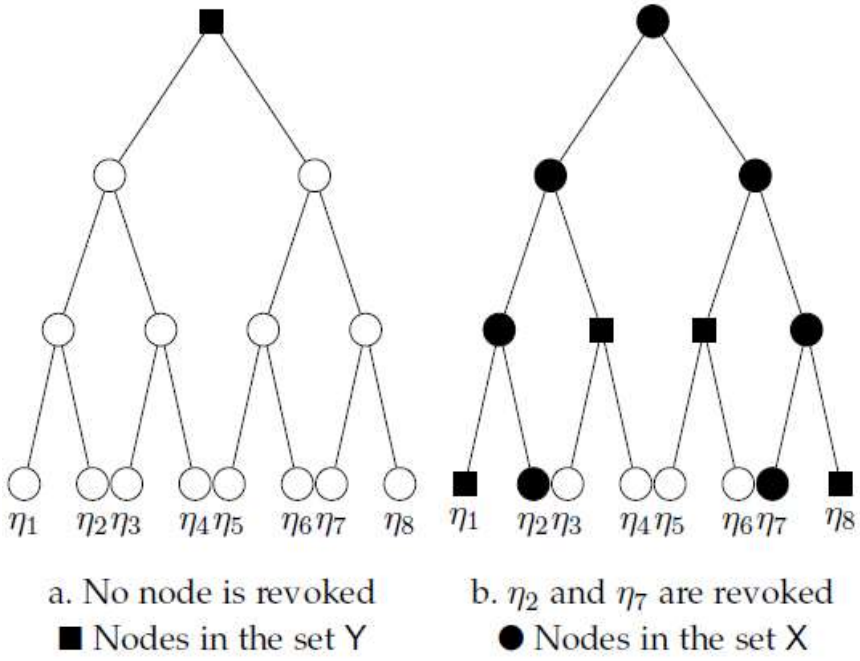

Fig. 2. An instance of the algorithm KUNodes.

Informally, to identify the set Y, the algorithm first marks all the ancestors of revoked nodes as revoked, then outputs all the non-revoked children of revoked nodes. As an example, we present two instances of the algorithm KUNodes in Fig.2. The formal description is given below.

Algorithm 1 KUNodes($\mathcal{BT}, RL, t$)

```
1: X,Y ← ∅
2: for all (η_i, t_i) ∈ RL do
3:    if t_i ≤ t then
4:       Add Path(η_i) to X
5:    end if
6: end for
7: for all θ ∈ X do
8:    if θ_l ∉ X then
9:       Add θ_l to Y
10:   end if
11:   if θ_r ∉ X then
12:      Add θ_r to Y
13:   end if
14: end for
15: if Y = ∅ then
16:    Add the root node ε to Y
17: end if
18: return Y
```

IV. RESULTS

Results of this paper is as shown in bellow Figs.3 to 8.

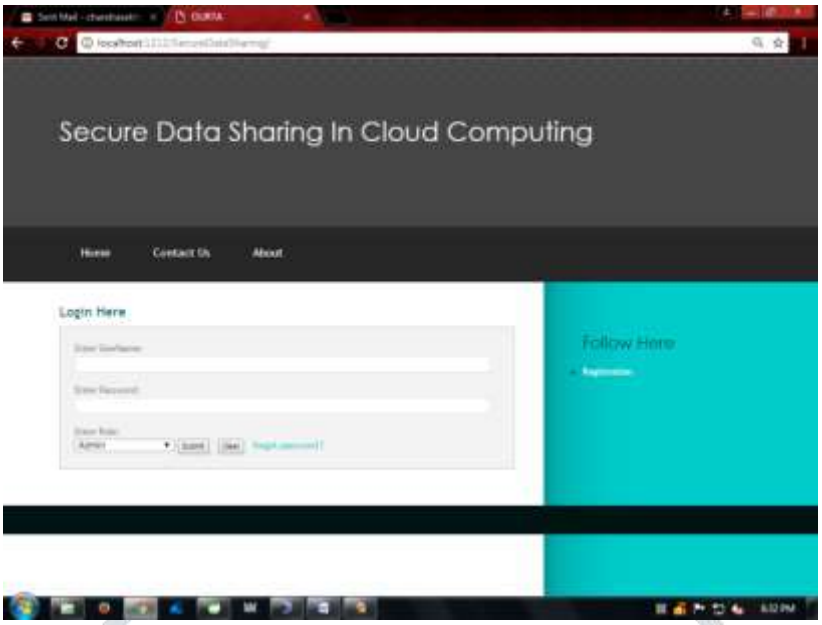

Fig.3. Login Page.

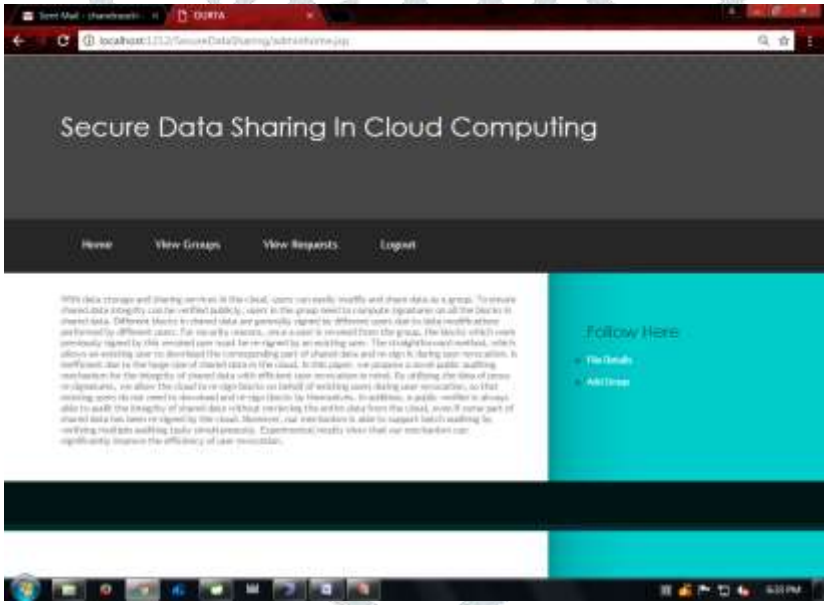

Fig.4. Admin Home Page.

Fig.5. User Home Page.

User can able to upload the file and can download the file.

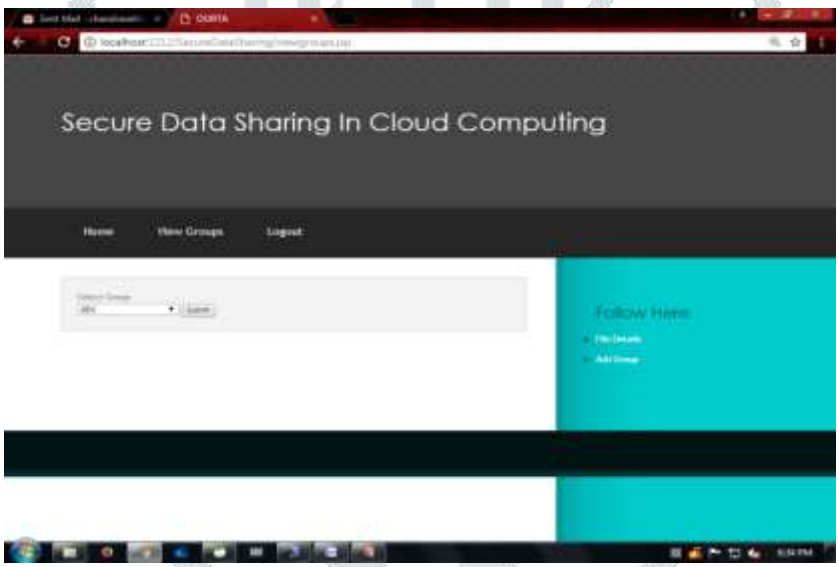

Fig.6. Admin View Groups.

Admin can select the group name and can able to view the group members.

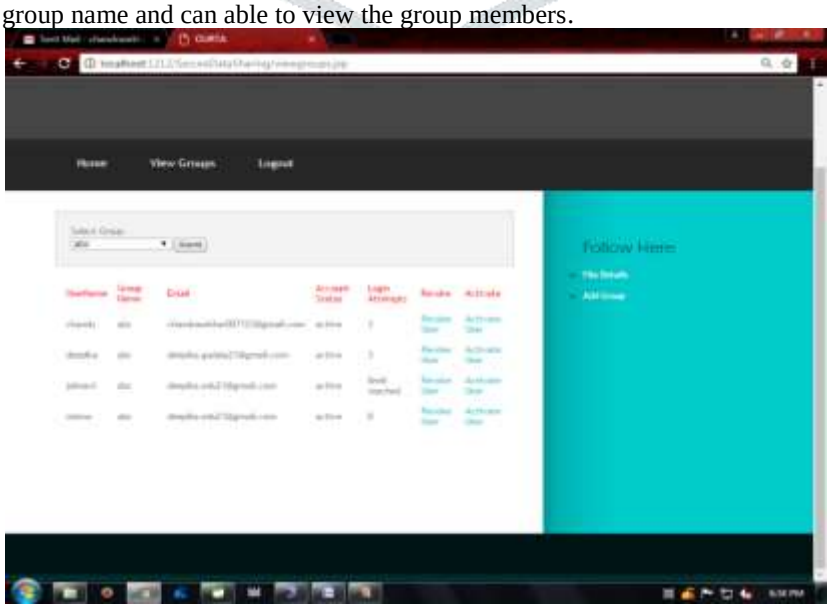

Fig.7. Group Details.

When the admin was select the group then it is showing group details.

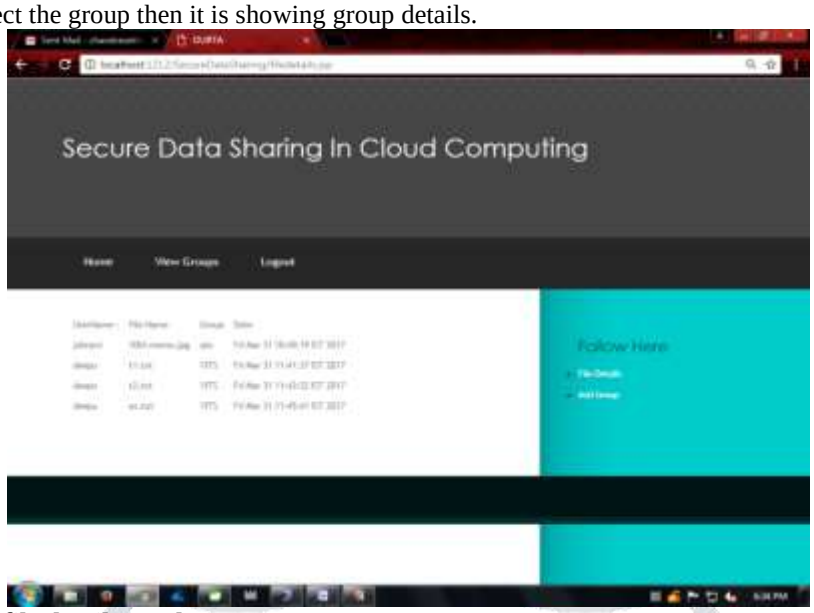

Fig.8. This will shows the file details in admin page.

VI. CONCLUSION

Distributed computing brings awe inspiring accommodation for people. Especially, it splendidly coordinates the expanded want of sharing data over the net. during this paper, to assemble a savvy and secure data sharing framework in distributed computing, we tend to projected an inspiration known as RS-IBE, that underpins temperament denial and ciphertext refresh at identical time with the tip goal that a denied consumer is unbroken from reaching to beforehand shared data, and in addition on these lines shared data. Moreover, a solid development of RS-IBE is introduced. The projected RS-IBE plot is incontestable versatile secure within the commonplace model, below the decisional ℓ-DBHE presumption. The correlation results exhibit that our arrange has preferences as so much as productivity and utility, and consequently is additional gettable for right down to earth applications.

VII. REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "Abreak in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.
[2] iCloud. (2014) Apple storage service. [Online]. Available:https://www.icloud.com/
[3] Azure. (2014) Azure storage service. [Online]. Available:http://www.windowsazure.com/
[4] Amazon. (2014) Amazon simple storage service (amazon s3).[Online]. Available: http://aws.amazon.com/s3/
[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloudcomputing: A vision for socially motivated resource sharing,"Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563,2012.
[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreservingpublic auditing for secure cloud storage," Computers,IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.
[7] G. Anthes, "Security in the cloud," Communications of the ACM,vol. 53, no. 11, pp. 16–18, 2010.
[8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocolfor data storage in cloud computing," Parallel and DistributedSystems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.
[9] B. Wang, B. Li, and H. Li, "Public auditing for shared datawith efficient user revocation in the cloud," in INFOCOM, 2013Proceedings IEEE. IEEE, 2013, pp. 2904–2912.
[10] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized accesscontrol with anonymous authentication of data stored in clouds,"Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2,pp. 384–394, 2014.
[11] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, andJ. Zhou, "Cost-effective authentic and anonymous data sharingwith forward security," Computers, IEEE Transactions on, 2014, doi:10.1109/TC.2014.2315619.
[12] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng,
"Key-aggregate cryptosystem for scalable data sharing in cloudstorage," Parallel and Distributed Systems, IEEE Transactions on,vol. 25, no. 2, pp. 468–477, 2014.
[13] A. Shamir, "Identity-based cryptosystems and signature schemes,"in Advances in cryptology. Springer, 1985, pp. 47–53.
[14] D. Boneh and M. Franklin, "Identity-based encryption from theweil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.
[15] S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.[16] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identityrevocation," in Advances in Cryptology–CRYPTO 1998. Springer,1998, pp. 137–152.
[17] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracingschemes for stateless receivers," in Advances in Cryptology–CRYPTO 2001. Springer, 2001, pp. 41–62.
[18] C. Gentry, "Certificate-based encryption and the certificate revocationproblem," in Advances in Cryptology–EUROCRYPT 2003.Springer, 2003, pp. 272–293.

[19] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security.Springer, 2007, pp. 247–259.
[20] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryptionwith efficient revocation," in Proceedings of the 15th ACM conferenceon Computer and communications security. ACM, 2008, pp. 417–426.
[21] B. Libert and D. Vergnaud, "Adaptive-id secure revocable identitybasedencryption," in Topics in Cryptology–CT-RSA 2009. Springer,2009, pp. 1–15.
[22] "Towards black-box accountable authority ibe with short ciphertexts and private keys," in Public Key Cryptography–PKC2009. Springer, 2009, pp. 235–255.
[23] J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, "Revocable identity-based encryption from lattices," in Information Security andPrivacy. Springer, 2012, pp. 390–403.
[24] J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction," in Public-Key Cryptography–PKC 2013. Springer, 2013, pp. 216–234.
[25] "Efficient delegation of key generation and revocation functionalities in identity-based encryption," in Topics in Cryptology–CT-RSA 2013. Springer, 2013, pp. 343–358.
[26] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud based revocable identity-based proxy re-encryption scheme forpublic clouds data sharing," in Computer Security-ESORICS 2014.Springer, 2014, pp. 257–272.
[27] D.-H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler, "Adaptive cca broadcast encryption with constant-size secret keysand ciphertexts," International journal of information security, vol. 12,no. 4, pp. 251–265, 2013.
[28] R. Anderson, "Two remarks on public-key cryptology (invitedlecture)," 1997.
[29] M. Bellare and S. K. Miner, "A forward-secure digital signaturescheme," in Advances in Cryptology–CRYPTO 1999. Springer, 1999,pp. 431–448.
[30] M. Abdalla and L. Reyzin, "A new forward-secure digital signaturescheme," in Advances in Cryptology–ASIACRYPT 2000.Springer, 2000, pp. 116–129.

Author's Details:

SHRUTI CHAUHAN (STUDENT) Department of CSE with ASHOKA INSTITUTE OF ENGINEERING & TECHNOLOGY. shrutichauhan94@gmail.com

MRS. DEEPA JOTHI, PhD (CSE)from ANNA University-Chennai. Having experience of 10 years in Teaching. She is currently working as Head of Department of CSE with ASHOKA INSTITUTE OF ENGINEERING & TECHNOLOGY. M.E.(CSE)from ANNA UNIVERSITY-2009, B.E(CSE)from ANNA UNIVERSITY-2007 **deepjothi.a@gmail.com**

MR. M SREENU, PhD (CS) pursuing from Hyderabad Central University. Having experience of 13 years in Teaching and 21/2 years in R&D. He is currently working as a professor in Department of CSE with ASHOKA INSTITUTE OF ENGINEERING & TECHNOLOGY. M.Tech.(CSE) from Osmania University-2006, B.Tech.(CSE) from Kakatiya University-2000. **pittunaik723@gmail.com**