International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 23 Issue 8 –NOVEMBER 2016.

IDENTITY BASED PROXY RE-ENCRYPTION ALGORITHM FOR SECURE DATA SHARING MODEL IN CLOUD COMPUTING

Naveen Kumar C.G[#1] and Dr.SanjayPande.M.B[*2]

[#] *Research Scholar, Department of Computer Science, Bharathiar University, Coimbatore, India.*

[*] *Professor& Principal, Sampoorna Institute of Technology & Research, Ramanagar, Karnataka, India.*

***Abstract*— Cloud computing is rapidly growing due to the provisioning of elastic, flexible, and on-demand storage and computing services for users. In cloud based storage concept, data owner does not have full control over own data because data controlled by the third party called cloud service providers (CSP). Data security is challenging problem when data owner shares own data to another known as data sharer on cloud. Many researchers have addressed this issue by cryptography with different encryption schemes that provides secure data sharing on cloud. In this paper, we design a secure data sharing model for data service to provide confidentiality and fine-grained access control for data stored in the cloud using identity based proxy re-encryption algorithm. This mechanism enables the cloud users to enjoy a secure outsourced data services at a minimized security management overhead. The main idea of secure data sharing model is to outsource not only the data but also the security management to the cloud in a trust manner.**

Index Terms*— *Cloud Computing, Data security, Cloud Service Providers (CSP), Secure data Sharing model, and Identity based proxy re-encryption

I. INTRODUCTION

Cloud Computing is the result of evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them [1]. The cloud aims to cut costs, and help the users focus on their core business instead of being impeded by IT obstacles. Cloud computing as a fast growing technology provides many scalable services. It moves user's data to the centralized large data centers, where the management of the data and services may not be fully trustworthy. Users may not know the machines which actually process and host their data in a cloud environment. Users also start worrying about losing control of their own data. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. Such fears are becoming a significant to the wide adoption of cloud services [2]. It is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. For example, users need to be able to ensure that their data are handled according to the service level agreements made at the time they sign on for services in the cloud.

Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in distributed environments, are not suitable, due to the following features characterizing cloud environments [3]. First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also delegate the tasks to others, and so on [4]. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments. Some of major requirements of secure data sharing in the Cloud are as follows. Firstly the data owner should be able to specify a group of users that are allowed to view his or her data [5-6]. Any member within the group should be able to gain access to the data anytime, anywhere without the data owner's intervention. No-one, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider. The data owner should be able to add new users to the group [7,8 and 9]. The data owner should also be able to revoke access rights against any member of the group over his or her shared data [10]. No member of the group should be allowed to revoke rights or join new users to the group. One trivial solution to achieving secure data sharing in the Cloud is for the data owner to encrypt his data before storing into the Cloud, and hence the data remain information-theoretically secure against the Cloud provider and other malicious users. When the data owner wants to share his data to a group, he sends the key used for data encryption to each member of the group. Any member of the group can then get the encrypted data from the Cloud and decrypt the data using the key and hence does not require the intervention of the data owner [11]. However, the problem with this technique is that it is computationally inefficient and places too much burdenon the

data owner when considering factors such as user revocation. When the data owner revokes access rights to a member of the group, that member should not be able to gain access to the corresponding data. Since the member still has the data access key, the data owner has to re-encrypt the data with a new key, rendering the revoked member's key useless [12-13]. Moreover one user may possess many attribute and conversely one attributes may be possessed by many users which makes the data owner difficult to set up the correspondence between the users and attributes. These observations motivate us to propose a novel data sharing mechanism in cloud computing.

In this work, we propose secure data sharing model, a user-efficient and secure data sharing mechanism in cloud computing, which enables the users to enjoy a secure outsourced data services at a minimized security management overhead. To achieve this, we adopt an identity-based proxy re-encryption scheme which allows a cloud user to encrypt his data under his identity to protect his data from leaking and, at the same time, to delegate his data management capability to the cloud. Furthermore the cloud user could delegate his access control capability to the cloud, which could grant the access of an authorized user by transforming the cipher extencrypted with the data owner's identity to the one with the sharer's identity.

II. LITERATURE SURVEY

This section aims to present a summary of existing review articles related to secure data sharing in the Cloud. The review articles and surveys presented in this section focus specifically on secure data sharing in the Cloud. The study of secure data sharing in the Cloud is fairly new and has become increasingly important with the advancements and growing popularity of the Cloud as well as the growing need to share data between people. We categorise the existing review articles in two aspects: data sharing and Cloud security.There have been a number of reviews on security and privacy in the Cloud.

Xiao and Xiao [14] identifies the five concerns of Cloud computing; confidentiality ,integrity, availability, accountability, and privacy and thoroughly reviews the threats to each of the concerns as well as defense strategies. Chen and Zhao [15] outlines the requirements for achieving privacy and security in the Cloud and also briefly outlines the requirements for secure data sharing in the Cloud. Zhou [16] provided a survey on privacy and security in the Cloud focusing on how privacy laws should also take into consideration Cloud computing and what work can be done to prevent privacy and security breaches of one's personal data in the Cloud.

Wang et al. [17] explored factors that affect managing information security in Cloud computing. It explains the necessary security needs for enterprises to understand the dynamics of information security in the Cloud. Wang [18] carried out a study on the privacy and security compliance of Software-As-A-Service (SaaS) among enterprises through pilot testing privacy/security compliance. They then carry out analysis work on the measurements to check whether SaaS complies with privacy and security standards. The method does not however take into account other Cloud models such as Platform-As-A-Service (PaaS) and in particular Infrastructure-As-A-Service (IaaS), as needed for data sharing.

Oza et al. [19] carried out a survey on a number of users to determine the user experience of Cloud computing and found that the main issue of all users was

trust and how to choose between different Cloud Service Providers. This is also highlighted in [12] as it states, "Although researchers have identified numerous security threats to the Cloud, malicious insiders still represent a significant concern." There are many examples [13] of insider attacks such as Google Docs containing a flaw that inadvertently shared user documents, MediaMax going out of business in 2008 after losing 45 % of stored client data due to administrator error, Salesforce.com leaking a customer list and falling victim to phishing attacks on a number of occasions. It's clear from many of the reviews, that the Cloud is very susceptible to privacy andsecurity attacks and currently there is on-going research that aims to prevent and/orreduce the likelihood of such attacks.

The importance of data sharing and the need to ensure privacy and security isdiscussed in a number of existing articles. Saradhy and Muralidhar [20] review the impact of the Internet on data sharing across many different organisations such as government agencies and businesses. They classify data sharing into data dissemination, query restriction, and record matching. They also provide a framework for secure and useful sharing of data on the internet. Butler [21] describes the issues of data sharing on the Internet where sharing information can allow users to infer details about users. This is useful as it raises awareness to organisations that the data they choose to share with the public can still raise privacy issues and does not guarantee the confidentiality of its users. Mitchley [22] describes the benefits of data sharing from a banking perspective and highlights the privacy issues still affecting it. Feldman et al. [23] discuss the important benefit of data sharing in terms of public health, in particular for education and professional development. Geoghegan [24] discuss a list of organisations that effectively and secure share information via the Cloud. However, it doesn't discuss the methodologies the organisations use to secure data or the downside of these organisations. There is also literature that focus on oneaspect of security as well as data sharing; access control. Access control can be used

to authorise a subset of users to view confidential data provided they have the right permission.

Sahafizadeh and Parsa [25] survey a number of different access control models and evaluates its effectiveness. In [26], S. Yu, et al. exploit a novelcryptographic approach, key policy-attribute based encryption scheme (KP-ABE), to achieve the secure data outsourcing storage and access control in the semi-untrusted cloud servers, and also apply re-encryption scheme in revocation phase to reduce the cost of data owner. However, we argue that in a dynamic cloud, the ABE based approach may not be efficient to provide user access control due to frequent node revocations.

MdMozammil et al.[27], The mobile device is used for uploading, downloading and sharing of data butit has limited capacity of computation. so, when mobile user want to share

own mobile device data to another on cloud by secure way can follow the proposed solution by this researchers where data owner encrypts the data using blowfish algorithm which is fast and required small amount of memory which is suitable for mobile devices and sends it to cloud storage. The data owner sends email of encrypted file to the sharer then privately provide secret key to the data sharer. Sharer decrypt the file received in mail using secret key and get the original data

Uma et al. [28]: In Cloud computing, maintain data confidentiality, authentication and integrity is main problem when data sharing take place with another person on cloud. so, as per proposed solution by researchers message digest of plain text is signed by owner with RSA algorithm and plaintext message is encrypted by the public key of recipient. Recipient will decrypt the cipher text to plaintext with his private key, and from that compute the message digest code ,which is compare with the singed message digest code by owner if both are identical then signature is valid and data say data share securely. This technique solves the problem of data confidentiality, authentication and integrity.

Mazhar et al. [29]: For share data in group on cloud access control of user, forward and backward secrecy problem is comes which is solved by researchers. They have proposed SeDaSC methodology by introducing CS (cryptographic server), encryption/decryption operations are performed at the CS which is a trusted party in the SeDaSC. When user want to upload/ download the shared file on cloud comes along with own secret key provided by CS and CS will takes the appropriate actions on the plaintext/cipher text file. The proposed SeDaSC provides confidentiality of data, securely share data, access control of user and control the forward and backward access

The survey however, is limited to only software systems and does not take into consideration Cloud systems.

III. EXISTING SYSTEM

The use of Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in distributed environments, are not suitable, due to the two following reasons.

1. First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and theses entities can also delegate the tasks to others, and so on.
2. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments [24].

In one existing system the user's private data are sent to the cloud in an encrypted form, and the processing is done on the encrypted data. The output of the processing isde-obfuscated by the privacy manager to reveal the correct result[25][26]. However, the privacy manager provides onlylimited features in that it does not guarantee protection once the data are being disclosed.

A. Drawbacks from existing system given below:

1. The conventional access control approach must require any dedicated authentication and storage system.
2. The user cannot have the information regardingusage or access of data by other users.
3. Requires third-party services to complete the monitoring and focuses on lower level monitoring of system resources.

IV. PROPOSED SYSTEM

The network model is assumed to comprise of the following parties: data owners, cloud servers, and data sharers. Both of the data owners and data sharers have device to easily access the Internet. To protect data from leaking to the third party, data owner forwards the encrypted files on the cloud servers to either for sharing or for personal use. The data sharers, who want to access data files, will be authorized by the data owner to decrypt the file. Cloud servers are assumed to have abundant storage capacity and computation power and are assumed to be always online.

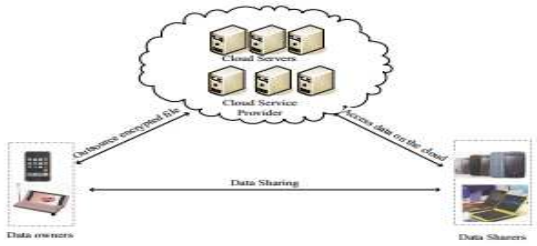

Fig.1 System Model

In this work, we mainly consider the threats from the semi-trusted cloud server in the data storing and malicious sharer in the data sharing. Similar to [24], we consider the cloud servers to be semi-trusted. That is to say, cloud servers will honestly implement the proposed protocol in general, but try to find out as much secret information as possible based on users' inputs. Malicious sharers may try to access the data without permission by data owner. The goal of our protocol is to guarantee that only authorized sharer can access the data and conversely unauthorized sharer will learn nothing. Moreover the collusion attack of the malicious sharers and the semi-trusted cloud servers should also be considered. In some cases, the collusion attack launched by the sharers and the cloud servers even corrupts the data owner's secret key, which should be strictly resisted in our mechanism.

Following the definition in cryptography, we assume the ability of the adversary A in our protocol could be adaptive. It means that the adversary A can gain some additional information to help them to compromise the system. In our protocol, each user entering the system has a unique identity and a secret key corresponding to his identity. The adversary A can corrupt some users' secret keys and manipulate the server to achieve some proxy re-encryption keys before he launches the attack. After the adversary A gets sufficient additional information, he will launch an attack. In the attack phase, the adversary A chooses one user id∗as his target goal. We will give some restrictions on choosing an attack target

id∗. The secret key of the attack target user id cannot be compromised by the attacker.

Our goals addressed in this paper are to achieve a secure data service mechanism of cloud users. We emphasize on the problem of confidentiality and access control of network users' outsourced data in the cloud circumstances. A solution to this problem should have the following requirements:

1. Protect the cloud users data from leaking to the cloud.
2. Guarantee the authorized sharers can access the data, while unauthorized sharers cannot learn anything about data.
3. Provide cloud users easy operations on setting and changing the access policies.
4. Reduce the communication cost of mobile user.

We present secure data sharing model to achieve the secure data management including the secrecy and data access control in the cloud computing. In our protocol, we will employ identity based proxy re-encryption to realize the secrecy of data. The proxy re-encryption scheme (PRE) [26], [27] is to allow a semi-trusted proxy to transform the data encrypted with Alice's public-key into the one encrypted with Bob's public key. The most natural application of PRE is in the transmission of Email to allow Bob to read Alice's encrypted emails while she is on vacation. In the mobile cloud computing, we employ the PRE to realize the access control of data and offers the following benefits:

1) Strong access control: Only authorized user can decrypt the data. Data owner can distinguish the identity information of sharers.

2) Flexibility: Our protocol is flexible to operate and scalable with the growth of data sharers. Data owner only need to forward a re-encryption key to cloud which can complete the transformation of ciphertext. No requiring classify the sharers in attributes by data owner makes our protocol easy to operation. Moreover, due to the lower cost of communication, our protocol is fit for the scalability of network.

3) Low overhead: The cost of achieve, change and update access policy is relatively lower.

Each user needs to register with an identity in the system and thus obtains the secret key corresponding to his identity. Cloud users explore IB-PRE encryption algorithm to encrypt the data which guarantees the data secrecy of the cloud service, and the ciphertext can be transformed to the one that could be decrypted by others in the future. Before encryption, the file F is divided into n blocks F = (m1, m2, · · · ,mn). For each block mi data owner encrypts it under his secret key. At the same time, data owner should generate the proxy re-encryption key to the authorized user. And different sharer's identity corresponding to different proxy re-encryption key is generated. The size of re-encryption key is almost similar to the size of a block mi in file F.

Given the proxy re-encryption key by the owner, the cloud can convert the ciphertext outsourced by the data owner to the ciphertext that can be decrypted by the sharer. As mentioned above, in our proposal the role of the cloud is twofold:

- Providing secure storage for the cloud users
- Serving as the secure proxy.

From the perspective of the cloud user, the task of convert ciphertext is relinquished to the cloud, and the cloud user just only needs to upload a key whose size is far less than the whole file.

A. PROPOSED IDENTITY PROXY RE-ENCRYPTION ALGORITHM

Let (G_1, G_T) be a pair of bilinear groups with prime order q. Let e be a bilinear map, and let H_1 and H_2 be two independent hash functions.

Setup(1^λ):

Given the security parameter 1^λ, this algorithm outputs the system params= (G_1, G_T, g, g^s) $(s \leftarrow Z_q^*)$ and the params master key msk=s.

KeyGen(ID_A, params, msk) :

Given the user's identity ID_A, this algorithm computesthe secret key corresponding to his identity ID_A sk: sk = $H_1(ID_A)^s$

Encrypt(params, ID_A, m):

To encrypt the message m under users identity ID_A asthe public key, this algorithm does the following: choosea random r ∈ Z_q^* and calculated as ciphertext

RKGen(params, sk_{ID_A}, ID_A, ID_B):

Given the identity ID_A, ID_B and a random chosen $X \leftarrow G_T$ this algorithm generates the re-encryption key

Reencrypt (params, $rk_{IDA \to ID_B}$, C_{ID_A}):

Given an ciphertextfor ID_A, and a re-encryption key from ID_A to ID_B, this algorithm outputs the ciphertext: $C_{ID_B} = (c_1, c_2, c_3)$.

Decrypt(params, sk_{ID_B}, C_{ID_B}):

Given the ciphertext C_{ID_B}, the secret key of ID_B, thisalgorithm decrypts the ciphertext and obtainsm by computing $\frac{c_2}{e(c_1, H_2(x))}$

V. IMPLEMENTATION

The proposed system of this project is divided into four majormodules and described as below.

1. SETUP
2. DATA ENCRYPTION
3. DATA SHARING
4. ACCESS DATA

5. POLICY UPDATION

A. MODULES DESCRIPTION

1) SETUP

In this phase, by using the setup and KeyGen algorithms the system parameters and users secret key are built up. We set the system master secret key msk = s. Each cloud user registered in the system can obtain a private key corresponding to his identity. The master key s is only used in the process of user registration. The data owner can share his data only given the identity of the sharers.

2) DATA ENCRYPTION

The data F is divided in to n fractions $F = (m_1, m_2, ..., m_n)$. For m_i data owner runs the Encrypt algorithm and generates m_i . After implementing the encryption of F, the user uploads files to the cloud.

3) DATA SHARING

In this phase, data owner runs the R K Gen algorithm and generates the proxy key to cloud, where X is randomly selected from G_T . The re-encryption key rk will be used by the cloud to transform the ciphertext F′to the ciphertext under sharer's public key. The data owner forwards rk to the cloud which means that the cloud is delegated to manage the data in behalf of the owner. The cloud can deploy the re-encrypt key rk to permit the authorized user to get the ciphertext decrypted with his own secret key

4) ACCESS DATA

When the sharer wants to access the file, he sends a request to the cloud server. The cloud determines the validity of the sharer by checking if it has a re-encryption key to the sharer. With the re-encryption key is existed, the cloud server can run the RK Gen algorithm and achieve the re-encryption ciphertext. Thenthe sharer fetches the re-encrypted data from the cloud servers, and runs the Decrypt algorithm on Mi with his secret key to obtain the m_i. As doing so, the sharer gets the entire file $F = (m_1, m_2, ..., m_n)$.

5) POLICY UPDATION

In practice the mobile user may want to update the list of sharers with creating or revoking some sharers in a large and dynamic mobile network. Using our approach the mobile user might do this task even without retrieving and decrypting the ciphertext from cloud. To implement the updating or deleting sharers means to create new re-encryption keys, or delete old re-encryption keys in the system.

VI. PERFORMANCES ANALYSIS

We measure the performance of our protocol in Windows XP operation system. All experiments are conducted on the Intel Pentium(R) Dual-Core E6300 with 2 GB RAM. During the operation of data, it involves the multiplication, exponentiation, and the pairing in a cyclic group. Based on cryptographic library MIRACL [18], we estimate the time consumption of these operations in graph. To demonstrate our advantage in computation and communication overhead. For comparison, we also analyze the cost of trivial solution which makes the user to endure the heavy cost in distribution of data. In other words, the trivial solution allows the data owner to compute and forward the different ciphertext to different sharer by his own.

A. ENCRYPTION AND DECRYPTION TIME

Due to the unlimited computing resources of cloud, in our performance analysis we will mainly consider the overhead on the side of users including the cost in the encryption data and generating the re-encryption key. In this graph time require for encryption by proposed system are shown. It shows that reduction in time and since using proposed algorithm encryption process is to strong in fig.2.

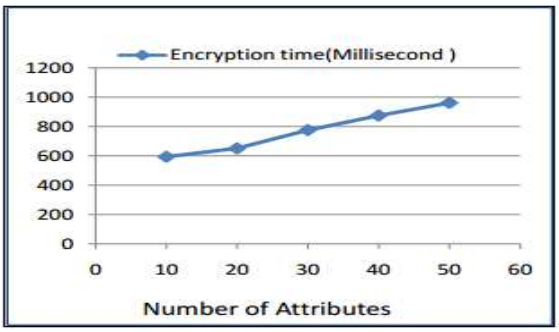

Fig .2 Encryption Time

In this graph time require for decryption by proposed system figure.3 where user's private key which is generated on the identity based proxy re-encryption algorithm assigned to user.

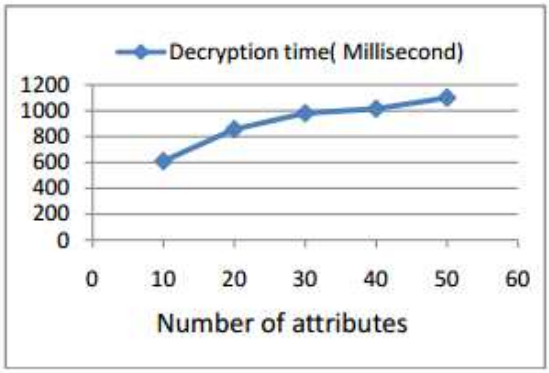

Fig .3 Decryption Time

B. KEY SIZE

In proposed Scheme private key assign to user which is computed using user's shares. So it has overcome the

limitation of existing system of complex key size to remember.

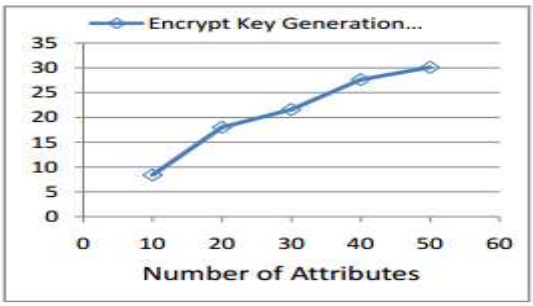

Fig.4 Encryption Key size

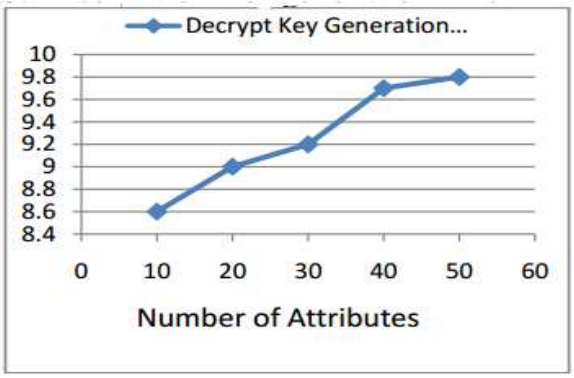

Fig..5 Decryption Key size

VII. CONCLUSION

In this paper, we presented a secure data mechanism to solve the problem of data secrecy and privacy in mobile cloud computing. We first summarize the possible approaches to realize the access control in cloud computing, and show that the situation when mobile users may arbitrarily join or leave the mobile network makes these approaches not suitable to be used in mobile cloud computing. Afterwards, in this paper we explored identity based proxy re-encryption scheme to make mobile users easily implement fine-grained access control of data and also guarantee the data privacy in the cloud. At the same time, the cost of updating of access policy and communication is also reduced in our mechanism.

REFERENCES

[1] Mell P, Grance T (2012) The NIST definition of cloud computing. NIST Spec Publ 800:145.National Institute of Standards and Technology, U.S. Department of Commerce. 145.pdf. Accessed on Oct 2012
[2] Wikipedia definition of Cloud computing (2012). Source: http://en.wikipedia.org/wiki/Cloud/computing. Accessed on Oct 2012
[3] Healey M (2010) Why IT needs to push data sharing efforts. Information Week. Source: http://www.informationweek.com/services/integration/why-it-needs-to-push-data-sharing-effort/225700544. Accessed on Oct 2012
[4] GellinA (2012) Facebook's benefits make it worthwhile. Buffalo News.
[5] Riley DA (2010) Using google wave and docs for group collaboration. Library Hi Tech News.
[6] Wu R (2012) Secure sharing of electronic medical records in cloud computing. Arizona StateUniversity, ProQuest Dissertations and Theses
[7] Pandey S, VoorsluysW, Niu S, Khandoker A, Buyya R (2012) An autonomic cloud environmentfor hosting ECG data analysis services. Future GenerComputSyst 28(1):147–154
[8] Bender D (2012) Privacy and security issues in cloud computing. Comput Internet Lawyer1–15.
[9] Judith H, Robin B, Marcia K, Fern H (2009) Cloud computing for dummies. For Dummies.
[10] SeongHan S, Kobara K, Imai H (2011) A secure public cloud storage system. International conference on internet technology and secured transactions(ICITST) 2011, pp 103–109.
[11] Zhou M, Zhang R, Xie W, Qian W, Zhou A (2010) Security and privacy in cloud computing: a survey. Sixth international conferences on emantics knowledge and grid (SKG) 2010:105–112
[12] Rocha F, Abreu S, Correia M (2011) The final Frontier: confidentiality and privacy in the cloud, pp 44–50.
[13] Huang R, Gui X, Yu S, Zhuang W (2011) Research on privacy-preserving cloud storage framework supporting ciphertext retrieval. International conference on network computing and information security 2011:93–97
[14] Xiao Z, Xiao Y (2012) Security and privacy in cloud computing. IEEE Commun SurveysTutorials 99:1–17
[15] Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. International conference on computer science and electronics, engineering, pp 647–651.
[16] Zhou M (2010) Security and privacy in the cloud: a survey. Sixth international conference onsemantics knowledge and grid (SKG) 2010:105–112
[17] Wang J, Liu C, Lin GTR (2011) How to manage information security in cloud, computing, pp1405–1410.
[18] Wang Y (2011) The role of SaaS privacy and security compliance for continued SaaS use. International conference on networked computing and advanced information management (NCM)2011:303–306
[19] Oza N, Karppinen K, Savola R (2010) User experience and security in the cloud-An empirical study in the finnish cloud consortium. IEEE second international conference on cloud computing technology and science (CloudCom) 2010:621–628
[20] Sarathy R, Muralidhar K (2006) Secure and useful data sharing. Decis Support Syst 204–220.
[21] Butler D Data sharing threatens privacy, vol449 (7163). Nature Publishing, Group, pp 644–645.
[22] Mitchley M (2006) Data sharing: progress or not? Credit, Manage 10–11.
[23] Feldman L, Patel D, Ortmann L, Robinson K, Popovic T (2012) Educating for the future:another important benefit of data sharing. Lancet 1877–1878.
[24] Geoghegan S (2012)The latest on data sharing and secure cloud computing. Law, Order 24–26.
[25] Sahafizadeh E, Parsa S (2010) Survey on access control models. 2nd international conference future computer and communication (ICFCC) 2010, pp V1–1-V1-3.
[26] MdMozammilAlam, SouravHati, Debashis De and SamiranChattopadhyay,Secure Sharing of Mobile Device Data using Public Cloud,Confluence The Next Generation Information Technology Summit,2014,149 – 154.
[27] Uma Somani,Kanika Lakhani and Manish Mundra, Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing ,Parallel Distributed and Grid Computing ,2010,211-216.
[28] Raseena M , Harikrishnan G R ,Secure Sharing of Data over Cloud Computing using Different Encryption Schemes An Overview,International Journal of Computing and Technology 1,no. 2,2014,8-11.
[29] Mazhar Ali, RevathiDhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li and Albert Y. Zomaya,Se DaSC:Secure Data Sharing in Clouds,SYSTEMS JOURNAL PP,no.99,2015,1-10.