International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Index Copernicus Value (2015): 62.86 | Impact Factor (2015): 3.791

A Survey on Various Multi-Owner Data Sharing Techniques On Cloud Computing

Ayushi Shukla[1], Prof. Umesh Lilhore[2], Prof. Nitesh Gupta[3]

[1]M.Tech Scholar, NRI Institute of Information Science & Technology, Sagar, India
[2]Asso. Professor, NRI Institute of Information Science & Technology, Bhopal, India
[3]Asso. Professor, NRI Institute of Information Science & Technology, Bhopal, India

Abstract: ***As time goes on, humans accumulate more and more information. This information is utilized to construct valuable information which permits us to build decisions. Not all data is in one database, still. Humanity's information is dividing among millions of unusual owners: companies, entity and governments. To facilitate produce better information for better decisions, data sharing can be utilized. On the other hand, the different inspirations of the owners can origin difficulties in the data sharing method. Here in this paper a survey of all the Data Sharing techniques is done which are implemented for Secure Data Sharing over Cloud and other Environment. Also various issues and challenges can be analyzed so that on the basis of their various advantages and disadvantages a new and efficient technique is implemented in future.***

Keywords: Cloud information storage, hardware visualization, order preserving encryption, two round research able encryption, key generation

1. Introduction

Current advances in IT have deeply facilitated inaccessible information storage and distribution. New applications such as online societal networks and online documents provide very convenient conduct for nation to accumulate and share various data including personal profile, electronic documents and etc on remote online data servers. Cloud Computing, regarded as the opportunity IT architecture, and even promise to present unconstrained and expandable luggage compartment supply and other computing resources as a service to cloud users in a very cost-effective way [1]. Even though still at its premature period, Cloud Computing has previously haggard great concentration and its reimbursement have involved an growing numeral of users to contract out their limited information centers to remote cloud servers.

Statistics security is a significant concern for inaccessible data storage. On one hand, discovery of perceptive information, such as health records, stored on remote data servers has to be strictly protected before users have liberty to use the data services. Fine-grained statistics admittance organize mechanisms habitually need to be in position to swear apposite discovery of perceptive data between several users. On the other supply, in inaccessible data storage space users do not actually enjoy their statistics. Remote data overhaul providers are approximately convinced to be outside the users' trust domain, and are not allowed to learn users' sensitive information stored on their servers. As such, they only have to pay their cloud overhaul providers for the allocated resources. Indeed, these providers offer to their clients the possibility to store, retrieve and share data with other users in a transparent way. Unfortunately, in addition to its several advantages, cloud storage brings several security issues, namely data confidentiality preservation. Kamara and Lauter [2], and Chow et al. [3] decided that encrypting outsourced statistics by the customer is a good substitute to moderate such concerns of information discretion. So that, the client conserve the decrypting keys out of attain of the cloud supplier However, the confidentiality provisioning becomes more intricate with plastic data distribution surrounded by a assembly of users. It requires proficient allocation of decrypting keys stuck between poles apart allowed users. As such, only endorsed users are able to acquire the clear text of statistics stored in the cloud. Figure-1 illustrates eloquent network planning for cloud cargo space. It relies on the following entities, permitting a customer to store, retrieve and share data with multiple users:

- **Cloud Service Provider (CSP)** – a CSP has significant possessions to administer disseminated cloud storage space servers and to supervise its database servers. It also provides effective communications to host function military These armed forces can be used by the buyer to deal with his data stored in the confuse servers.
- **Client (C)** – a client is a statistics possessor who makes use of provider's property to store, retrieve and share data with multiple users. A client can be either an individual or an enterprise. Each client has a unique and authentic identity, denoted by IDC.
- **Users (U)** – the users are able to admission the satisfied stored in the cloud, depending on their admission civil rights which are authorizations approved by the patron, like the privileges to read, write or re-store the personalized figures in the cloud. These contact civil liberties serve to indicate several groups of users. Each grouping is characterized by an identifier IDG and a set of admission civil rights.

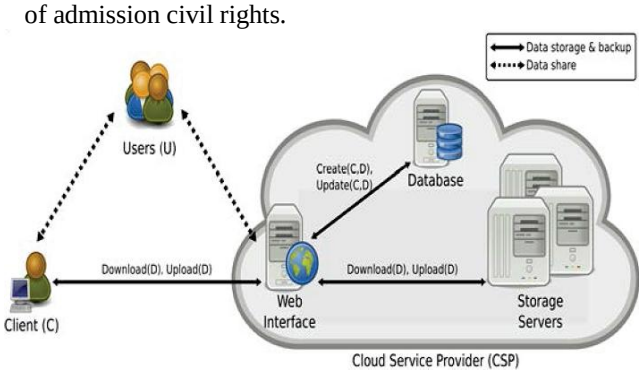

Figure 1: Architecture of cloud information storage

In perform, the CSP provides a web boundary for the client to store up statistics into a set of cloud servers, which are management in a cooperate and dispersed approach. In toting up, the web boundary is used by the user to salvage, amend, and re-store information from the cloud, depending on their admission human rights. Furthermore, the CSP relies on folder servers to map client's identity to their store data identifiers and group's identifiers.

One of the most elementary military existing by cloud provider is statistics cargo space. Let us believe a realistic data application. Expressly, the shade servers managed by cloud provider are not effusive trusted by users while the figures files stored in the cloud may be insightful and off the record, such as industry plans. To conserve data solitude, a basic explanation is to encode statistics files, and then upload the encoded statistics into the cloud. Unhappily, conniving an competent and protected data allocation method for group in the cloud is not an easy mission due to the subsequent demanding issues.

2. Theoretical Background

Cloud compute is one of the maximum display place which provides storage of data in very lower cost and available for all time over the internet. Cloud computing is Internet-based computing, whereby communal possessions, software and in sequence are provide to computers and strategy on command. Quite a few trends are aperture up the era of Cloud Computing, which is an Internet-based expansion and use of processor knowledge. Cloud Computing means more than simply saving on IT implementation costs. One of the most primary military accessible by cloud provider is information storage space. A companionship allows its staffs in the same assembly or branch to store up and contribute to documentation in the cloud. By utilize the cloud, the staffs can be entirely unconfined from the nuisance some narrow data storage space and safeguarding however, it also poses a noteworthy risk to the discretion of those store records. purposely, the obscure servers manage by darken provider are not completely trust by users while the information records stored in the blur may be receptive and private. To conserve data solitude a basic key is to encode information files, and then upload the encrypted information into the obscure. unhappily, conniving an well-organized and protected data allocation method for group in the cloud is not an easy chore due to the subsequent demanding issues. quite a few refuge scheme for statistics distribution on untrusted servers have been planned [4], [5], and [6]. Thus, unlawful users as well as storeroom servers cannot be taught the contented of the information documentation since they have no acquaintance of the decryption keys. Though, the complexity of user contribution and revocation in these scheme are linearly mounting with the numeral of data owners and the integer of revoke users, correspondingly.

3. Varieties of Data Sharing

These different motivations give rise to several different types of data sharing. These methods range from simple to complex, and we enumerate some of them now.

- **Distributed Data Mining:** Distributed data mining is simply the act of using raw data to produce meaningful information in a distributed setting. If the only goal is to produce meaningful information, then the task of distributed data mining can be done in a manner not dissimilar from local data mining. However, this is often not the case, and entities may wish to keep their data private while still getting meaningful information, or they may wish to keep communication and computation cost down.
- **Privacy-Preserving Data Mining:** Several methods have been developed for doing distributed data mining while maintaining privacy. These include anonymization techniques, perturbation techniques, and cryptographic (secure multiparty computation) techniques. Anonymization strips sensitive and identifying elements from the data before performing the data mining. Perturbation adds noise to the data before the data mining process, resulting in similar information learned, but without enlightening the original data. Perturbation sacrifices utility for privacy. Cryptographic techniques use homomorphic encryption, secret sharing, virtual circuits, and other tools to exactly compute the correct result without enlightening any of the information to other parties. These cryptographic protocols invariably take longer to run than the original data mining process, however. Thus, the cryptographic protocols provide a tradeoff between privacy and efficiency.
- **Secure Multiparty Computation:** Data mining is a subset of multiparty computation, which is the general computing of a function between multiple parties. Secure mutual subtraction is the method of computing such a function without revealing the inputs to the other parties. There are general methods for drama secure multiparty calculation, but these another time require very expensive cryptographic protocols.
- **Data Outsourcing:** Due to lack of infrastructure or resources, an entity may wish to outsource its data to another entity, who we will call the provider, for the purposes of processing. Thus, in order to make use of the provider's increased computing resources, the entity has the provider hold its data. Then, the owner of the data sends queries to the provider, which the provider will use its considerable resources to run. The result is then returned to the owner.

4. Cloud Security Issues

The Cloud refuge is also the focal point of this employment. Unlike preceding survey of cloud refuge issues, our eventual goal is to make accessible a much more whole and methodical reporting of the investigate writing connected to this subject. We give a extensive general idea of publication in the fields of cloud computing sanctuary and sanctuary of inaccessible storage space and working out [7].

- **Security shortcomings of hardware virtualization:** We depict the troubles that have surfaced by the side of with the substantial use of hardware virtualization by confuse providers. We indicate how virtualization can be exploited to obtain unauthorized in sequence from

susceptible users, and also point toward alleviation scheme that can be engaged.

- **Cloud accountability, or its capability to incarcerate and interpretation wrongful commotion:** We converse capabilities that a held answerable coordination should have and solutions for achieving these capabilities most cloud providers charge their users according to the actual usage of their infrastructure during a pre-determined time slice. In the case of a service that is being flooded, this usage will be obviously high, which, in its turn, will most likely translate to bills that are much higher than expected.
- **Challenges and solutions for remote storage protection:** We describe several techniques that can be employed by cloud clients to verify integrity of their outsourced data.
- **Protection of outsourced computation:** Finally, we give an overview of current approaches for assuring privacy and integrity of outsourced computations.

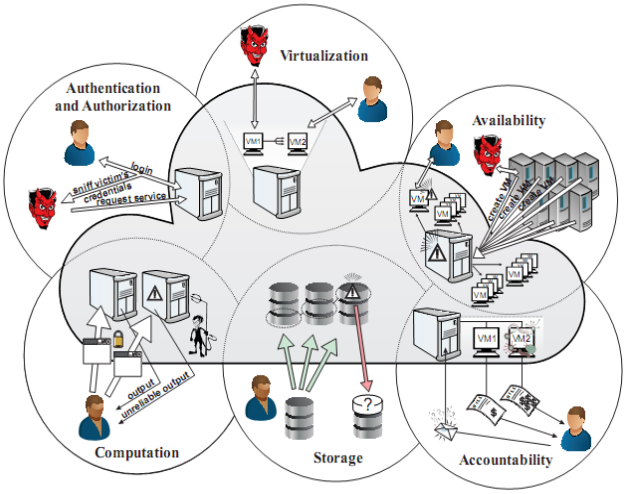

Figure: Overview [7] of cloud security issues

5. Prepare Secure Data Sharing Schemes for Cloud Computing

Secure Data Sharing in Cloud Computing: Cloud Computing is a promising next-generation IT architecture which provides elastic and unlimited resources, including storage, as services to cloud users. In Cloud Computing cloud users and cloud service providers are almost certain to be from different trust domains. A secure user-enforced data access control mechanism must be provided before cloud users have the liberty to outsource sensitive data to the cloud for storage. Compared to previous work [8-10], their scheme provides better scalability when providing fine-grained data access control because the complexity of most system operations in our scheme is linear to the number of attributes rather than the number of users/data files. In Cloud Computing, cloud servers are very powerful but cloud users could be resource-constrained devices such as mobile phones. To reduce the computation load for cloud users, we combine various computation delegation techniques with ABE and securely offload computation-intensive tasks to powerful cloud servers. For example, we integrate the technique of proxy re-encryption into ABE and securely mitigate the laborious user revocation task from the data owner to cloud servers. Using another computation delegation technique, we reduce the computation load for data consumers to constant complexity and make it affordable to user devices such as mobile phones. The proposed scheme also significantly saves the computation load for cloud servers by exploiting the technique of lazy re-encryption [5]. Both performance analysis and security proof are provided.

Access Control for Distributed Data Storage: In WSNs, storing data at local sensor nodes or at designated in-network nodes would greatly save the network-wide communication load and brings forth a lot of benefits such as energy-efficiency and ease of distributed data retrieval. However, unattended wireless sensor nodes are easily subject to strong attacks such as physical compromise and cannot be trusted by the owner. To make the expensive ABE encryption operation affordable to resource-constrained sensor nodes, we divide the lifetime of sensor nodes into phases and then distribute the underlying mathematical operations in ABE over these phases. To minimize the communication and computation load on sensor nodes in case of user revocation, we revise an existing ABE scheme and make the user revocation complexity on sensor nodes constant. Formal security proof and experimental results shows that our proposed solution is provably secure and affordable to contemporary sensor nodes. To the best of our knowledge, the only existing work prior to ours that addresses the issue of secure distributed data storage and retrieval in WSNs is [11].

6. Literature Survey

In this paper [12], here author has put forward a novel model, referred to as secure, scalable and efficient multi-owner (SSEM) data sharing in clouds. The SSEM integrates identity-based encryption and asymmetric group key agreement to enable group-oriented access control for data owners in a many-to-many sharing pattern. Additionally, with SSEM, users can join in or leave from the group suitably with the privacy of both group data and user data. Here they proposed the key-cipher text homomorphism method to build an SSEM method with short cipher texts.

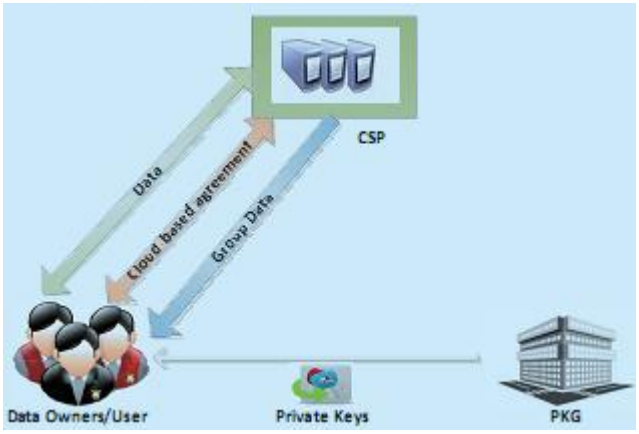

Figure: Overview [12] of proposed architecture

The security analysis demonstrates that our SSEM method accomplishes data security against unauthorized accesses

and collusion attacks. Both theoretical and experimental effects authenticate that their proposed method takes users little costs to share and access outsourced data in a group approach. As well as, SSEM allows membership varying with forward and backward security.

M. Armbrust et al. [13] presented a security one of the most often-cited objections to cloud computing; analysts and skeptical companies ask "who would trust their essential data, out there " somewhere?" There are also requirements for auditability, in the sense of Sarbanes-Oxley azon spying on the contents of virtual machine memory; it's easy to imagine a hard disk being disposed of without being wiped, or a permissions bug making data visible improperly. There an obvious defense, namely user-level encryption of storage. This is already common for high-value data outside the cloud, and both tools and expertise are readily available. This approach was successfully used by TC3, a healthcare company with access to sensitive patient records and healthcare claims, when moving their HIPAA-compliant application to AWS. Similarly, auditability could be added as an additional layer beyond the reach of the virtualized guest OS, providing facilities arguably more secure than those built into the applications themselves and centralizing the software responsibilities related to confidentiality and auditability into a single logical layer. Such a new feature reinforces the Cloud Computing perspective of changing our focus from specific hardware to the virtualized capabilities being provided.

S. Kamara et al. [14] proposed a security for customers to store and share their sensitive data in the cryptographic cloud storage. It provides a basic encryption and decryption for providing the security. However, the revocation operation is a sure performance killer in the cryptographic access control system. To optimize the revocation procedure, they present a new efficient revocation scheme which is efficient, secure, and unassisted. In this scheme, the original data are first divided into a number of slices, and then published to the cloud storage. When a revocation occurs, the data owner needs only to retrieve one slice, and re-encrypt and republish it. Thus, the revocation process is accelerated by affecting only one slice instead of the whole data.

D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia [15] the data centers hardware and software is what we will call a cloud. When a cloud is made available in a pay-as-you-go manner to the general public, they call it a public cloud; the service being sold is utility computing. They use the term private cloud to refer to internal data centers of a business or other organization, not made available to the general public, when they are large enough to benefit from the advantages of cloud computing that we discuss here. Thus, cloud computing is the sum of SaaS and utility computing, but does not include small or medium-sized data centers, even if these rely on virtualization for management. People can be users or providers of SaaS, or users or providers of utility computing. They focus on SaaS providers (cloud users) cloud providers, which have received less attention than SaaS users.

In this paper [16], we introduce the concepts of similarity relevance and scheme robustness to formulate the privacy issue in searchable encryption schemes, and then solve the insecurity problem by proposing a two-round searchable encryption (TRSE) scheme. Novel technologies in the cryptography community and information retrieval (IR) community are employed, including homomorphic encryption and vector space model. In the proposed scheme, the majority of computing work is done on the cloud while the user takes part in ranking, which guarantees top-k multi-keyword retrieval over encrypted cloud data with high security and practical efficiency. Our contributions can be summarized as follows:

We propose the concepts of similarity relevance and scheme robustness. We, thus, perform the first attempt to formulate the privacy issue in searchable encryption, and we show server-side ranking based on order-preserving encryption (OPE) inevitably violates data privacy.

We propose a TRSE scheme, which fulfills the secure multi-keyword top-k retrieval over encrypted cloud data. Specifically, for the first time, we employ relevance score to support multi-keyword top-k retrieval.

Thorough analysis on security demonstrates the proposed scheme guarantees high data privacy. Furthermore, performance analysis and experimental results show that our scheme is efficient for practical utilization. By security analysis, we show that the proposed scheme guarantees data privacy. According to the efficiency evaluation of the proposed scheme over a real dataset, extensive experimental results demonstrate that our scheme ensures practical efficiency.

Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in the context of Cloud Computing. To achieve our design goals on both system security and usability, we propose to bring together the advance of both crypto and IR community to design the ranked searchable symmetric encryption scheme, in the spirit of "as-strong-as-possible" security guarantee. Specifically, we explore the statistical measure approach from IR and text-mining to embed weight information (i.e. relevance score) of each file during the establishment of searchable index before outsourcing the encrypted file collection.

In this paper [17], for the first time they define and solve the problem of effective yet secure ranked keyword search over encrypted cloud data. Ranked search greatly enhances system usability by returning the matching files in a ranked order regarding to certain relevance criteria (e.g., keyword frequency), thus making one step closer towards practical deployment of privacy-preserving data hosting services in Cloud Computing. We first give a straightforward yet ideal construction of ranked keyword search under the state-of-the-art searchable symmetric encryption (SSE) security definition, and demonstrate its inefficiency.

In this paper [18], they recommend a protected cloud cargo space organization behind privacy-preserving communal auditing. Our employment is amongst the first few ones to prop up privacy-preserving community auditing in cloud computing, with a focus on data storage. Besides, with the prevalence of cloud computing, a foreseeable increase of auditing tasks from different users may be delegated to TPA. Extensive analysis shows that our schemes are provably secure and highly efficient. We abscond the full-fledged accomplishment of the instrument on commercial public cloud as an importantfuture extension, which is expected to robustly cope withvery large scale data and thus encourage users to adopt cloudstorage services more confidently.

The Table given below is the analysis and comparison of various Encryption algorithms. The Analysis given here on the basis of Initialization and Key Generation and Encryption and Decryption. The Analysis also shows the relationship it supports.

Where,

G Time Cost of Point multiplication in G
|G| The Length of the element in G
Time cost of point multiplication in
| The length of the element in
g Time Cost of operation of Point in G
Time Cost of operation of Point in
P Time Cost of pairing
a The number of all attributes
t The number of users's attributes
c The number of all message types
v The number of aggregated message types
r The number of revoked users

Scheme	Initialization	KeyGen	Encryption	Decryption
KACS [19]	2 c G	v (G + g)		
Mona [20]	6 G + P	2 G		
EEAC [21]		a (2 G + g)		
SSEM [12]	2 G	3 G + g		

Table 1: Survey of length of Computational cost of time

Scheme	Encryption	Decryption
KACS [19]		(2v-1)G+2P+g+2
Mona [20]		17G+7P+9g+6
EEAC [21]		2tP+t
SSEM [12]		2P+

Table 2: Survey of length of Computational cost of time

The Table given below is the analysis and comparison of various Encryption algorithms. The Analysis given here on the basis of Public Key Size and Secrete Key size and the length of the cipher text.

Scheme	Public Key Size	Secrete Key Size	Ciphertext Size
KACS [19]	(2c+2)|G|	|G|	3|G|+||
Mona [20]	(2r+11)|G|+||	2|G|	5|G|+||
EEAC [21]	|G|+a(|G|+||)	|G|	3|G|+||
SSEM [12]	5|G|+||	3|G|	4|G|+||

Table 3: Analysis of the sizes of messages

7. Conclusion

Here in this paper summary and analysis of all the existing techniques that is implemented for Efficient Data Sharing over Cloud Computing. Here the technique implemented for the Data Sharing and their various advantages and Disadvantages is analyzed and discuss, hence on the basis of their various limitations a new and efficient technique is implemented in future.

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. USB-EECS-2009-28, Feb 2009.
[2] S. Kamara and K. Lauter. Cryptographic cloud storage. In Proceedings of the 14th international conference on financial cryptograpy and data security, FC'10, Berlin, Heidelberg, 2010. Springer-Verlag.
[3] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. Controlling data in the cloud: outsourcing computation without outsourcing control. In Proceedings of the 2009 ACM workshop on Cloud computing security, pages 85–90. ACM, 2009.
[4] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.
[5] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
[6] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
[7] EveraldoAguiar, Yihua Zhang, and Marina Blanton, "An Overview of Issues and Recent Developments in Cloud Computing and Storage Security" 2012.
[8] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati. Over-encryption: Management of Access Control Evolution on Outsourced Data. In Proc. of VLDB'07, Vienna, Austria, 2007.
[9] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc.of NDSS'05, 2005.
[10] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. Of ESORICS '09, 2009.
[11] N. Subramanian, C. Yang, and W. Zhang, "Securing distributed data storage and retrieval in sensor networks," in Pervasive and Mobile Computing Journal (Special Issue for PerCom 2007), November 2007.

[12] Shungan Zhou, Ruiying Du, Jing Chen, Hua Deng, Jian Shen, Huanguo Zhang, "SSEM: Secure, Scalable and Efcient Multi-Owner Data Sharing in Clouds"IEEE China Communications Volume: 13, Issue: 8, Aug. 2016.
[13] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
[14] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int"l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.
[15] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
[16] Jiadi Yu, Peng Lu, Yanmin Zhu, GuangtaoXue and Minglu Li, "Toward Secure Multi-keyword Top-k Retrieval over Encrypted Cloud Data" IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 10, NO. 4, JULY/AUGUST 2013.
[17] Cong Wang, NingCao, JinLi, KuiRen, and Wenjing Lou, "Secure Ranked Keyword Search over Encrypted Cloud Data" 2011.
[18] Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage" IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013.
[19] Chu C, Chow S, Tzeng W, Zhou J, Deng R. Key-aggregate cryptosystem for scalable data sharing in cloud storage [J]. Parallel and Distributed Systems, IEEE Transactions on. 2014. 25(2): 468-477.
[20] Liu X, Zhang Y, Wang B, Yan J. Mona: secure multi-owner data sharing for dynamic groups in the cloud [J]. IEEE Trans on Parallel and Distributed System. 2013, 24(6):1182-1191.
[21] Yang K, Jia X, Ren K, Xie R, Huang, L. Enabling efficient access control with dynamic policy updating for big data in the cloud[C].// IEEE INFOCOM, 2014:2013-2021