REVIEW ARTICLE

Review on Privacy Preservation and Secure Data Sharing on Cloud Storage

Chavhan Bhaurao* and Kamble Rutuja

Department of computer science & engineering, G. H. Raisoni college of engineering and Management, Amravati

**Corresponding Author Email -chavhanbhaurao@gmail.com*

Manuscript Details

Received : 10.11.2014
Revised : 21.11.2014
Revised Received :01.12.2014
Accepted: 05.12.2014
Published : 10.12.2014

ISSN: 2322-0015

Editor: Dr. Arvind Chavhan

Cite this article as:
Chavhan Bhaurao and Kamble Rutuja. Review on Privacy Preservation and Secure Data Sharing on Cloud Storage, *Int. Res. J. of Sci. & Engg.*, 2014; 2 (6): 226-234.

ABSTRACT

Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Privacy preservation and secure sharing of the data over un-trusted cloud is still a challenging issue, due to the frequent change of the membership. A secure multi owner data sharing technique is proposed for dynamic groups in the cloud. By using group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. In this paper we will review various techniques which used for secure data sharing and privacy preservation with its pitfalls.

Keywords: Cloud computing, data sharing, privacy-preserving, access control, dynamic groups.

1. INTRODUCTION

Cloud frameworks can be utilized to empower information offering abilities and this can master vide a plenteous of profits to the client. There is at present a push for IT associations to expand their information offering exertions. As per review completed Chavhan and Wadhe (2014) on cloud services in which data sharing is done has various security problem and to overcome we have to implement some technique for secure data sharing. The Cloud however is defenceless to numerous protection and security issues. As per a review completed by IDC Enterprise Panel (2008), Cloud clients viewed security as the top test with 75 % of studied clients agonized over their basic business and IT frameworks being defenceless against assault. Apparently, numerous security and security assaults happen from inside the Cloud supplier themselves as they normally have immediate access to put away information and take the information to offer to outsiders so as to addition benefit. In today's reality, there is a solid need to impart data to gatherings of individuals around the globe. Since the Cloud is loaded with such a variety of security issues, numerous clients are still anxious about offering their most basic information to different clients.

Some of real necessities of secure information offering in the Cloud are as per the following. Firstly the information manager ought to have the capacity to point out a gathering of clients that are permitted to view his or her information. Any part inside the gathering ought to have the capacity to get access to the information whenever, anyplace without the information manager's intercession. Nobody, other than the information holder and the parts of the gathering, ought to get access to the information, including the Cloud Service Provider. The information manager ought to have the capacity to add new clients to the gathering. The information holder ought to additionally have the capacity to renounce access rights against any part of the gathering over his or her imparted information. No part of the gathering ought to be permitted to deny rights or join new clients to the gathering.

One inconsequential answer for accomplishing secure information offering in the Cloud is for the information holder to encode his information before putting away into the Cloud, and henceforth the information remain data hypothetically secure against the Cloud supplier and different pernicious clients. At the point when the information holder needs to impart his information to a gathering, he sends the key utilized for information encryption to every part of the gathering. Any part of the gathering can then get the scrambled information from the Cloud and unscramble the information utilizing the key and thus does not require the mediation of the information holder. On the other hand, the issue with this procedure is that it is computationally wasteful and puts an excessive amount of trouble on the information holder when considering elements, for example, client renouncement. At the point when the information holder disavows access rights to a part of the gathering, that part ought not have the capacity to get access to the relating information. Since the part still has the information access key, the information manager needs to re-encode the information with another key, rendering the repudiated part's key pointless. At the point when the information is re-scrambled, he must disseminate the new key to the remaining clients in the gathering and this is computationally wasteful and puts a lot of trouble on the information holder when considering expansive gathering sizes that could be in overabundance of a large number of clients. Henceforth this arrangement is unfeasible to be conveyed in this present reality for exceptionally discriminating information, for example, business, and government related information. In this article, we audit existing systems for accomplishing information imparting in the Cloud that is both secure and productive.

2. RELATED WORK

There have been various surveys on security and protection in the Cloud. Xiao and Xiao (2012) recognizes the five concerns of Cloud figuring; privacy, trustworthiness, accessibility, responsibility, and protection and completely surveys the dangers to each of the concerns and also safeguard procedures. Chen and Zhao (2012) plots the necessities for accomplishing security and security in the Cloud furthermore quickly traces the prerequisites for secure information imparting in the Cloud. Zhou (2010) gave a study on security and security in the Cloud concentrating on how protection laws ought to likewise contemplate Cloud figuring and what work is possible to forestall security and security ruptures of one's close to home information in the Cloud. Wang *et al*. (2011) investigated elements that influence overseeing data security in Cloud processing. It clarifies the essential security requirements for ventures to comprehend the motion of data security in the Cloud. Wang (2011) completed a study on the protection and security agreeability of Software-As-A-Service (SAAS) among endeavours through pilot testing security/security consistence. They then complete examination chip away at the estimations to check whether Saas conforms to security and security guidelines. The strategy does not however consider other Cloud models, for example, Platform-As-A-Service (Paas) and specifically Infrastructure-As-A-Service (Iaas), as required for information offering. Oza *et al*. (2010) did a study on various clients to focus the client knowledge of Cloud processing and found that the fundamental issue of all clients was trust and how to pick between distinctive Cloud Service Providers.

The criticalness of information imparting and the need to guarantee security and security is examined in various existing articles. Sarathy and Muralidhar (2006) audit the effect of the Internet on information imparting crosswise over numerous diverse associations, for example, government orgs and organizations. They order information imparting into information dissimilar country, question confinement, and record matching. They additionally give a structure to secure and helpful imparting of information on the web. Steward (2012) portrays the issues of information offering on the Internet where imparting data can permit clients to gather insights about clients. This is valuable as it brings issues to light to associations that the information they decide to impart to the general population can at present raise security issues and does not ensure the secrecy of its clients. Mitchley (2006) depicts the profits of information imparting from a saving money point of view and highlights the protection issues as of now influencing it. Feldman *et al.* (2012) talk about the imperative advantage of information offering regarding general wellbeing, specifically for instruction and expert advancement. Geoghegan (2012) examine a rundown of associations that adequately and secure offer data by means of the Cloud. Nonetheless, it doesn't talk about the philosophies the associations utilization to secure information or the drawback of these associations. There is additionally writing that concentrate on one part of security and information imparting; access control. Access control can be utilized to approve a subset of clients to view private information gave they have the right authorization. Sahafizadeh and Parsa (2010) review various distinctive get to control models and assesses its adequacy. The review on the other hand, is restricted to just programming frameworks and does not think seriously about Cloud frameworks.

3. Traditional Approach

A minor answer for information imparting and cooperation in the Cloud includes an information holder conveying encryption keys to each client he approves. Each one client that has approved access can then get the scrambled information from the Cloud and unscramble the information utilizing the supplied key. This guarantees that no unapproved client gets access to information regardless of the fact that he figures out how to download the cipher text from the Cloud as he doesn't have the key for decoding. This arrangement notwithstanding, is not both effective and compelling. Once the information holder chooses to deny a client from getting to their information, one minor arrangement would be for the information manager to decode the information and re-encode the information once more, this time with another key and circulate this new key to the remaining clients in the gathering. This can get to be greatly expensive and places an immense trouble on the information holder when considering gathering sizes in overabundance of thousands to a large number of clients. Moreover, as parts of the gathering consistently join and leave, constantly re-scrambling information and sending re-encryption keys to a gathering of this size gets to be unreasonable for the information manager and infeasible to actualize in this present reality. Right now, there is continuous research on this issue.

3.1 Review of Works on Key Management

Lei *et al*. (2010) showed the requirement for legitimate key administration in the Cloud environment. A Cloud Key Management Infrastructure (CKMI) is proposed which contains a Cloud Key Management Client (CKMC) and Cloud Key Management Server (CKMS). The convention incorporates objects which contain keys and declarations, and so forth, the operations upon them, for example, creation, erasure, recovery and overhauling of keys, authentications, furthermore ascribes identified with the item being referred to, for example, the article identifier. The system is powerful for fitting key administration be that as it may, if the server is broken, the entire client's information is lost and there is no legitimate reinforcement and recuperation instrument, a key prerequisite of key administration as depicted previously.

Huang *et al*. (2011) attempted to expand on top of the Leakage Resilient Authenticated Key Exchange (LR-AKE) initially proposed by Fathi *et al*. (2006) and proposed the LR-AKE Cluster mode convention for powerful key administration. The LR-AKE includes the client recollecting a secret key while moreover putting away a high-entropy mystery on the customer machine to permit correspondence between distinctive servers. In the LR-AKE Cluster mode, the customer produces validation insider facts for every server and fractional information keys. Each one sets validates and speaks with one another to consolidate halfway keys to uncover full information keys when client demands. The principle shortcoming with this convention is that if any of the servers or the customer comes up short, the information is lost as the keys used to get to the information won't be accessible. The LR-AKE Cluster+ mode expands on the LR-AKE Cluster mode, where beside the client individual watchword, the customer picks an irregular secret key (256 bits in length) and an alternate gadget (e.g., a USB drive) stores this arbitrary secret key and also the verification insider facts for included security and higher accessibility. Mysteries are needed from both gatherings of the correspondence and subsequently information still remains data hypothetically secure and secret. One of the disadvantages to this methodology is that it requires the support of various servers and the customer, which adds undesirable intricacy when attempting to draw in substantial number of clients to the Cloud.

Sanka *et al*. (2010) proposed ability records for powerful key administration and information access where the information manager does not need to be online at all times. The model includes utilizing a capacity list where the information manager makes a rundown containing a passage for every client and the consents for record get to and stores this rundown in the CSP. At the point when a client appeals access to a document, he demands access to the record specifically to the CSP, subsequently information manager does not need to be online at all times and just needs to be online when enlisting new clients or disavowing clients from the rundown. The model is secure and classified against the Cloud and unapproved clients since they never know the substance of the encoded information since the key is an imparted symmetric key between the information holder and client. The fundamental issue with the model on the other hand, is that it accept the CSP won't adjust the capacity list. The CSP has admittance to the decoded ability list and can perniciously adjust or close out records from clients.

Bennani *et al*. (2010) proposes a model which duplicates the database in the cloud n times where n speaks to the quantity of parts. At the point when a part is repudiated access rights, the comparing database is evacuated. Changing a parts access rights heads in the most detrimental possibility to the creation starting with no outside help another perspective and re-keying the relate ing database. One of the principle issues with this model is that it is infeasible to actualize since it presents high excess and subsequently is not productive.

3.2. Discussion

The Table 1 shows a summary of the existing literature based on key management in the Cloud. The works that were reviewed had a strong focus on preventing the need for the data owner to be online at all times. Many of the works that were reviewed also had a strong focus on preventing the Cloud from viewing any of the plaintext at all times. However, in terms of achieving proper key management in the Cloud, some form of redundancy had to be introduced in some of the works.

Proper key management in the Cloud can lead to more secure and confidential sharing of data in the Cloud. A poor key management system can lead to the complete unreliability of the Cloud and can also lose trust from its consumers. Hence it is imperative that more research needs to done in achieving a more robust key management for the Cloud not only to attract more consumers and build trust but also to provide a foundation for secure and private data sharing in the Cloud.

4. RECENT APPROACHES

In this segment, we give a survey on present works of writing on empowering secure and classified information imparting in the Cloud.

4.1 Attribute-Based Encryption

Attribute Based Encryption (ABE) is one viable and guaranteeing strategy that is utilized to give fine-grained access control to information in the Cloud. At first, get to information in the Cloud was given through Access Control Lists (Acls) nonetheless, this was not versatile and just given coarse-grained access to information (2010). Characteristic Based encryption initially proposed by Goyal *et al.* (2006) gives a more adaptable and fine-grained access control to information in correlation to Acls. Trait Based Encryption is a right to gain entrance control instrument where a client or a bit of information has characteristics connected with it. A right to gain entrance control strategy is characterized and if the properties fulfil the right to gain entrance control arrangement the client ought to have the capacity to get access to the bit of data. There are two sorts of ABE, which are depicted as takes after.

Table 1 : Summary of literature on key management in the Cloud

Method	**Data/Key**	**Data owner**	**Confidentiality preserved**	**Single point**
	redundancy	online at all times	from CSP	of failure
Lei *et al.*	N	N	Y	Y
Huang *et al.*	Y	N	Y	N
Sanka *et al.*	N	N	N	N
Bennani *et al.*	Y	N	Y	N

Y yes, *N* no

- *Key-Policy ABE (KP-ABE)*

The right to gain entrance control arrangement is put away with the client's private key and the scrambled information also stores various properties connected with the information. A client can just unscramble the information if the characteristics of the information fulfil the right to gain entrance control arrangement in the client's key. The right to gain entrance control approach is normally characterized as a right to gain entrance tree with inside hubs speaking to edge entryways and leaf hubs speaking to characteristics.

- *Ciphertext-Policy ABE (CP-ABE):*

Essentially the opposite of KP-ABE. The right to gain entrance control strategy is put away with the information and the qualities are put away in the client's key.

- *ABE for Data Sharing and Collaboration*

ABE is likewise utilized for information offering and joint effort meets expectations. Tu *et al.* (2012) made utilization of CP-ABE in the setting of big business applications furthermore created a renouncement system that at the same time permits high versatility, fine-grained access control and disavowal. The office allots clients a set of properties inside their mystery key and disperses the mystery key to the separate clients. Any client that fulfills the right to gain entrance control strategy characterized by the information associate can get to the information. At the point when a client is repudiated access rights, the information is re-scrambled in the Cloud rendering the renounced client's key futile. The plan is ended up being semantically secure against picked ciphertext assaults against the CP-ABE model. On the other hand, the plan is not rich on account of client denial since the overhauling of ciphertexts after client repudiation puts overwhelming reckoning overhead regardless of the possibility that the trouble is exchanged to the Cloud. Li *et al.* (2013) influences ABE in the setting of the offering of individual wellbeing records (PHR) in the Cloud. Their system comprises of an open area comprising of clients who make gets to on expert records, for example, specialists, medical attendants and medicinal analysts, furthermore individual space, which comprise of clients who are generally connected with the information holder, for example, family and close companions. Part ascribes are relegated to the clients in general society area that speaks to their proficient part and they recover their mystery keys from a characteristic power. This is viable as the information manager require not be online at all times. As far as access control, information managers define part based fine-grained access control approaches for their PHR documents. Utilizing part based access strategies extraordinarily diminishes key administration overhead for managers and clients as the manager does not need to oversee keys for every individual client.

4.2. Proxy Re-encryption

Intermediary Re-encryption is an alternate strategy that is quick getting to be received for empowering secure and secret information imparting and joint effort in the Cloud. Intermediary Re-encryption (2010) permits a semi-trusted intermediary with a re-encryption key to interpret a cipher text under the information manager's open key into an alternate cipher text that can be decoded by an alternate client's mystery key. At no stage will the intermediary have the capacity to get to the plaintext. Specialists have used intermediary re-encryption in connection to the Cloud and specifically for secure and secret information offering and joint effort in the Cloud. We show a fundamental Proxy Re-encryption plan with the chart beneath. A client, say Alice, scrambles her information m, utilizing her open key. When she needs to offer the information with an alternate client, say Bob, she sends the encoded information to an intermediary. The intermediary then changes over the information encoded under Alice's open key into information that is scrambled under Bob's open key and sends this to Bob. Weave can now utilize his private key to decode the figure message and uncover the substance.

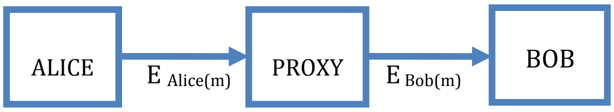

Fig.1: A Basic proxy re-encryption plan

Intermediary Re-encryption for Data Sharing and Collaboration

Various works in writing have propositioned intermediary re-encryption for empowering secure and private information imparting and coordinated effort in the Cloud. Tran *et al.* (2011) utilizes the thought of Proxy Re-encryption plan where the information manager's private key is separated into two sections. One half is put away in the information manager's machine while the other is put away in the Cloud intermediary. The information manager encodes the information with a large portion of his private key, which then gets encoded again by the intermediary utilizing his other 50% of the key. An alternate client who has been allowed access rights will then have the same key isolated with distinctive parts. One half will be continued the conceded client's machine and the other half put away on the Cloud intermediary. The client who has access rights can then recover the information as the intermediary will unscramble the cipher text with a large portion of the client's private enter in the intermediary and afterward decode again on the client's side to recover the full plaintext. At the point when the information holder wishes to repudiate a client from getting to the information, he basically illuminates the Cloud intermediary to evacuate the client's key piece. The primary quality with this plan is that it doesn't oblige re-encryption if a client's rights are repudiated and henceforth saves money on calculation costs, particularly when considering the vast number of clients in gatherings. The model additionally expects that the information holder has officially offered authorization to various clients to get to the information.

4.3. Hybrid ABE and PRE

ABE and Proxy Re-encryption have additionally been utilized as a part of blend with one another to give additional security and protection to information offering and joint effort in the Cloud. Various works in writing are exploiting joining the force of the two plans to give a heartier and ensure further trust in the information holder for the protected imparting of information in the Cloud.

Yu *et al*. (2010) was one of the first works, which consolidated ABE, Proxy Re encryption and languid encryption plans for Cloud security and security. The plan meets expectations by information manager scrambling his information utilizing a symmetric key and after that encoding the symmetric key utilizing a set of credits as indicated by KP-ABE plan. Another client joins the framework when the information holder allots a right to gain entrance structure and its comparing mystery key and circulates this to the new client. To disavow a client, the information holder decides the base number of properties, which will never fulfil the denied client's right to gain entrance structure and redesign these as vital. All the remaining clients’ mystery keys will likewise be overhauled. Because of the overwhelming load of the information holder which may oblige him to be online at all times to give key upgrades, intermediary re-encryption is acquainted with permit the Cloud to do these errands. Thus the greater part of the computational overhead is appointed to the Cloud. The information holder's information is kept secure and confidential at all times as the Cloud is just presented to the cipher text and not the first information substance.

Yang and Zhang (2011) likewise proposed a mix of the ABE plan and Proxy Re-encryption plan to empower secure information imparting in the Cloud. The model includes an information manager, say Alice, scrambling information d with an arbitrary key k.alice then decides an alternate irregular worth k1 and utilizing access control strategy poll, encodes k1 utilizing ABE. Alice then registers k2 utilizing operations on k and k1, ie, k2 = k $*$ k1 and encodes with her open key utilizing intermediary re-encryption. The two keys (ABE key and proxy key) and the encoded information are then put away in the Cloud. Utilizing an authorisation list, if an approved client exists, he can then acquire the intermediary key which is then scrambled with the client's key. Utilizing this, he unscrambles the ABE key, then figure k, ie, k1 $*$ k2 lastly acquires the decoded record. This method guarantees information is kept classified against the Cloud and from any unapproved clients. In the situation that a client is renounced access rights, the information holder basically advises the Cloud to evacuate that client's section in the authorisation rundown and subsequently is computationally proficient. In any case, this plan does not manage the situation where a denied client rejoins the bunch with distinctive access benefits. The disavowed client still has the decryption keys relating to ABE and henceforth in principle can recover access to information he is not permitted.

Liu *et al*. (2012) proposed a clock-based intermediary re-encryption plan (C-PRE) and joined CP-ABE to accomplish fine-grained access control and adaptable client repudiation. In C-PRE, the information holder and the Cloud impart a mystery key and this key is utilized to figure the PRE keys focused around the Cloud's inside clock. The Cloud will re-scramble the cipher text with the PRE keys. Every client is connected with a situated of properties and a qualified time which decide to what extent the client can get to the information. The information itself is connected with a right to gain entrance control structure by CP-ABE furthermore has a right to gain entrance time. At the point when a client appeals record get to, the Cloud decides the current time utilizing its interior clock and afterward utilizes the imparted key to figure PRE keys in time design for all the qualities in the right to gain entrance structure. The PRE keys are then used to re-encode the cipher text. Just clients whose traits fulfil the right to gain entrance control structure and whose qualified time fulfils the right to gain entrance time can unscramble the information. The fundamental advantage with this procedure is that the re-encryption of all the information is designated to the Cloud rather than the information holder and subsequently is productive from the information manager's point of view. The client disavowal issue is likewise tackled since the information must be gotten to if the client's property fulfils the right to gain entrance control structure and their qualified time fulfils the right to gain entrance time. One issue with this strategy however, is that information is re-encoded each time a client makes a right to gain entrance demand. Despite the fact that the re-encryption is assigned to the Cloud, it is still not an exceptionally effective arrangement particularly when considering huge information sizes.

4.4. Discussion

The Table 2 shows a summary of the existing literature based on secure and confidential data sharing in the Cloud. Many of the works reviewed had a strong focus on preventing collusion attacks as well as researching ways for the data owner to be online only when required. In terms of user revocation, some of the reviewed literature showed fast methods of user revocation where revocation involves simply removing a key for instance. Other works required the data to be re-encrypted and the keys to be re-distributed in a secure method and this mainly occurred with works that used ABE techniques. Data sharing and collaboration in the Cloud is still currently a strong focus of research today and in particular many works are focusing on solving the user revocation problem as well as ways to manage the sharing and collaboration of large data sizes.

5. FUTURE DIRECTIONS

In this section, we have investigated writing on approaches to give a safe environment where an information manager can impart information to parts of his gathering while keeping any untouchables from picking up any information get to in the event of noxious exercises, for example, information misfortune and robbery. Then again, all through the section we expect that parts of the gathering won't complete pernicious exercises on the information manager's information. Evaluating and Accountability in the Cloud is a potential for future research in the connection of information offering in the Cloud. As examined in Sect. 1,many clients, specifically associations and endeavours, advantage from information imparting in the Cloud. Be that as it may, there is dependably a probable risk that parts of the gathering can do illicit operations on the information, for example, making unlawful duplicates and disseminating duplicates to companions, overall population, and so on so as to benefit. A future exploration course would be to discover routes for an information manager to consider responsible any part that does malignant exercises on their information. An alternate examination direction would be to give the information manager physical access control over his information. Rather than responsibility, the information holder can make a set of access control leads on his information and send the information alongside the right to gain entrance control strategy. Along these lines, any part with access to the information can just utilize the information as a part of such a route, to the point that maintains the right to gain entrance control strategy. In the event that a part endeavours to make unlawful duplicates of the information, the right to gain entrance control arrangement ought to "bolt" the information to keep the part from doing so. Likewise, since information put away in the Cloud are generally put away and imitated in distinctive land areas as far and wide as possible, it is critical that the legitimate wards are regarded and emulated. A potential examination heading would be to discover approaches to store and methodology information in a manner that does not rupture the security and security laws of the area.

Table 2: Summary of literature on secure and confidential data sharing

Method	ABE	PRE	Likelihood of collusion attacks	User revocation	Data Owner online all times
Tu *et al.*	Y	N	N	S	N
Li *et al.*	Y	N	N	F	N
Tran *et al.*	N	Y	Y	F	N
Yu *et al.*	Y	Y	N	S	N
Yang and Zhang	Y	Y	N	F	N
Liu *et al.*	Y	Y	N	S	N

Y yes, N no, F fast, S slow

6. SUMMARIES & CONCLUSION

Information Sharing and Collaboration in the Cloud is quick getting to be accessible within a brief span of time as requests for information offering keeps on growing quickly. In this section, we displayed a survey on empowering secure and classified information imparting and cooperation utilizing Cloud figuring engineering. We analyzed definitions identified with Cloud registering and protection. We then took a gander at protection and security issues influencing the Cloud emulated by what is consistently done to address these issues. We then talked about why information imparting in the Cloud is paramount and the customary methodology to information offering in the Cloud. We examined key administration in the Cloud and how legitimate key administration prompts more secure and classified information which can help secure and private imparting of information in the Cloud. we surveyed current condition of the- workmanship writing identified with key administration in the Cloud. we clarified the distinctive procedures, specifically ABE and PRE that are right now used to empower secure information offering in the Cloud. We likewise audited current condition of-the-craftsmanship writing in connection to secure and private information imparting in the Cloud and gave a concise review on the fate of information offering in the Cloud where the information holder could have more control over the utilization of their information.

REFERENCES

1. Bennani N, Damiani E, Cimato S. Toward cloud-based key management for outsourced databases. IEEE 34th annual computer software and applications conference workshops (COMPSACW) 2010; pp 232–236.
2. Chavhan BB & Wadhe AP. Review Paper on Security problems in Cloud services. *International Journal of Current Engineering and Technology* 2014; 4 (2):836-841.
3. Chen D, Zhao H. Data security and privacy protection issues in cloud computing. *International conference on computer science and electronics, engineering*, 2012; pp 647–651.
4. Fathi H, Shin S, Kobara K, Chakraborty S, Imai H, Prasad R. LR-AKE-based AAA for networkmobility (NEMO) overwireless links. *IEEE J Select Areas Commun,* 2006*;* 24(9):1725–1737
5. Feldman L, Patel D, Ortmann L, Robinson K, Popovic T. Educating for the future: another important benefit of data sharing. Lancet, 2012; 19; 379 (9829): 1877–1878. doi: 10.1016/S0140-6736(12)60809-5.
6. Geoghegan S. The latest on data sharing and secure cloud computing. Law, Order, 2012;pp 24–26.
7. Goyal V, Pandey O, Sahai A, Waters B . Attribute-based encryption for fine-grained access control of encrypted data. 13th ACM conference on computer and communications security (CCS '06) 2006, pp 89–98.
8. Huang R, Gui X, Yu S, Zhuang W. Research on privacy-preserving cloud storage framework supporting ciphertext retrieval. *International conference on network computing and information security,* 2011:93–97 70
9. Lei S, ZishanD, JindiG(2010) Research on keymanagement infrastructure in cloud computing environment. 9th *International conference on grid and cooperative computing* (GCC) 2010, pp404–407.
10. Li J, Zhao G, Chen X, Xie D, Rong C, Li W, Tang L, Tang Y (2010) Fine-grained data access control systems with user accountability in cloud computing. IEEE second *International conference on cloud computing technology and science(CloudCom)* 2010, pp 89–96.
11. Li M, Yu S, Zheng Y, Ren K, Lou W (2013) Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Trans Parallel Distrib Syst*, 131–143.
12. Liu Q, Wang G, Wu J (2012) Check-based proxy re-encryption scheme in unreliable clouds. 41st *International conference on parallel processing workshops* (ICPPW) 2012, pp 304–305.
13. Mitchley M (2006) Data sharing: progress or not? Credit, Manage, 10–11.
14. 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
15. Sahafizadeh E, Parsa S (2010) Survey on access control models. 2nd *International conference future computer and communication* (ICFCC) 2010, pp V1–1-V1-3.
16. Sanka S, Hota C, Rajarajan M (2010) Secure data access in cloud computing. IEEE 4th *International conference internet multimedia services architecture and application* (IMSAA) 2010,pp 1–6.
17. Sarathy R, Muralidhar K (2006) Secure and useful data sharing. *Decis Support Syst,* 204–220.
18. Tran DH, Nguyen HL, Zha W, Ng WK (2011) Towards security in sharing data on cloudbased social networks. 8th *International conference on information, communications and signal processing* (ICICS) 2011, pp 1–5.
19. Tu S, Niu S, Li H, Xiao-ming Y, Li M (2012): 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.
20. Wang J, Liu C, Lin GTR (2011) How to manage information security in cloud, computing, pp 1405–1410.

21. Wang X, Zhong W (2010) A new identity based proxy re-encryption scheme*. International conference biomedical engineering and computer science (ICBECS)* 2010:145–153

22. 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

23. Xiao Z, Xiao Y (2012) Security and privacy in cloud computing. *IEEE Commun Surveys Tutorials,* 99:1–17

24. Yang Y, Zhang Y (2011) A generic scheme for secure ata sharing in cloud. 40th *International conference parallel processing workshops (ICPPW)* 2011, pp 145–153.

25. Yu S,Wang C, Ren K, LouW(2010) Achieving secure, scalable, and fine-grained data access control in cloud computing. In: *INFOCOM, 2010 proceedings IEEE*, pp 1–9

26. Zhou M (2010) Security and privacy in the cloud: a survey. *Sixth International conference on semantics knowledge and grid (SKG)* 2010:105–112

27. Zhou M, Zhang R, XieW, 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