Int J Pharm Bio Sci 2015 April; 6(2): (B) 494 - 502

Review Article **Applied Science**

International Journal of Pharma and Bio Sciences **ISSN 0975-6299**

TRUSTED AUTHENTICATION AND SECURITY OF MEDICAL DATA IN CLOUD COMPUTING

K. RAMKUMAR*1 AND DR.G.GUNASEKARAN*2

[1] Research Scholar, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli - 627012, India
[2] Principal, Meenakshi College of Engineering, Anna University, West KK Nagar, Chennai-600078, India

ABSTRACT

Cloud computing provides shared, on-demand and scalable services over internet with user's data being processed in remote machines and required services provided. The main barrier in using this new technology in different field is the users fear on data security, availability and integrity of their own data in remote servers. In this paper, an efficient cloud storage system for storing medical records of patients between hospitals located in different countries with data security and integrity has been proposed. Multifactor authentication for user login to cloud, homomorphic encryption for storing the data with integrity checking has been used effectively in the proposed system. Experimental study has been done to demonstrate the effectiveness of the proposed approach.

KEYWORDS: **storage security, integrity, availability, cloud computing**

K. RAMKUMAR
Research Scholar, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli - 627012, India

***Corresponding author**

INTRODUCTION

Cloud computing provides huge storage capability for internet users with cost based on usage of facility. Users store their sensitive data in cloud according to service level agreements they sign and usually the data handling of users are outsourced to cloud service providers. Different entities merge or leave the cloud in elastic manner leading to more complicated key management, searchable encryption techniques, access control etc. Sensitive data are encrypted before outsourcing to cloud thereby providing privacy preservation. This outsourced data will be secure with a service provider while some selected data are shared with other service provider based on service level agreement. The common attacks encountered in cloud are

• *XML signature wrapping attack* where administrative rights of cloud are taken by hacker.
• *Cross site scripting attack* using which hackers bypass access control mechanisms.
• *Flooding attack problem* where the workload of the cloud servers is consumed needlessly.
• *Denial-of-Service attack* where injected *m*alicious code deny services to legitimate users
• *Data stealing problem* where user account and password are stolen by hacker.

The paper is organized as follows: section 2 provides the literature survey; section 3 provides the proposed approach and section 4 the conclusions.

2. Literature Survey

Cloud technology faces the threat of privacy based on services offered by Apple, Google, Amazon [1] according to user's perspective. Privacy preservation of users data is a challenge as the internal operations provided by service providers is not accessible to users. Yanbin Lu and Gene Tsudik [2] listed many issues in preserving privacy in cloud. For preserving cloud privacy, Siani Pearson et al [3] recommended a privacy manager and. Jianwang [4] suggested an anonymity based method. Miao Zhou [5] suggested improved key management for preserving privacy. Qin Liu [6] recommended a keyword searching method based on bilinear graph. Swarnlaet al.[7] suggested computational drug designing which in fact needs huge cloud storage. Marten van Dijk et al [8] concluded that cryptography alone is not adequate to preserve privacy. Yanbin Lu et al [9] suggested an improved method and ShuchengYu [10] proposed an enhanced attribute based encryption. Adi Shamir [11] proposed an 'Identity-Based Cryptosystems and Signature Schemes' that was superior to many other methods. AmitSahai et al [12] proposed fuzzy based Attribute-Based Encryption (ABE). Based on [12], Vipul Goyal et al. [13] proposed 'Key - Policy Attribute-Based Encryption (KP-ABE)' that uses third party. Bethencourt et al. [14] proposed 'Ciphertext-Policy Attribute Based Encryption' (CP-ABE) that provides secure storage for non-trusted server. Lu and Tsudik [2] , using [11,12,13,14] developed a novel cryptosystem for preserving privacy Patients disclose their personal health-related information to doctors for treatment [15]. The Health Insurance Portability and Accountability Act (HIPAA) [16] give protection to patient's health information and allow doctors and nurses to access the data with patient's consent.

3. Proposed model for hospital data management in cloud

3.1 Authentication

In addition to user name and password authentication, multifactor authentication of data user can be used to tighten the security level, when the data accessed from cloud is sensitive. The multi-factors used in authentication can be user ID and password, fingerprint biometrics and random secret keys. User ID and password shows what user know, fingerprint biometric represents what user are, and random secret keys are used for verifying user identity to server. The user can be considered to be a doctor or any healthcare person or can be the person entering or editing records in cloud. Any authenticated user can login to cloud using three stage authentication processes as in Figure 1. First stage is the user name and password authentication, second stage is the fingerprint or iris authentication and third stage is secret key sms sent to user from cloud.

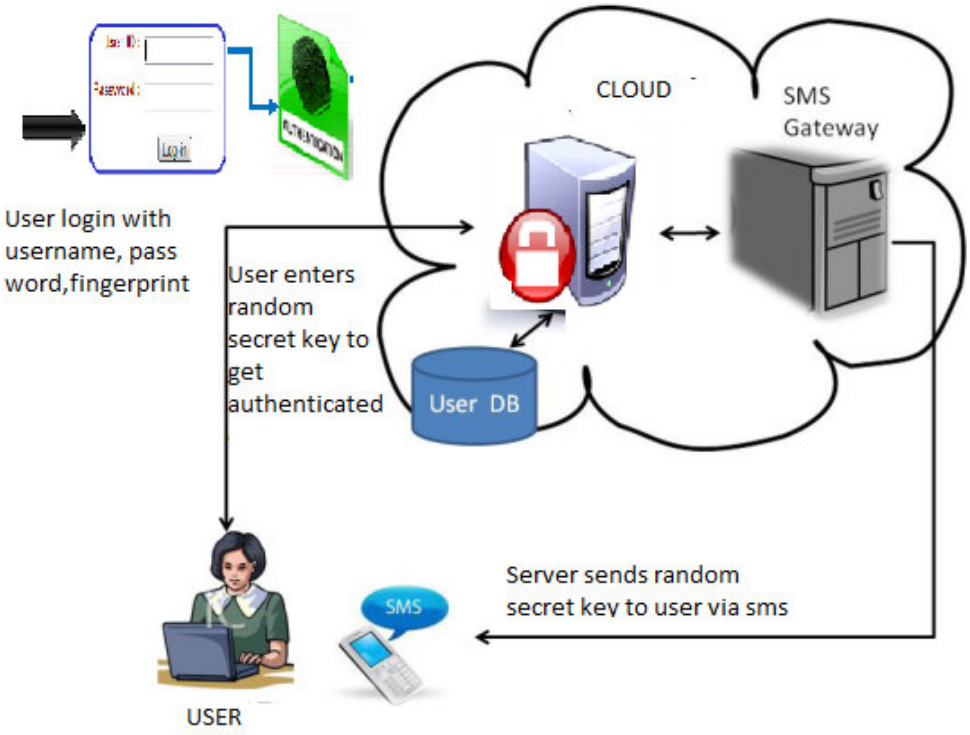

Figure 1
Multifactor authentication by user in cloud

3.2 Encryption and key management

As the patients sensitive private data is stored in cloud with no local copy it has to be encrypted before uploading to preserve privacy and encryption can be done by using RSA/ECC/AES with RSA being the most commonly used encryption algorithm. Efficient key management also becomes an important concern because of the encrypted data. As encrypted data in cloud must support search also, homomorphic encryption is followed in our system. The concept of homomorphic encryption works as given below:

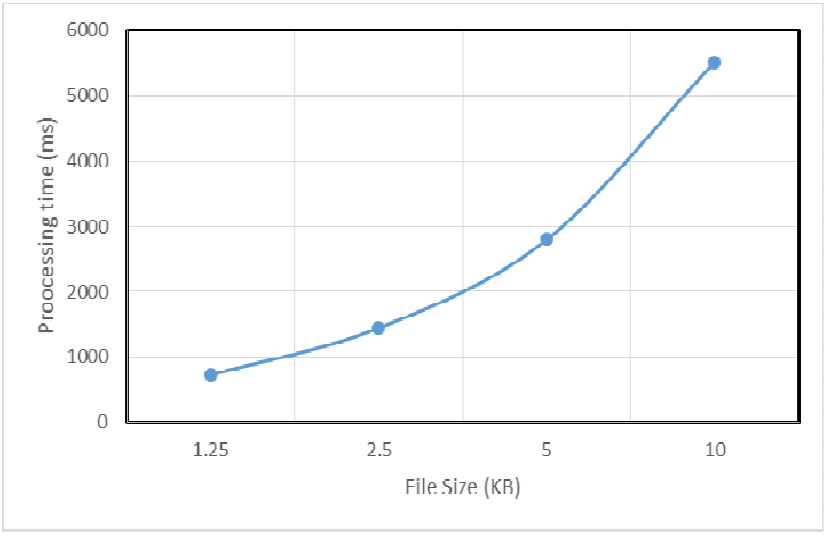

Figure 2
Processing time for generating homomorphic tags.

Let $E_{pk}(.)$ be the encryption function whose public key is p_k and $D_{pr}(.)$ represent the decryption function whose private key p_r. Any homomorphic system must satisfy the requirements given below:

(1) If $E_{pk}(m_1)$ and $E_{pk}(m_2)$ represents the encryption of m_1 and m_2 is, then there exists an algorithm to compute m_1+m_2 public key encryption ie. $E_{pk}(m_1+m_2) := E_{pk}(m_1) +h E_{pk}(m_2)$.

(2) If a constant k and $E_{pk}(m_1)$ the encryption of m_1, are provided then an algorithm to calculate the public key encryption of $k.m_1$ must exist denoted by $E_{pk}(k.m_1) := k \times h E_{pk}(m_1)$. For a data block (whole data is split into fixed size chunks) of length 160 bits, the processing time for generating homomorphic tags for different file sizes are shown in figure 2. It can be seen that as the file size increases the processing time increases. Table 1 shows some important key management literature comparing features like redundant key/data, confidentiality and single failure point.

Table 1
Comparison of selected key management literature

Method	Redundant key/Data	Confidentiality	Single failure point
Lei et al[17]	X	√	√
Sanka et al[18]	√	X	X
Bennani et al[19]	√	√	X

The model for key management can be considered to be containing the following entities

- The cloud provider (C) provides storage services
- The data owner(D) contains the root or master key and has the key management system
- The sub data manager (S) of tree, can derive all child node decryption keys . Each node contains two decryption keys- one decrypts encrypted data of that node and the other finds the keys for the children.
- A user or another sub-tree data manager (U), can use or share S's data.

In this asymmetric encryption (as encryption and decryption keys are different) data stored in each node is encrypted by one encryption key connected with two decryption keys as in figure 3. If e_{ij} is the encryption key and d_{ijk} its decryption keys, i representing the level of a tree, j the index of nodes and k the index of decryption keys. The model can be explained as follows:

- D generates a master key, d_0, that can find all decryption keys and encryption keys.
- Each node obtains a master decryption key d_{ij1} and a secondary decryption key d_{ij2}, generated from root key(d_{ij2} is derived from d_{ij1}).
- S gets the master key d_{ij1}, using which all node keys of the sub-tree, including the secondary keys can be generated.
- User U can request a secondary decryption key d_{ij2} from D for retrieving the encrypted data stored in node N_{ij}.

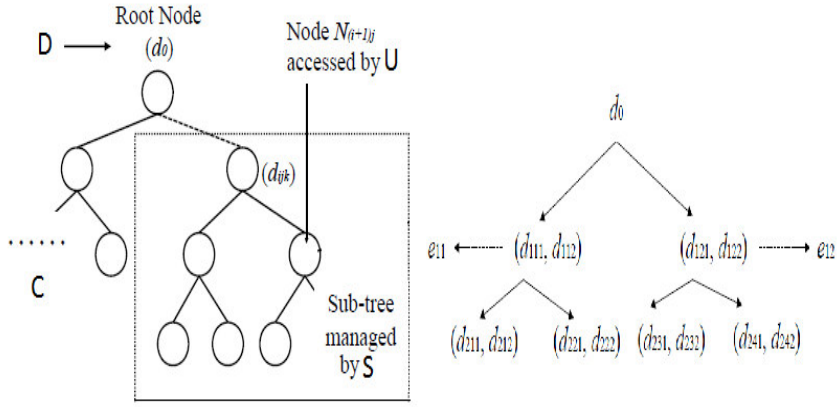

Figure 3
Key derivation procedure

3.3 Data Access Procedure

Attribute based encryption and Proxy Re-encryption[26] are the two powerful techniques that provide extra security and privacy for data sharing and the literature in Table 2 provides the history of the hybrid usage of this technique. The extensive security issues during cloud storage usage are provided in [27].

Table 2
Literature on secure and confidential data sharing

Method	Attribute based Encryption	Proxy Re-Encryption	Likelihood of collusion attacks	User revocation
Tu et al [20]	√	X	X	Slow
Li et al[21]	√	X	X	Fast
Tran et al[22]	X	√	√	Fast
Yu et al[23]	√	√	X	Slow
Yang and Zhang[24]	√	√	X	Fast
Liu et al[25]	√	√	X	Slow

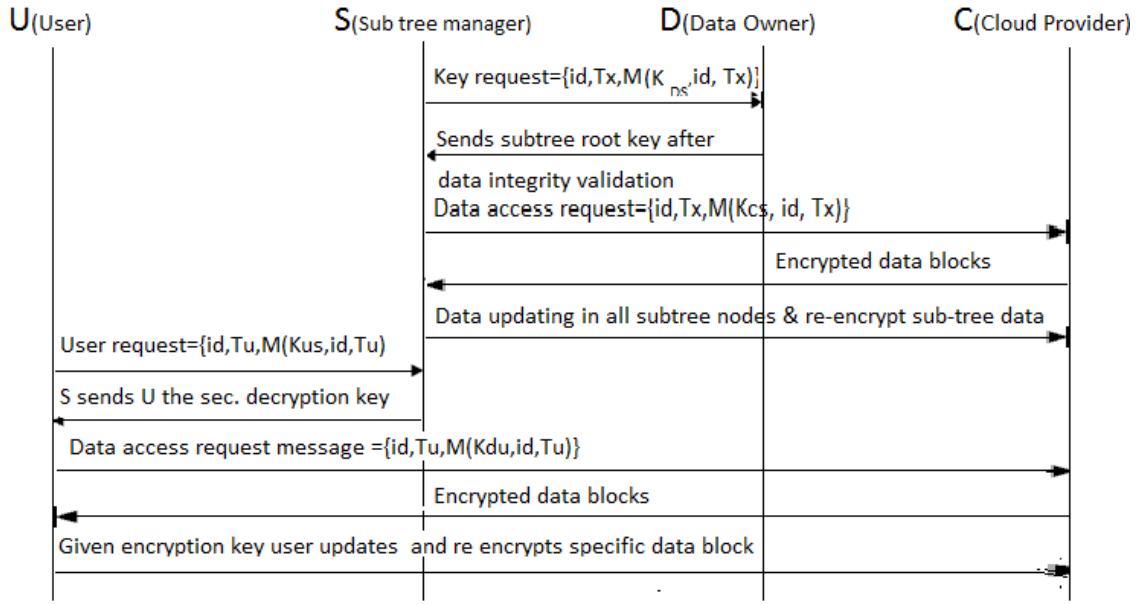

Figure 4
Data access process

The secure privacy preserving data access technique used in the proposed system is shown in figure 4. The confidential data of patients is maintained in cloud by a common data owner D. When a hospital(S) wants to update the details of a patient, it gives a key request to D, who sends a subtree root key after data integrity verification. The encrypted data blocks are sent to S, based on data access request from S to C. The data is updated and sent to C by re-encrypting it.

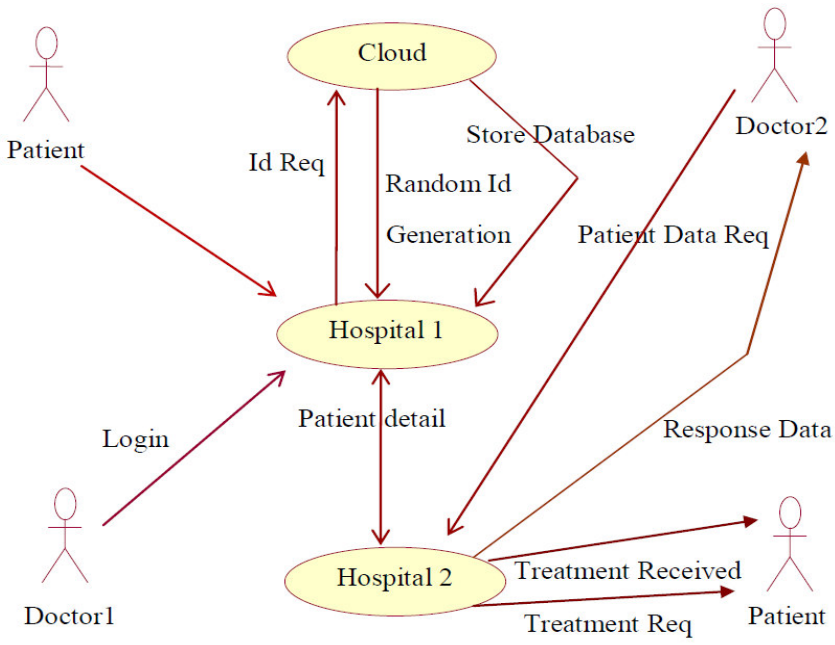

Figure 5
Information flow in hospital cloud management.

When another user U, who may be a healthcare person, wants to access the data to give treatment to the same patient in some other place, gives a request to S, who sends the secondary decryption key. U gives data access request to C, which sends its encrypted blocks. User decrypts it, and if considered legitimate user, can update it and re-encrypt and send to C as in figure 4. In the scenario presented in figure 5, the patient gets admitted in hospital 1. Doctor1 treats him and all his records are collected. The data entry operator in the hospital logs in to the cloud with three stage authentication as in figure 1 stores the encrypted data in the cloud. After some years, if due to another illness, the patients get admitted in another hospital in another country, all his history can be tracked from the cloud and treatment can be received effectively.

3.4 Remote integrity check for private data

Large number of cloud users store their important data and images in cloud servers without having a local copy in their own computers. When data in cloud has to be checked for integrity, checker must take care that data is not lost or corrupted. Downloading large amount of data for checking data integrity is loss of communication bandwidth. Many works [27] were done to design a data integrity checking protocols, which allow data integrity to be checked without completely downloading the data. D uses keygen algorithm to generate public and secret key (p_k,s_k). TagGen generates homomorphic tags for all data blocks and sends it to C along with P_k and data blocks. Verifier V request integrity check for data blocks of file M. V generates a challenge to C and verifier checks the integrity of outsourced data as in [28]..Computational cost at verifiers and server with different file length and fixed block size ($2^{16)}$ is shown in figure 6.

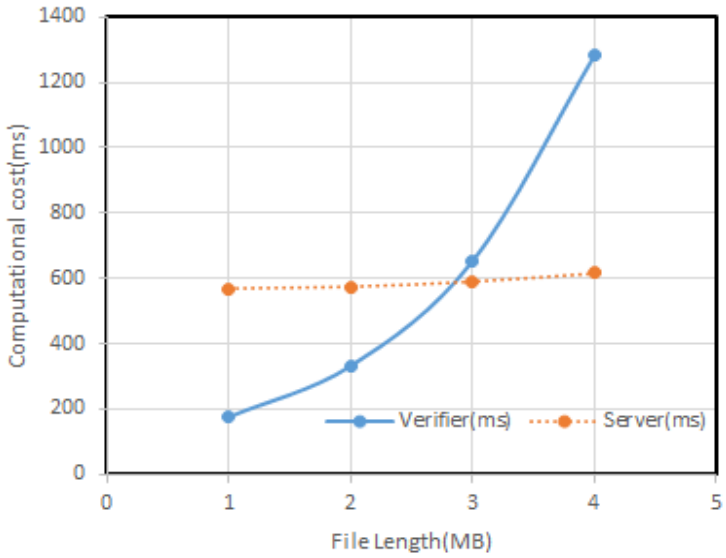

Figure 6
Computational cost comparison at verifiers and server

Figure 7 shows the preprocessing time of client with different block length. It can be inferred from figure that as block size increases, the processing time also increases.

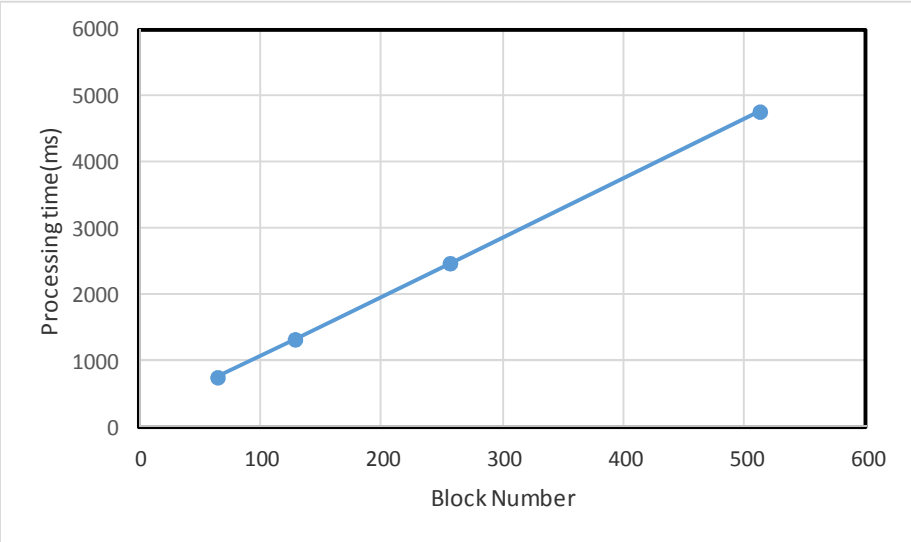

Figure 7
Clients preprocessing time with different block length

4. CONCLUSION

In this paper, a new technique for securing data access and integrity checking of medical data in cloud has been proposed. The proposed architecture provides three stage authentication, secure data access and public verifiability. The proposed method is secure against unauthorized access, untrusted server and also against third party verifiers. The experimental results shows that the proposed method is very efficient with the only drawback being that during data modification, the tags and blocks must be updated with computation and communication costs. Our future work will concentrate on developing access control for different level of users.

REFERENCES

1. Security Challenges for the Public Cloud. Kui Ren, Cong Wang, and Qian Wang.*Internet Computing, IEEE.* 16, 1(2012).
2. Privacy-Preserving Cloud Database Querying. Y. Lu and G. Tsudik. *Journal of Internet Services and Information Security (JISIS)*. 1, 4(2011).
3. A Privacy Manager for Cloud Computing. Siani Pearson, Yun Shen, Miranda Mowbray. First *International Conference, CloudCom* Proceedings(2009).
4. Providing privacy preserving in cloud computing. Jian Wang, Yan Zhao, Shuo Jiang, Jiajin Le, *Test and Measurement*, *vol. 2, ICTM '09, International Conference.*(2009).
5. Privacy enhanced data outsourcing in the cloud. Miao Zhou , Yi Mu , Willy Susilo , Jun Yan , Liju Dong. *Journal of Network and Computer Applications.* 35. 1367–1373, 4(2012).
6. Secure and privacy preserving keyword searching for cloud storage services. Qin Liu, Guojun Wang, Jie Wu. *Journal of Network and Computer Applications*. 35, 927–933 (2012).
7. Computational drug designing. Swarnla, Panchal, Balasubramaniam and Kulshestra. *Int J Pharm Bio Sci.* 3,3 (2012).
8. On the Impossibility of Cryptography Alone for Privacy-Preserving Cloud Computing. Marten Van Dijk, Ari Juels. *IACR Cryptology*, (2010).
9. Drivers of SaaS-Adoption – An Empirical Study of Different Application Type, Alexander Benlian, Thomas Hess, Peter Buxmann. *Business & Information Systems Engineering*, 1, 357-369, 5(2009).

10. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing, Shucheng Yu Cong Wang, Kui Ren , Wenjing Lou, *INFOCOM*, IEEE Proceedings (2010).
11. Identity-Based Cryptosystems and Signature Schemes. Adi Shamir. *Proceedings of CRYPTO 84*
12. Fuzzy Identity Based Encryption. Amit Sahai, Brent Waters, *24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Proceedings Aarhus, Denmark, May 22-26, (2005).
13. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. Vipul Goyal,Omkant Pandey, Amit Sahai, Brent Waters. *Proceeding CCS '06, Proceedings of the 13th ACM conference on Computer and communications security*,ACM, 89 - 98 (2006).
14. Ciphertext-Policy Attribute-Based Encryption, Security and Privacy. John Bethencourt, Amit Sahai, Brent Waters,(2007).
15. Saying privacy, meaning confidentiality. Schwab AP, Frank L, Gligorov *N Am J Bioeth* 44–45. (2011).
16. HIPAA Privacy (2012) U.S. Department of Health and Human Services. Source: http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html. Accessed on Nov 2014
17. Research on keymanagement infrastructure in cloud computing environment. Lei S, ZishanD, JindiG. *9th international conference on grid and cooperative computing* (GCC), pp 404–407(2010).
18. Secure data access in cloud computing. Sanka S, Hota C, Rajarajan M. *IEEE 4th international conference internet multimedia services architecture and application(IMSAA)*, pp 1–6(2010).
19. Toward cloud-based key management for outsourced databases. Bennani N, Damiani E, Cimato S (2010). *IEEE 34th annual computer software and applications conference workshops (COMPSACW)*, pp 232–236(2010).
20. Fine-grained access control and revocation for sharing data on clouds.Tu S, Niu S, Li H, Xiao-ming Y, Li M. *IEEE 26th international parallel and distributed processing symposium workshops and PhD forum (IPDPSW)*.2146–2155(2012).
21. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. Li M, Yu S, Zheng Y, Ren K, Lou W. *IEEE Trans Parallel Distrib Syst* 131–143. (2013).
22. Towards security in sharing data on cloud based social networks. Tran DH, Nguyen HL, Zha W, Ng WK. *8th International conference on information, communications and signal processing (ICICS)*. pp 1–5(2011).
23. Achieving secure, scalable, and fine-grained data access control in cloud computing.Yu S,Wang C, Ren K, LouW*In: INFOCOM, 2010 proceedings IEEE*, pp 1–9(2010).
24. A generic scheme for secure data sharing in cloud. Yang Y, Zhang Y. *40th intl. conference parallel processing workshops (ICPPW)*. 145–153(2011).
25. Check-based proxy re-encryption scheme in unreliable clouds. Liu Q, Wang G, Wu J. *41st international conference on parallel processing workshops (ICPPW).* pp 304–305(2012).
26. Attribute-Based Encryption With Verifiable Outsourced Decryption. Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng. *IEEE Transaction on Information Forensics and Security*, 8, 8(2013).
27. Security Issues with Possible Solutions in Cloud Computing-A Survey. Abhinay B. Angadi, Akshata B. Angadi, Karuna C. Gull. *International Journal of Advanced Research in Computer Engg. & Technology (IJARCET)*.2,2(2013).
28. Zhou, Miao, Data security and integrity in cloud computing, Doctor of Philosophy thesis, School of Computer Science and Software Engg., University of Wollongong (2013).