Privacy Assurance with Content Based Access Protocol to Secure Cloud Storage

Vitthal Sadashiv Gutte and Kamatchi Iyer

1 Introduction

In cloud computing, security is the most important constraint which is only the main focus of this study and implementation. There are different modules like Encryption process module where processes will do. The Decryption process module works on keys to get the files. The Splitter module helps to split the data in given input format. The joiner module uses the method to provide higher level of security in the process. In the process of encryption change the original content of input with some code to add the security to the data. The method of encryption includes some private key used to encrypt the data. Dynamic nature of Moving data in cloud servers provide more reliable to end users. In the context of resource management and data management user should not have worries about the privacy in public cloud if the method used is appropriate. There are many people and organization they are trying to solve the problem since so many days and years [1]. The security and privacy concern more when we are using personalized cloud so it's part of private cloud in the environment. Now a day's several pioneers are there for cloud vendors such Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3).The providers take care of security of data and maintenance on behalf of users so less worries about the complexity. The vendors provide huge amount of data storage with respective of personal or organizational request. The time of use and majorly security factors prove the vendors choice on public and private cloud. Hybrid Cloud uses regularly more security approach as the part of both the systems [2].

In the process of higher security aspect encrypted data added one more encryption again to provide different level of security in the content. In context of process

V. S. Gutte (✉) · K. Iyer (✉)
Department of Computer Science and Engineering, Amity University, Mumbai, India
e-mail: 1vitthal.gutte@mitcoe.edu.in; Kamatchi.iyyer@amityunivery.edu.in

S. Smys et al. (eds.), *New Trends in Computational Vision and Bio-inspired Computing*, https://doi.org/10.1007/978-3-030-41862-5_10

decryption with the help of the public key of owner we can get the decrypted data in original form to particular user, and hence security to the data is provided [3]. Before encryption the original data is splitter into chunks with the help of Splitter module. And during Decryption all the decrypted chunks get joined together with the help of the Joiner module. Attribute revocation means to get or to revoke the original data which is encrypted. Multi-authority cloud storage means multiple users can use the data to store and download from the cloud. In such a way higher level of security is provided in cloud storage [4].

Aspect of security standalone there when we share data or image. The danger factor in publishing your digital media online, whether you are publishing the data professionally or just putting images on your personal website or blogs. Creating a watermark with different methods, for digital media whether it is images or videos is a great way to discourage people from copying general or personal photos that you have on your website or any portal available online [5]. While still allowing the image to be seen. The watermark proves you're your own work this helps to avoid same data use by different people. The courage of person will get reduced when the system is used. The person can claim the data ownership if he puts watermark. As a cloud is open source so concern of security and data ownership is the big task as well storage space maintaining also occurs[6, 7].

Cloud providers provide the services in the network where information security regarding the data availability for all users. Data in a system should be secured to find the authenticity of users for the different operations. The infrastructure of cloud deeply works with to provide the central user level security and infrastructure level security. In the process major concern of adoption of design required to play a vital role for cloud computing infrastructure. The cloud helps in future to provide new version of success in networking across the globe. As the history of cloud it has brought different benefits which were unpredictable. It has different computing model to use at different level to gain maximum profit and security in different resource usage [8, 9].

Aspect of security not provided in cloud computing where many companies have their own structure of security. The different structure provides the level of security on the data and different resources. The cloud is open to all so breaching the security is easy for the different attacker. We are providing a new security architecture and uniform solution to have in all types of cloud new security architecture which tackle the problem of data in cloud. One of the major thing of cloud with correction and data integrity where the unauthorized servers. The servers act as a proxy server which should stop with the different solution in the major concern [10]. The unique type of security has been approached to provide the solution for both the problems. The infrastructure of different stake holders which need to act at a different. As an example byzantine attack make more damage to user this may be more serious when saving more money and different benefits Without local copy of data it can have a solution where the client will have efficient way system to communicate over the cloud. The system will check the integrity periodically this will help to avoid untreated resources in the cloud environment [11] (Fig. 1).

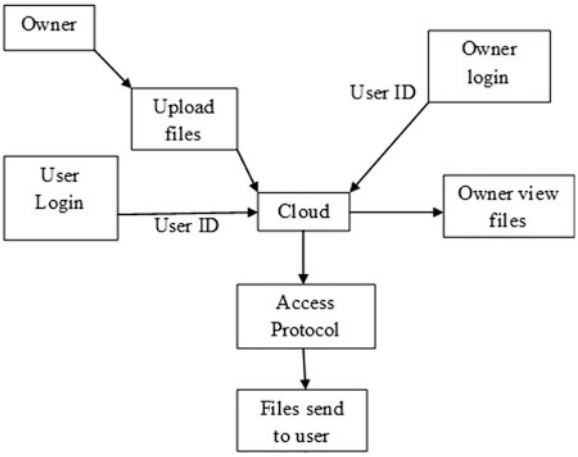


Fig. 1 Basic structure

2 Literature Survey

[12] In a research work author has addressed the different challenges of the credential leakage in the algorithm. He has used the CP-ABE. The cloud storage system designed by the accountable authority and recoverable crypto cloud. This supports to the white box testing traceable and auditing in the cloud environment. The crypto cloud system is used. This system also supports to accountable authority over different aspects in cloud. The task of effective revocation performed here CryptCloud+ helps to find trace and find malicious cloud users of Leaking credentials. The method also supports to the different issue like if user's credentials are distributed across the system then this helps to reunite it. The distributed across the network by the semi trusted authority. In implementation they have used Parallel which is same as encryption method for serving as an extractable assurance white-box traceability method. In improving efficiency process of tracing they have used light weight extractable commitment for it. The algorithm used for this is used taking master secret key for input. This helps to achieve white box traceability to find the users in cloud which has malicious behavior. Author also fails to provide fully and partially public tracing ability to with greater performance or same performance.

[13] Researchers work has main focus on implementation of a software system. The generated prototype which implements access control architecture. This system helps to store the data in cloud environment which is completely untrusted as a concern of security. While implementing this idea system algorithm checks different aspects of it. The acceptable complexity, functionality and also for the complexity in implementation. It has some key benefits such as ability to customize the policies while accessing data without duplicating. On cloud large number of users available to participate in the same system. One more important ability is dynamic accessing the data. The unaffected users need no to change the data or no need of faction on that data for regular changes. The integrity of all transaction and about that data

which need grant the permission of access or change the content is maintained. The system uses block chain and smart card to provide the access. They have used different accesses like facts gain access of a file. Inability to edit the data guaranteed.

[14] While implementation of research works the author used different approach to tackle the problem and give the appropriate solution. The combined method of cloud infrastructure side and data owner side which provide access control but completely in encrypted form on cloud storage. This resist to, which is resistant to DDoS attacks as well EDoS attacks. This is efficient which provide the resource consumption in process. The system supports CP-ABE (cipher text policy attribute based encryption). The system is completely secure against the attack from malicious data users. They have provided architecture which supports to avoid covert cloud provider in architecture. They have provided a relaxed architecture which works with semi trusted provider which is more practical and much more relaxed notation. In process of providing more security or use of covert security used the bloom filter. At a same time probabilistic checking is done for resource consumption accounting. This reduces the overhead. With the performance testing it proves that overhead of system construction is marginally small over the present system.

[15] In this work, stated two different attacks first give two attacks on DAC-MACS and EDAC-MACS in this work. This attack has shown for the backward security revocation. Then they have introduced a new control scheme for multi authority cloud storage system. The NEDAC-MACS is introduced to avoid the vulnerabilities. The helps to enhance the revocation security system. The method can with stand of two different vulnerabilities. This works even the non-revoked users reveal their received key to revoked users. NEDAC-MACS method has ability to withstand the two different vulnerable capabilities. Even though both are non-revoked users. They reveal their received key, update keys to the revoked user in the environment while working at a same time. In the process of action the NEDAC-MACS the users has no chance to decrypts any objective cipher text. Even the actively eavesdrop to obtain an arbitrary number of non-revoked users key update. It accept any transmitted information likewise Cipher text Update Keys CUK. It works ahead with the formal cryptanalysis of NEDAC-MACS which is presented to assure the more security. At last stage they have proved simulations which prove that overall storage, communication, computation, working efficiency, overheads etc. works more guaranteed working in positive direction (Table 1).

3 Existing System

As we can find different solutions. Now the different author has proposed solutions in their own ways like frameworks. One of the method available is called OIRS. The methods works like the outsourced image recovery service. The technique used in compressed with sense of privacy assurance. Author has main focus on secure outsource the image which is stored on cloud. The image has exploit techniques from different domains and aim to provide the security. The image circulation in

Table 1 Taxonomy table

Paper	Technology used					
	Cryptographic techniques	File splitting	Compression	Access control	Authentication	TPA
Privacy-Assured Outsourcing of image reconstruction service in cloud	✓		✓	✓		
Secured outsourcing of image reconstruction service in cloud using attribute based encryption	✓		✓	✓		✓
Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage	✓			✓	✓	
An Analytical study on stereo image using DCT-II and vector quantization			✓			
Privacy preserving approaches in cloud				✓	✓	✓

environment of cloud where the security is prime concern in all aspect. The author has proposed an architecture which contain the process and different methods which helps to provide the infra-structure architecture in a path which provide correct solution. [16]. the method of OIRS has a unique capability. The data owners have rights that they can use the benefits of compress sensing to consolidate sampling. The image compression via only one path that with linear measurements in process. In a process Data users can leverage clouds abundant resources to outsource image recovery optimization. This works without revealing either compressed sample or the content of that image which underlying in process. In the architecture it shows very simplicity but it provides the robustness and achieve the efficiency which is required. The proper approximation is done with image data. Sparse data or non-sparse data is managed with approximation algorithm.

4 System Architecture

In this paper we have proposed a new architecture which provides the solution to security approach in cloud. The scheme is distributed and dynamic. This approach helps to provide flexibility and ensure data security with the highest priority. The user's data on the cloud is always correct this assures with data correction always

with dynamic approach. The file storage preparation to provide the guarantee of data dependability and redundancies in the environment. The scheme provides the correction of infrastructure with greatest values of security. The data confidentiality plays the vital role over the operations from one stake holder to other stake holder in the cloud environment Most of the time the trusted and secure transfer of data required which is provided with our system. We have used a secure encryption system for the effectively and efficiently working on data. The security is always main concern while working on storage data.

The cloud environment has one of the major problems with entrusted cloud servers which are heavily traffic and large number in data. To ensure the access control on data while it's in part of use with different stakeholder in the global presence. This problem mast be tackled by the system architecture which is provided by us. We always ensure about the data security with use of splitting data methodology and maintain the access control on same data. For the splitter we have used one approach which is capable to provide enough support in our architecture. While working on it we also work on minimizing the cost obn cloud with use of compression technique. This technique provide us the guarantee of data originality while accessing it (Fig. 2).

Owner of data: One of the stake holders of our system which has complete rights on data He is the One most important apart of system. This entity has the rights on data and he would like to share his/her data with different stakeholders. He can outsource that to cloud servers. All the cloud servers managed by the cloud service providers in global presence. The owner of data defines the different access policies with their own attributes. The multi authority scheme is used to perform the task of allocation of access. The owner sends the compressed data to the cloud servers which are late on used by the different stake holders.

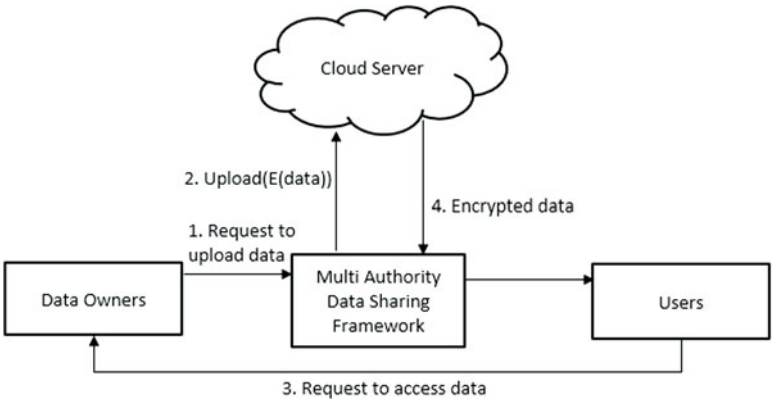
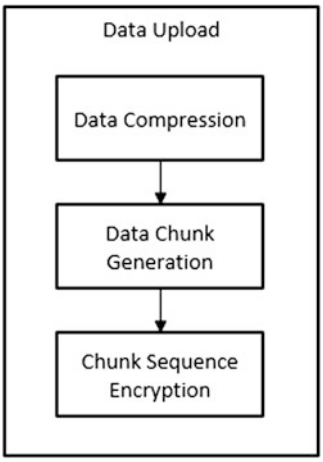
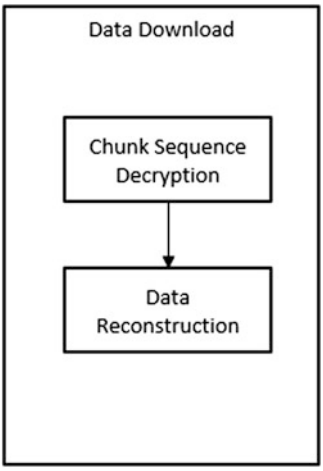


Fig. 2 System Architecture



4.1 Owner Side Functionality

User in system: The cloud architecture is used by everyone from anywhere. Every user has a unique identification in the system to locate in system. Also the users have multiple attributes and a secret key for the security concern. Users have multiple categories in a system which defines with their access policy controls. Everyone has some limitation while they are interacting in the system.



4.2 User Side Functionality

Upload Module: The module works where the uploading process is going on the different tasks perform as follows.

File Compressor: The file compressor works on the images. The module accept input as a image input and perform the compression technique using the DCT algorithm for particular task. After the image compressed then owners signature is added to that image with the watermarking. The watermark is invisible for the users.

1. Compute four filters with hear wavelet transformation that is Lo_D, Hi_D, Lo_R, Hi_R
2. Perform Wavelet Decomposition of input image with input level using calculated wavelet Lo_D, Hi_D which returns decomposition vector c and bookkeeping matrix s
3. Calculate threshold and number of coefficients for compression.
4. Perform level dependent compression with the help of calculated decomposition vector c, bookkeeping matrix s threshold and input level

File Splitter: This module works for the diving a file. The image will get split in to 10 different chunks with allocated size. One Meta data file also generated which contained all chunk files sequence. This also stored on the clouds. The chunks are encrypted as well Meta data file also encrypted.

Image division into chunks:
Input: Image I
Output: Image chunks

1. Read(I)
2. Image size = file Byte Array. length
3. chunk size = image size / chunk number
4. for each sub chunk size in chunk size
5. Write sub chunk size
6. Store sub chunk size in metadata file

Encryption: This module also takes Meta data file as an input for encryption. We are using AES for the encryption.

AES Encryption:

In a process of encryption it has specially derived keys. I called the round keys. They are applied along with different other operations. On array data holds exactly

on block of data. Data to be encrypted with the format. This array called as a state array.

Steps of encryption for a 128-bit block:

1. Derive the set of round keys from the cipher key.
2. Initialize the state array with the block data (plaintext).
3. Add the initial round key to the starting state array.
4. Perform nine rounds of state manipulation.
5. Perform the tenth and final round of state manipulation.
6. Copy the final state array out as the encrypted data (cipher text).

4.3 Download Module

Joiner for the file: In a process of downloading the any image it has to follow the specific process. The process deals with a sequence of allocation process. The joiner gets the location of that image where the spitted file present. The meta data file help then to join the allocated place. The all are in encryption form. In a process of downloading any image file joiner get all detail sequence of chunks from a specific location. The data is present in spitted format and sequence present in metadata file.

Image division into chunks:
Input: Image chunks
Output: Image I

(1) For each chunk in image chunk
(2) File Byte Array = Read(chunks)
(3) Image .append (file Byte Array)
(4) Write Image

4.3.1 Decryption

This module is as part of file joiner module. The module possess the data encrypted Meta data file. The joiner help to find the sequence of chunks in the Meta data and then the chunks' get arranged in sequence. The different chunks also in encrypted form so first get decrypted in the allocated format. The sequence of the procedure follows in process of downloading. The chunks then get attached and the image will be retrieved at the last. The user can download at last. Compete process of join will

be done after the request from another user only. For the same data owner should accept the request for that.

4.4 Storage Allocation Module

Here we are going to show our mathematical model and how data storage cost, request cost for the operations, data transfer cost in process and average storage allocation cost in cloud computing process with our architecture.

ST—Allocation of database storage in binary, TR—Number of data transfers for dataset from storage to site.

DB Size—Size of database in GB, DB Usage—Percentage of database accessed per user DB Req—Number of monthly storage requests in database for per user, Per Req Cost—Cost of each request from user

$$AvgST = \frac{STCost + TRCost + ReqCost}{Total\ GB\ stored} \tag{1}$$

$$STCost = \sum DBSize \times Cst \times ST \tag{2}$$

$$TRCost = \sum TR \times DBSize \times DBUsage \tag{3}$$

$$ReqCost = \sum ST \times DBReq \times perReqCost. \tag{4}$$

Our goal is to minimize the cost which will affect while storing data on cloud. The optimization of the storage is going to check. Our approach is to provide maximum storage but same time should follow the lower cost. The computing task performs on the different attribute so need to have more efficiency in occurring process. We come up with a formula which we have been stated earlier.

5 Experimental Results

In a process of execution we had taken parameter as execution time for the result in environment of our architecture. We have taken different images with different sixe and check the performance. We has checked every image for the total compression time in the process. We have also calculated the splitting time for different sizes. Table 2 shows the different images with different storage size is taken all the size in kB. We have checked the respective execution time for compression process with our approach (Fig. 3).

Table 2 Execution time for compression

Image	Size (kB)	Execution time
Allante	130	149
Imagerain	256	198
Sounchy	319	212
Violin	455	309

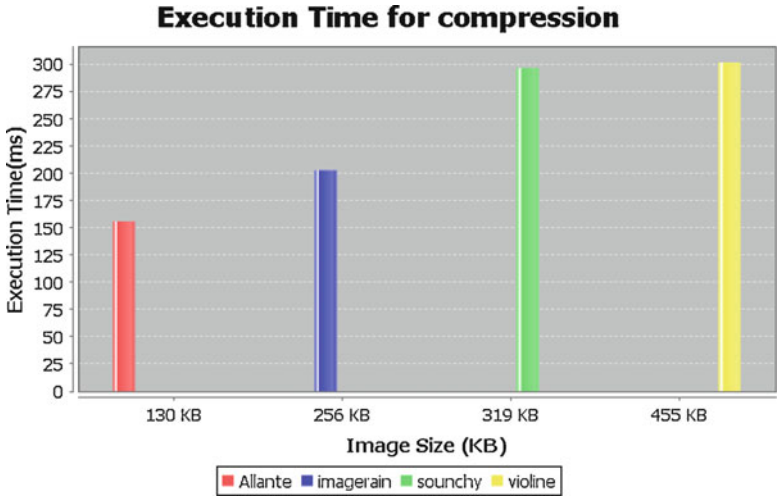


Fig. 3 Execution time for compression

Table 3 Execution time for spliting

Image	Size (kB)	Execution time
Allante	130	47
Imagerain	256	49
Sounchy	319	78
Violin	455	84

Table 3 shows that the splitter for the images, the execution time for the split proceess get calculated (Fig. 4). The size of different size of images considered.

Table 4 shows that the image reconstruction time required for that perticular image. The process of chunk reconstruction is calculated even if its in enrypted from (Fig. 5).

Table 5 has shown the owner and user data process is calculated in milliseconds in a complete process. The complete execution is calculated with the given result (Fig. 6)

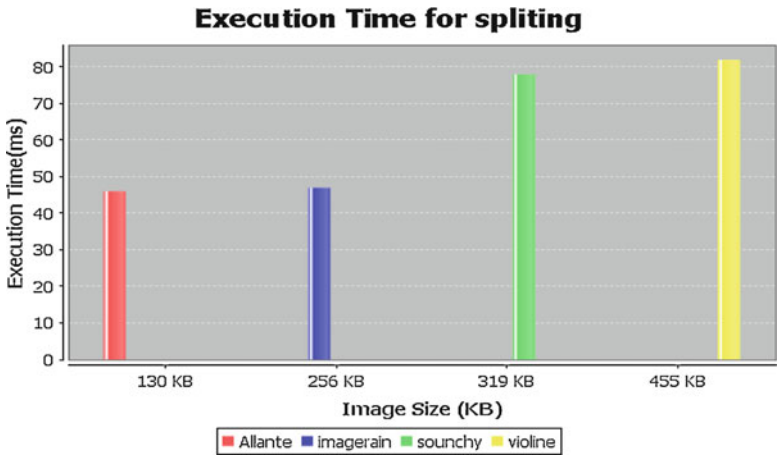


Fig. 4 Execution time for spliting

Table 4 Execution time image reconstruction

Image	Size (kB)	Execution time
Allante	130	24
Imagerain	256	28
Sounchy	319	31
Violine	455	37

Table 5 Owner and user process in ms

Image size (kB)	SOIRSCUABE owner	SOIRSCUABE user	PIMC owner	PIMC user
64	3081	8	47	43
728	3154	9	84	80

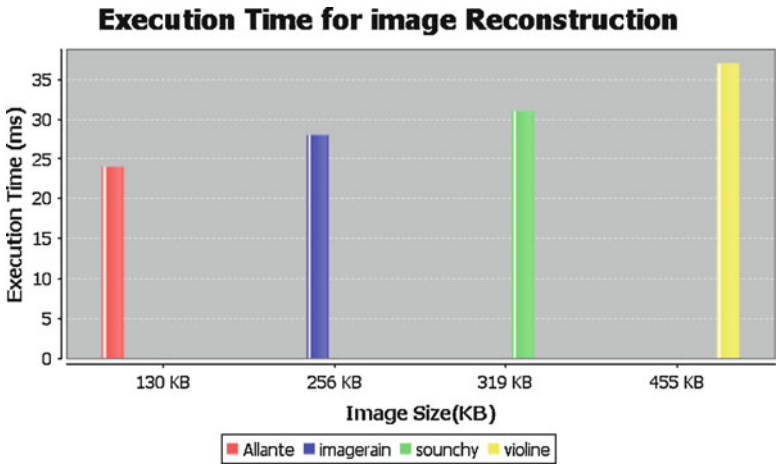


Fig. 5 Execution time image reconstruction

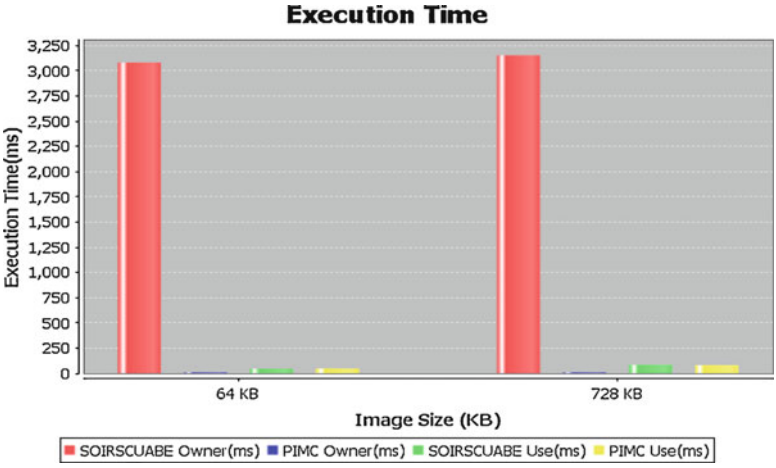


Fig. 6 Owner and user process in ms

6 Conclusion

We have received different results of our implemented system. Earlier the system has some lacuna which we have removed with our approach and provided a solution towards different aspects. We have provided more security in cloud storage data with minimum cost for that application.

References

1. CONG WANG1,BINGSHENG ZHANG2 KUI REN2 AND JANET M. ROVEDA3 "Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud" IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING 2013
2. M. Zhou, R. Zhang, W. Xie, W. Qian, and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," in Proc. SKG, 2010.
3. Kan Yang, and Xiaohua Jia, "Expressive, Efficient, and Revocable Data Access Control for Multi-authority Cloud Storage", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,Vol.25, No.7, pp. 1735–1744, 2014.
4. Ming Li, Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption" *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013*
5. Syam Kumar P, Subramanian R Department of Computer Science, School of Engineering & Technology Pondicherry University "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011

6. Vitthal S. Gutte, Priya Deshpande "Cost and Communication efficient auditing over public cloud" 2015 CICN 978-1-5090-0076-0/15 $31.00 © 2015 IEEE DOI https://doi.org/10.1109/CICN.2015.164
7. C. Rolim, F. Koch, C. Westphall, J. Werner, A. Fracalossi, and G. Sal-Vador, "A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions," in Proc. ETELEMED, 2010.
8. Raghavendra G, I. Manimozhi "Secured Outsourcing of Image Reconstruction Service in Cloud Using Attribute Based Encryption Raghavendra" India International Journal of Engineering Technology, Management and Applied Sciences June 2014, Volume 1 Issue 2 ISSN 2349-4476
9. R. Hummen, M. Henze, D. Catrein, and K. Wehrle, "A Cloud Design for User-controlled Storage and Processing of Sensor Data," in Proc. IEEE CloudCom, 2012.
10. H. Takabi, J. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security & Privacy, vol. 8, no. 6, 2010.
11. A. Acquisti, and J. Grossklags, "Privacy and Rationality in Individual Decision Making", IEEE Security and Privacy pp. 26–33. Vol. 3 No. 1, IEEE, 2011
12. Jianting Ning, Zhenfu Cao, Senior Member, IEEE, Xiaolei Dong, Kaitai Liang, Member, IEEE, Lifei Wei, and Kim-Kwang Raymond Choo, Senior Member, IEEECryptCloud+: Secure and Expressive Data Access Control for Cloud Storage DOI https://doi.org/10.1109/TSC.2018.2791538, IEEE 2017
13. Ilya Sukhodolskiy, Sergey Zapechnikov Department of Cryptology and Cybersecurity National Research Nuclear University "MEPhI Blockchain-Based Access Control System for Cloud Storage" 978-1-5386-4340-2/18/$31.00©2018 IEEE
14. Kaiping Xue, Senior Member, IEEE, Weikeng Chen, Wei Li, Jianan Hong, Peilin Hong Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage DOI https://doi.org/10.1109/TIFS.2018.2809679, IEEE
15. Xianglong Wu, Rui Jiang, and Bharat Bhargava, Fellow, IEEE "On the Security of Data Access Control for Multiauthority Cloud Storage Systems" DOI https://doi.org/10.1109/TSC.2015.2441698, IEEE
16. CONG WANG1, BINGSHENG ZHANG2, KUI REN2, AND JANET M. ROVEDA Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud 2168–6750 2013 IEEE