

PREVENTION OF UNAUTHORISED CONTENT SHARING USING WATERMARKING AND PROXY RE-ENCRYPTION IN CLOUD

¹Dr.S.Muthusundari,²Damisetty Hima Bindu ,³AishwaryaVinod Menon, ⁴Harshini S

¹ Associate Professor, Department of CSE, R.M.D. Engineering College, Kavaraipettai
^{2,3,4} Final Year Student, Department of CSE, R.M.D. Engineering College, Kavaraipettai
Mail: sms.cse@rmd.ac.in

Abstract- Cloud security consists of security measures to protect cloud-based systems and data, by introducing authentication rules for all individuals involved in it. However, such security measures may have fallen short. In one such case is the problem of security threats where the user that requests data, after getting access to the said data may try to send it to reveal it to a certain unauthorized user. This could potentially cause a crippling loss to the content provider. The content provider uploads cloud-based media files as encrypted format. When a user requests access to this content, the content provider rewrites the content using the new key and sends it to the requested user. After accessing cloud-based content by users, if they republish this content in the cloud, then this file could not be uploaded to the cloud and are considered users of unscrupulous behaviour. Allows secure distribution of exported media content to authorized users, while allowing you to track and redistribute illegal content in an appropriate manner. This paper analyses how water marking and bi directional proxy re-encryption can be used to reduce the security threat of unauthorized content sharing in cloud environment.

Index terms- filtering, Global recommending, Cluster, Quantization, Collaborative, Security

I.INTRODUCTION

These days, mixed media utilization is progressively turning into a fundamental piece of daily existence for end clients to get to various assets, and applications. An increasing number of mixed media content is created and shared every day[4]. There is an immediate need of big data storage whose basic requirement is to guarantee the confidentiality of the data while maintaining anonymity of the service clients[10][14][15]. Content suppliers also look towards distributed computing for media storage and sharing, as it can give cheaper, requested client maintenance and estimation. To ensure privacy of the content and anonymity if the client access control is the best and most fundamental security function [21][22]. Access control helps sharing information in a controlled manner by applying control over which resource can be accessed by which client and how much of that resource he can access based on a permission relationship between attributes of the user and resource [7][12][13]. Subsequently, it is vital to install security in making a cloud-based media sharing assistance right from the start, which gives access control to permit just approved admittance to posted media content[16]-[19].

To help oversee secure media sharing admittance to a cloud-based media place, there are two well-known strategies in the writing[2]. The first approach depends on Attribute based encryption (ABE), a related access structure provided over attributes, at the same time ciphertext with cloud code can be used to allow clients with credentials that fulfill policies and eliminate the rest[9]. The most recent rendition is Proxy Encryption (PRE), where an intermediary party is introduced to give the privilege to approved clients in a controlled manner. The key difference between ABE and PRE is that the content provider must download and decrypt the encryption and then again encrypt it in ABE[20]. This becomes a very tiresome task as the access control policies are continually evolving. However, that is not the case in PRE where an already encrypted version can be re encrypted by the intermediary party before providing it to the authorized client[1][6][7][8].

Watermarking helps us in fair-traitor tracing. When some content from the cloud content provider is shared to a client a distinct water mark is given to that particular content [24]. When a content is shared illegally, we can find the traitor just by scanning the content for watermark[23]. However, there are some limitations of watermarking. Here, we are focussing on PRE based secure media sharing in an encrypted cloud media centre.

To help secure the content in the cloud water marking and proxy re-encryption shall further be explained in section II and section III.

II. RELATED WORKS

Plenty of research and studies have been made for ensuring secure sharing of content in the cloud and security of these documents in the cloud as well. An overview of a few of them have been given here.

Here Leo Yu Zhang, YifengZheng, JianWeng, CongWang,ZihaoShan,KuiRen[1] suggest usage of a combination of characteristics of proxy re-encryption and water-marking for secure media sharing and fair traitor tracing. They focussed on trying to leverage homomorphicpropertiesresidinginproxyre-encryptiontoembraceoperationsinfairwater marking. M. Du, Q. Wang, M. He and J. Weng [4] propose efficient task assignment algorithms and also how to leverage both symmetric-key encryption and attribute-based encryption for secure channel establishment ensuring that the task is delivered securely and accurately by any untrusted server. H. Cui, X. Yuan and C. Wang in [5], "Harnessing encrypted data in cloud for secure and efficient mobile image sharing", proposes how bandwidth and energy consumptions by mobile clients can be saved by providing and index design that helps mobile clients to securely find a image of interest for sharing from the encrypted data set. They propose two encryption schemes that support secure image reproduction from encrypted candidate selection. Paper by C. P. Chen and C.-Y. Zhang[6][11], have also been referenced to understand the several methodologies on how to handle the "data deluge", like, granular computing [19], cloud computing, bio-inspired computing, and quantumcomputing. Q. Wang, M. He, M. Du, S. S. M. Chow, R. W. F. Lai and Q. Zou [3] in their paper have discussed about PECDK scheme and how it is based on IPE (Inner Production Encryption) and in doing so, have proposed an efficient PECDK scheme that reduces time and storage consumption. Z. Qin, H. Xiong, S. Wu, and J. Batamuliza[12] have created a survey and analysed Proxy Re- Encryption from various perspectives to understand how it works, its functions, its efficiency, security proofs of existing schemes, further extensions and applications.Archana U. Bhosale, Prog. Vharkate M.N., AparnaU.Bhosale[25] discussed how the data is allocated by the distributor or administrator in a way that it makes it easy to detect fake agents.

III. METHODOLOGY

This section describes all the models and methods utilized in the study. It includes Watermarking,traitor tracing, proxy re-encryption, guilt model analysis and agent guilt model.

1.WATER MARKING

The most common problem with digital documents is that it can be copied or altered. To prevent it from happening watermarking is used. Water marking or digital watermarking involves embedding of a certain code or certain pattern into a digital document of any kind. It canbe embedded into a particular document by using an embedding algorithm and it's difficult to separate the watermark from document without altering the document [2][24]. For every document that is stored in the cloud, each document has a unique watermark code or pattern.

2. AGENT GUILT MODEL

The Agent guilt model is used to determine who the traitor(Fake Agent) among the trusted set of authorized party (client) is. It determines the traitor by using fake objects. The fake objects are distributed along with the requested content to all the clients that request the content. The client will not be able to determine if the object is fake. It appears to the client as a real entity. If a certain content is leaked the guilty agent along with the probability distribution of data that is will be plotted in a report.

2.A. GUILT MODEL ANALYSIS

The fake object acts like a count value. It will be incremented each and every time the client transfers it. If a client is found to have more fake objects that seem to be leaked, the distributor can be sure that the client is guilty of being the traitor. An optimization technique is used to compare both the original data and leaked data [25].

3.PROXY RE-ENCRYPTION

Proxy re-encryption schemes are where an additional third party, called proxy is introduced, who will re-encrypt an already encrypted content given by the content provider. This scheme is used when the content provider does not wish to reveal its private key and the underlying content. Here, the proxy will re-encrypt the content with its

key and share this key with the client. This way it ensures the protection of the data as well as the private key of the content provider. The client may use it to decrypt the content.

The most important feature of PRE is the fact that the sender's information remains anonymous ensuring a guarantee of privacy of the sender.

A proxy changes the message encryption(authentication) or the signature in such a way that anyone without the beneficiary's key cannot access it.

Schemes like SSE and LSH have been proposed to fetch the file and ensuring that the files are leak proof while forwarding[2].

4. BI- DIRECTIONAL PROXY RE-ENCRYPTION

Proxy Re-Encryption (PRE) is when a proxy can re-encrypt an already encrypted content using the key provided by the content provider. The proxy is able to only re-encrypt the content but is not allowed to decrypt it and read the contents. PRE often occurs in one direction, say, from Alice to proxy to Bob and it cannot be reused. This decreases the efficiency of PRE incredibly. If the proxy is able re-encrypt the content in the reverse direction also say, From Bob to proxy to Alice the it is bidirectional. This ensures that the particular PRE scheme is reusable and can be used for multiple encryptions. Using a PRE scheme has its advantages; however, it is weak towards collusion attacks. Bidirectional PRE (BPRE) is not as vulnerable as it uses the same private key for signing and decryption as well.

IV. PROPOSED SYSTEM

In the proposed system, it supports secure media sharing with vendor tracking on encrypted cloud media. Specifically, it allows secure sharing of exported media content to authorized users, while allowing it to track and redistribute illegal content in an appropriate manner. Using proxy encryption and watermark embedding, we can track and prevent the re-distribution of illegal content that should be much lower than local service without cloud support. The content provider must be restricted from accessing users' watermarks during the secure media sharing process, in order for the user interface to be blocked. The proposed design above only needs to store one hard copy at each media item, thus overhead storage is minimized. In addition, the design does not require the number of users to be adjusted in advance, as the watermark of content providers is produced and embedded on thego.

1) SYSTEM ARCHITECTURE

Property description is the official description of a system, organized in a way that supports thinking about system properties. It defines system components or building blocks and provides a system in which products can be purchased, as well as improved systems, that will work together to run the entiresystem.

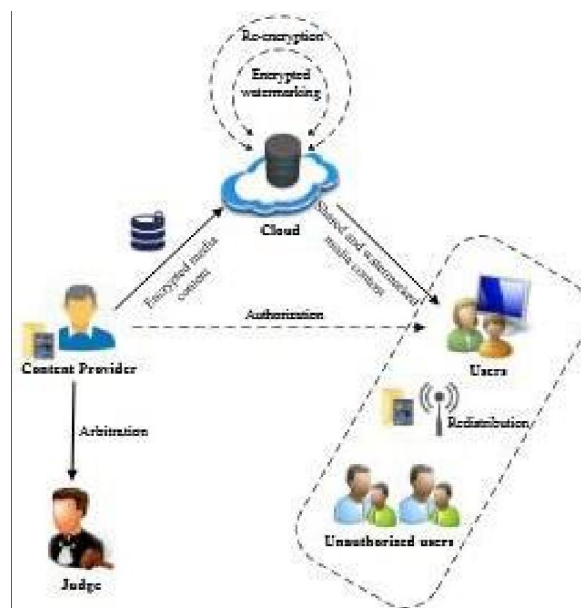


Figure 1. Architecture Diagram

2) CLASS DIAGRAM

The class diagram given below (fig 2) shows the structure of our rendition of this paper. All the modules of implementation for both the content provider (to upload the content) and by the client (Request media, Send Response) is given. Both the content provider and the client must be authenticated by the administrator.

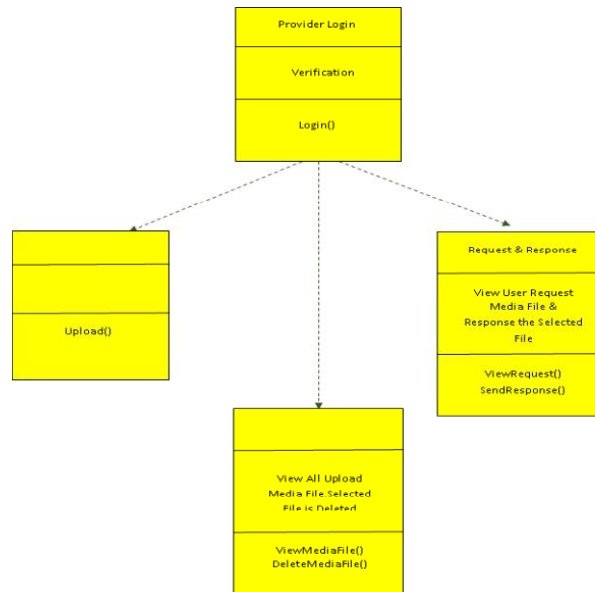


Figure 2. Class diagram

3) DATA FLOW DIAGRAM

Both the content provider and client are required to login to the cloud server. The content provider uploads his content to the server which undergoes the initial AES encryption. The client sends a request for the content to the content provider through the intermediary. The content provider has the choice of approving or rejecting the request. If the content provider approves the intermediary will perform water marking and re-encryption. They perform a key encryption, combine it with the request key and embed it within an image and the proxy(intermediary) will then share the key and encrypted content to the client who requested it. The client will decrypt the image and embedded key verification takes place if the key matches the content shall be decrypted else it an illegal access notification will be sent to the content provider.

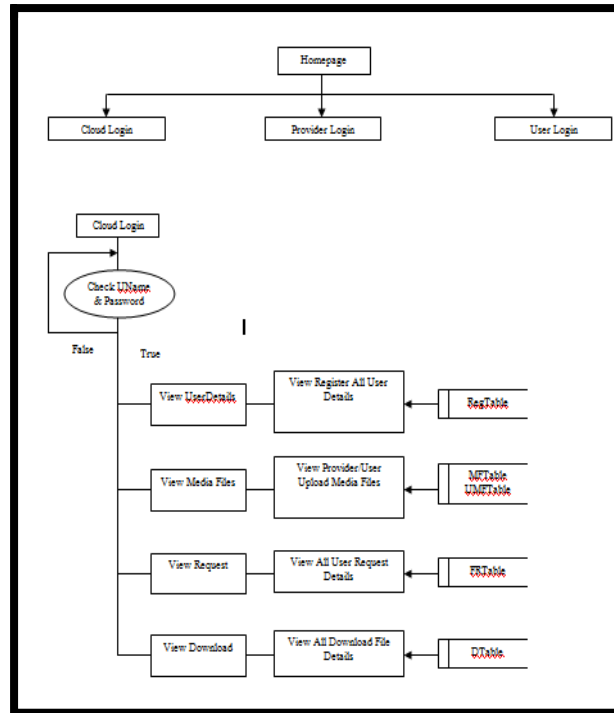


Figure 3. Flow Diagram

V. RESULTS AND DISCUSSION

A. OVERVIEW

The content provider introduces a new content into the cloud. The clients put forth a request for the content provider to get access to the said content. An intermediary will be present to provide more security for the content provider. The intermediary will watermark and re-encrypt the whole content before giving it to the client with a new private key. The client will then decrypt it and Embedded key verification is done. If it is verified the client may continue to decrypt the content else, he will be considered as a threat and be banned. Additionally, if the trusted client tries to send the content to an unauthorized party. The unauthorized party will get an empty file and the traitor that sent this file will be identified and blocked.

The following given are all the modules that have been implemented.

1) CLOUD PROVIDER

A content provider is an authorized person who owns a large amount of media content and wants to use the cloud for media hosting and sharing. To prevent data leaks and unauthorized access, CP will encrypt media collection. In order to share media content with an authorized user, the CP will send a cloud encryption key to grant encryption rights. Additionally, watermarks need to be securely embedded in shared media objects based on appropriate watermarking to track traitors.

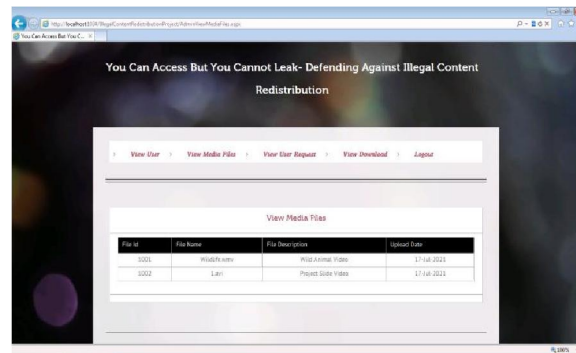


Figure 4a. Cloud Provider

2) USER

In this module, Users can register their data in the cloud to access the media content stored in the cloud. They are content buyers who can access media content once they have been authorized and given the right to remove encrypted content encryption. However, for financial gain or commercial interests, authorized users may redistribute media content that has been encrypted.



Figure 4b. User Module

3) CLOUD ADMIN

Cloud Administrator is a business responsible for maintaining a cloud server that contains files and data uploaded by a content provider. Administrator can view information about users registered on the server. It also looks at details of downloaded files and details of downloaded files. The cloud server stores all media encrypted CP content. When it receives a request from CP, it acts as a proxy to grant the right to encrypt the authorized user, and embedded both CP and user watermarks invisibly on the desired media object.

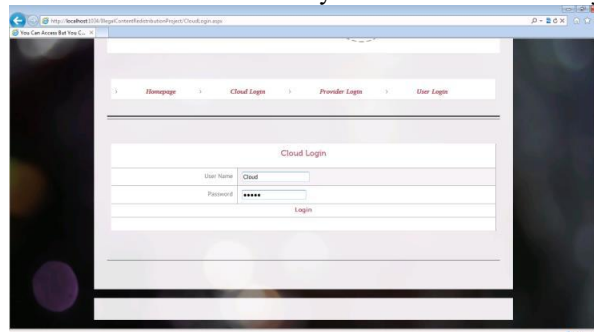


Figure 4c. Cloud Admin

4) UPLOADING FILE

Enables optimal viewer tracking for PREFERRED secure media sharing with minimal storage capability and flexible user support, it is desirable that the cloud can also embed CP watermarks into the cipher text on-the-fly on the security sharing. With such a structure, the CP does not need to locate versions with N watermark on each media object in advance, so the overhead of storage is reduced. On the other hand, as the CP watermark is produced and embedded in flight, it is naturally powerful.

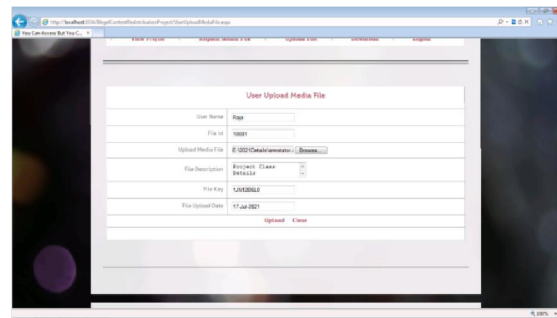


Figure 4d. Uploading a file by CP

5) DOWNLOADING THE FILE

Upon receipt of a request from the user, CP will configure the user reset key, which will be delivered later in the cloud. At the same time, it also generates a water tag to be embedded within the file to protect the manifest. By using this encryption key, the user can download the requested media content file from the cloud. When they attempt to redistribute this file to the cloud, when a suspicious copy is received, the CP turns to the judge for identification of the violation after showing evidence to the judge.

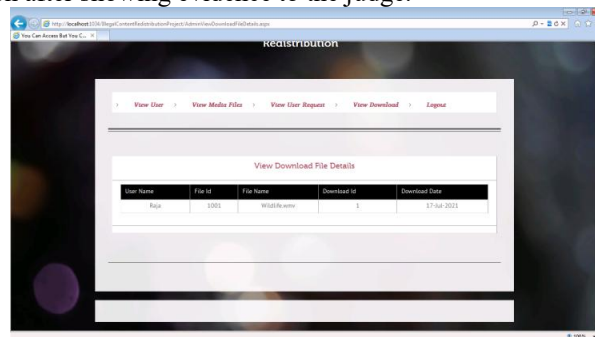


Figure 4e. Downloading the file

VI. CONCLUSION

The project emphasizes that the focus of this publication is not on designing a new watermarking scheme, but on combining special proxy rewriting with appropriate watermarking for secure media sharing and tracking of traitors in a cloud-based media center. In fact, the user may attempt to destroy watermark signals (usually by performing certain signal processing functions, such as compression, filtering, sound addition, etc., in his copy of the received media item), in order to avoid detection. However, it is noted that the appropriate watermarking scheme adopted in our construction provides sufficient strength against such attacks. This project achieves secure cloud media sharing through well-documented vendor.

REFERENCES

- [1] Leo Yu Zhang, YifengZheng, JianWeng, Cong Wang, Zihao Shan, KuiRen " You Can Access but You Cannot Leak: Defending Against Illegal Content Redistribution in Encrypted Cloud Media Center", Nov.-Dec. 2020, pp. 1218-1231, vol. 17.
- [2] PavithraGa, Dhavasumani Kb, KeerthikumarRc, Manoj Sd, Parthiban Ce " A Novel Watermarking and Re-EncryptionApproach to Avoid Illegal Content Sharing In Cloud " , Vol.12 No.2 (2021), 2603-2609.
- [3] Q. Wang, M. He, M. Du, S. S. M. Chow, R. W. F. Lai and Q. Zou, "Searchable encryption over feature-rich data", IEEE Trans. Dependable Secure Computing., vol. 15, no. 3, pp. 496-510, Jun. 2018.
- [4] M. Du, Q. Wang, M. He and J. Weng, "Privacy-preserving indexing and query processing for secure dynamic cloud storage", IEEE Trans. Inf. Forensics Security., vol. 13, no. 9, pp. 2320-2332, Sep. 2018.
- [5] H. Cui, X. Yuan and C. Wang, "Harnessing encrypted data in cloud for secure and efficient mobile image sharing", IEEE Trans. Mobile Computing., vol. 16, no. 5, pp. 1315-1329, May 2017.
- [6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. of IEEE Symposium on Security and Privacy, 2017, pp. 321–334.
- [7] Y. Wu, Z. Wei, and R. H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing networks," IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778–788, 2013.
- [8] F. Xhafa, J. Li, G. Zhao, J. Li, X. Chen, and D. S. Wong, "Designing cloud-based electronic health record system with attribute-based encryption," Multimedia Tools and Applications, vol. 74, no. 10, pp. 3441–3458, 2015.

- [9] J. Liu, X. Huang, and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption," *Future Generation Computer Systems*, vol. 52, pp. 67–76, 2015.
- [10] K. Liang, W. Susilo, and J. K. Liu, "Privacy-preserving ciphertext multi-sharing control for big data storage," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1578–1589, 2015.
- [11] J. Shao, R. Lu, X. Lin, and K. Liang, "Secure bidirectional proxy re-encryption for cryptographic cloud storage," *Pervasive and Mobile Computing*, vol. 28, pp. 113–121, 2016.
- [12] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, "A survey of proxy re-encryption for secure data sharing in cloud computing," *IEEE Transactions on Services Computing*, in press, 2016.
- [13] M. Du, Q. Wang, M. He, and J. Weng, "Privacy-preserving indexing and query processing for secure dynamic cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2320–2332, 2018.
- [14] Y. Zheng, H. Duan, and C. Wang, "Learning the truth privately and confidently: Encrypted confidence-aware truth discovery in mobile crowdsensing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 10, pp. 2475–2489, 2018.
- [15] P. Mohassel, O. Orobets, and B. Riva, "Efficient server-aided 2pc for mobile phones," *PoPETs*, vol. 2016, no. 2, pp. 82–99, 2016.
- [16] A. De Caro and V. Iovino, "JPBC: Java pairing based cryptography," in *Proc. of the 16th IEEE Symposium on Computers and Communications (ISCC'11)*, 2011, pp. 850–855.
- [17] J. Krause, M. Stark, J. Deng, and F.-F. Li, "3D object representations for fine-grained categorization," in *Proc. of IEEE International Conference on Computer Vision Workshops*, 2013, pp. 554–561.
- [18] T.-Y. Lin, M. Maire, S. Belongie, J. Hays, P. Perona, D. Ramanan, P. Dollár, and C. L. Zitnick, "Microsoft COCO: Common objects in context," in *Proc. of European Conference on Computer Vision*, 2014, pp. 740–755.
- [19] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. of IEEE International Conference on Computer Communications (INFOCOM'10)*, 2010, pp. 1–9.
- [20] H.-Y. Lin and W.-G. Tzeng, "A secure erasure code-based cloud storage system with secure data forwarding," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 6, pp. 995–1003, 2012.
- [21] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "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, pp. 131–143, 2013.
- [22] H. Wang, S. Wu, M. Chen, and W. Wang, "Security protection between users and the mobile media cloud," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 73–79, 2014.
- [23] Q. Wang, W. Zeng, and J. Tian, "A compressive sensing based secure watermark detection and privacy preserving storage framework," *IEEE Transactions on Image Processing*, vol. 23, no. 3, pp. 1317–1328, 2014.
- [24] Kulkarni, Pooja&Bhise, Shraddha&Khot, Sadhana. (2015). Review of Digital Watermarking Techniques. *International Journal of Computer Applications*. 109. 40-44. 10.5120/19275-1029.
- [25] Archana U. Bhosale, Prog. Vharkate M.N., AparnaU.Bhosale- A Study of Data Allocation Problem for Guilt Model Assessment in Data Leakage Detection Using Clou Computing- published at: "International Journal of Scientific and Research Publications (IJSRP), Volume 3, Issue 4, April 2013 Edition".