6th International Conference on Multidisciplinary Research (ICMR-2019)
Osmania University Campus, Hyderabad (India)
30th-31st May 2019 www.conferenceworld.in
ISBN : 978-93-87793-89-7

IMPLEMENTATION OF SECURED WATERMARKING FOR PROTECTING ILLEGAL CONTENT REDISTRIBUTION

Ankita S. Bunage[1] (PG Scholar)**, Prof. R. V. Mante**[2] (Assistant Professor)

1 (Department of Computer Science and Engineering, Government College of Engineering, Amravati, India)

2 (Department of Computer Science and Engineering, Government College of Engineering, Amravati, India)

ABSTRACT

The rising growth of multimedia contents is approaching forward the example of cloud-based media hosting today. However, the wide attacking surface of the public cloud and. the problem of secured outsourcing to only authorized users is not fully solved because copying media content is almost cost-free, and the authorized users later become betrayer that illegitimately redistribute the media content to the public after they are authorized with the decryption rights. Therefore, it is imperative to bestow secure cloud-based media sharing with the competence of tracing illegal content redistribution. In this paper, we developed a cloud based secure content sharing application for multimedia data. To improve the security of the content we used our new proxy-based watermarking technique which leads to help the content provider to detect the traitor if any illegal access occurred. So, for preventing the unauthorized access we build the media player which is used to access the downloaded media file if and only if user is an authorized one. Thus we prevented as well as detected the traitor. We also provide watermarking time for performance analysis, showing that our watermarking algorithm required less time as compared to existing system.

Keywords- Copyright Prevention, Illegal Redistribution, Leakage Detection, Media Player, Multimedia Content, Secure Watermarking

1. Introduction

In today's era, multimedia data has been generating in a vast speed. While, handling such huge data become crucial challenge for content providers. With the growing usage of cloud computing, content providers rely on cloud computing for multimedia content hosting and sharing. However, there are some security issues and challenges in cloud computing are: Data Breaches, Data Loss, Malicious Insiders, Denial of Service and Vulnerable Systems. To overcome this security threats and challenges, the prior effort is done by using the encryption algorithms and techniques. Still, the solution of encrypting data before outsourcing does not solve the complete problem. Because, the authorized receiver/ user is able to copy the data and can forward to the

unauthorized receiver or user. This problem is referred as content copyright problem. Securing this information is necessary and for the same there are many algorithm and techniques, some of which includes Cryptography and Watermarking. Digital Watermarking is a technique of embedding some secret information in the main digital content to provide security, integrity and authentication. The Digital watermarking has been proposed as a solution to the problem of copyright protection of multimedia data in a networked environment. It makes possible to tightly associate to a digital document a code allowing the identification of the data creator, owner, authorized consumer, and so on.. Many of the watermarking techniques had been proposed and studied. Different types of watermarking are available for different type of media file. No any common watermarking is yet developed foe all type of media file. Also, some advanced systems had developed to detect the traitor who leaked the authorized data to unauthorized party. However, along with traitor tracing, there is a need of preventing unauthorized access.

All of these problems enforced a solution by building a novel system for any file content protection on cloud by using watermarking with encryption. In this work we build a cloud based content sharing application and a media player for accessing downloaded media file. The main theme of the work is to provide and improve the security of the content media while sharing with multiple users. A new user defined encryption and watermarking technique is proposed in this work. The main objective of our work is to prevent and detect an illegal access. Along with that we used watermarking for all type of media file.

2. Related Works

A number of watermarking procedures have been projected to track down the distributors of illegal replicas [7], [8]. However, most of them ignore the fairness to the customers at all, and the others address the issue ineffectively, considering the current practice of law enforcement. Another mutual limitation of these protocols is the lack of appropriate mechanisms to protect customer privacy during transactions. The encryption may be a great and was the first strategy to avoid copyright [21],[30],[31]. A scalable and fine-grained cloud-based data sharing system is used in [32] by exclusively merging ABE, PRE, and lazy re-encryption.

All prior watermarking approaches had a restriction that a malicious content supplier may outline a client by unjustifiably imputing him of leaking a media protest. So, there was a need to improve watermarking procedures [18], [20], [21], [22], [23]. A secured system architecture is design as an initial effort for traitor tracing where an encoded cloud media centre is proposed which hosts the encrypted SVC videos [17]. A key shortcoming is that this technique is only applicable for videos.

Cloud based buyer dealer watermarking convention based on progressed SS conspire is outlined in [18]. Here, cloud as infrastructure as well as a platform service provider is used to speed up watermark and as an E- commerce platform respectively. The most downside of first one is that CP has to contact every buyer during transaction. However, in second one, it uses paillier cryptosystem which is very complex computational task.

Afterwards, a new grouping of proxy re-encryption (for safe media sharing) and fair watermarking (for fair defector tracing) used the homomorphic properties occur in in proxy re-encryption in [19]. The AES

algorithm and the homomorphic algorithm is used for encryption and proxy re-encryption with watermarking respectively. The drawback of this system is that it used AES and homomorphic algorithm. Both increases the extent of the cipher text and doubles the size of file. Only data leakage is detected but cannot prevent. After the study of all the above methods and approaches of watermarking and reviewing all existing systems, we observed: Size of a file increases after watermarking and there is no any way to prevent the access to leaked content access to leaked content.

3. Methodology

In the proposed model we are combining cloud-based sharing application and media player. Here, we are preventing the copyright access by implementing new watermarking technique. While securely uploading of media files over cloud, we use a use byte wise encryption algorithm and after uploading we are adding watermarking bytes to the file with the help of proxy server. The proposed system is basically consisting of two parts: one is cloud based secure content sharing application and another is media player to open the downloaded file. After the subscription of CP's services, authorized user would be able to download the file and media player (MP). Downloaded file would be is in encrypted format and to open that file, user need to use the provided media player only. MP would check whether the identities stored in that specific file and user credentials are matching or not. If identities are not matched then it means that authorized user whose identity is watermarked in a file is a leaker and at that time that file won't be decrypted or not open. On the other hand, CP would be notified about illegal redistribution of his copy with the help of web services. The working of the proposed system is as shown in figure 1.

3.1 User Section

The user can register and login in the system. The user can upload their own media files, manage the access permission, view and download the shared files by other users, and perceive the leakage report. Along with these they can view their cloud usage and cloud rent payment report on the monthly basis.

3.2 Admin Section

The cloud admin can see the list of all registered user, their payment details.

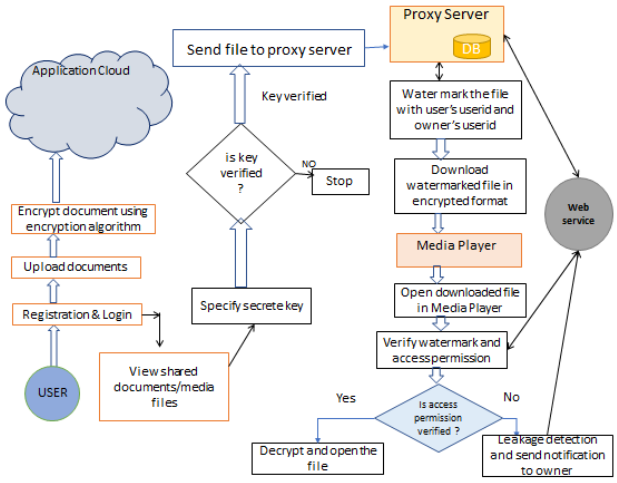

Fig. 1 System Architecture

3.3 Encryption

When the user uploads the media file for sharing, before uploading to cloud, the media file is encrypted using byte wise encryption. The random key would be generated and using this key mathematical operation would perform on bytes of data (8 bytes at a time).After that key would be reverse. This process continues till the complete encryption of file. Later on an encrypted file with encrypted key would be stored on cloud.

3.4 Watermarking

When the authorized user find the shared file with them and wants to download, the media file is watermarked at the proxy server. The proxy server gets owner id, receiver id and create an unique watermark for that file which is shared by owner to receiver. Afterwards, those watermark bytes are encrypted and bytes from encrypted file would be replace with encrypted watermark.

Algorithm:

- Take owner id and receiver id
- Create watermark string ‘str’ by uniquely combining both id
- Convert ‘str’ to byte array ‘byt[]’
- Generate key k randomly
- Encrypt byt[] using key k using encryption algorithm
- Calculate the length of byt[] and read that much bytes from encrypted file into watermark[]
- Store watermark[] bytes as a key into wkey[]
- Perform byte wise mathematical operation with byt[] and watermark[] and store result in watermarked[]
- Replace File bytes with watermarked[]
- Send file to user for download
- Set wkeystr=ConvertToString(wkey[])
- Store wkeystr on proxy server

3.3.2 Watermarking Detection

After watermarking user download an encrypted media file. To open that file they need an access to their media player which uniquely registered for their system only and cannot be shared with any another. If user is authenticated to media player, they can access the media file by browsing it into media player. If user is unauthorized then media player authentication would be failed. If user is authenticated for media player, when they try to open file by browsing it and specify the secret key (which is shared with authorized user only for decryption) ,at this time watermark detection would be done. Here, receiver id from encrypted bytes (which are watermarked) are matched with login id of media player. Thus, whether the user trying to open file is authenticated for that shared media file or not is checked out. If one authorized user give the file and secret key to unauthorized one. And they try to open the file into their registered media player, then leakage is prevented

and file would not decrypt. At the same time the receiver id from watermarked byte considered as a traitor and owner would gets notified about the leaker.

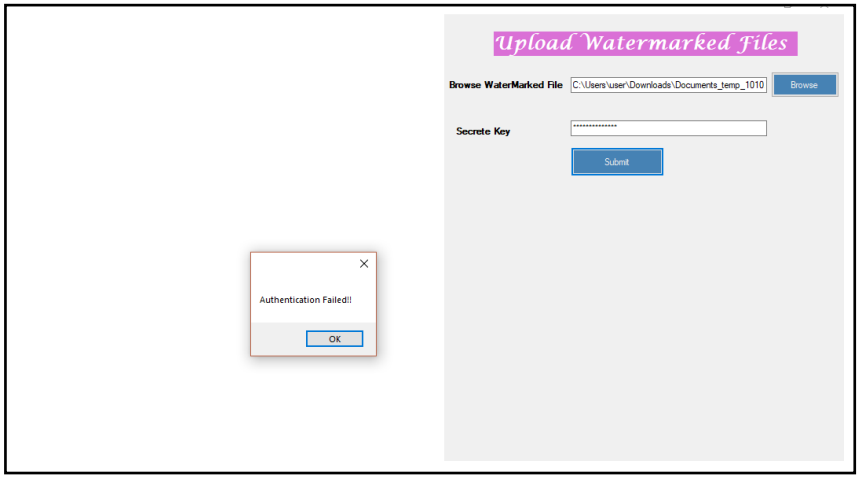

Fig.3.1. Leakage Prevention

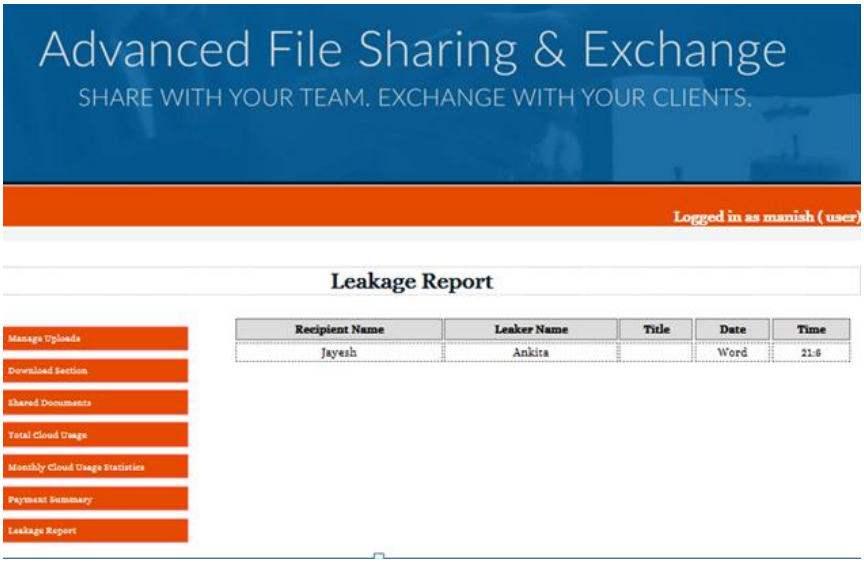

Fig.3.2. Leakage Detection and Traitor Tracing

4. Results

The result of the system is measured by the parameters Encryption time, Decryption time, Watermarking time and size of the file after encryption and watermarking. Table 4.1 shows the proposed watermarking time and existing watermarking for different file size.

Table 4.1. Proposed System Evaluation Table

File Size (in KB)	Average Existing Watermarking Time (mili -seconds)	Average of Proposed Watermarking Time (in mili -seconds)	Saved Time (mili - seconds)	No. of Times Watermarking Done	Proposed System Encryption Time (in mili -seconds)	Proposed System Decryption Time (imili -seconds)
349.191	30.93300056	0.005683833	30.92731673	6	30.933	33.0301
25.2617	93.32326508	0.0051315	93.31813358	2	93.3233	74.9732
562.855	1279.26001	0.005683833	1279.254326	6	1279.26	1105.2
1030.99	2714.763184	0.0036225	2714.759561	2	2714.76	2769.03
12512.3	25065.19922	0.009189077	25065.19003	13	25065.2	12096.4
46784.4	122724.8125	0.006038	122724.8065	1	122725	124981
4296.26	11076.1084	0.003622667	11076.10478	3	11076.1	11661.2

Figure 4.1. represent the graph of saved time in watermarking for a different file sizes. For large size of files, proposed watermarking algorithm efficiently saved the time with respective to existing system.

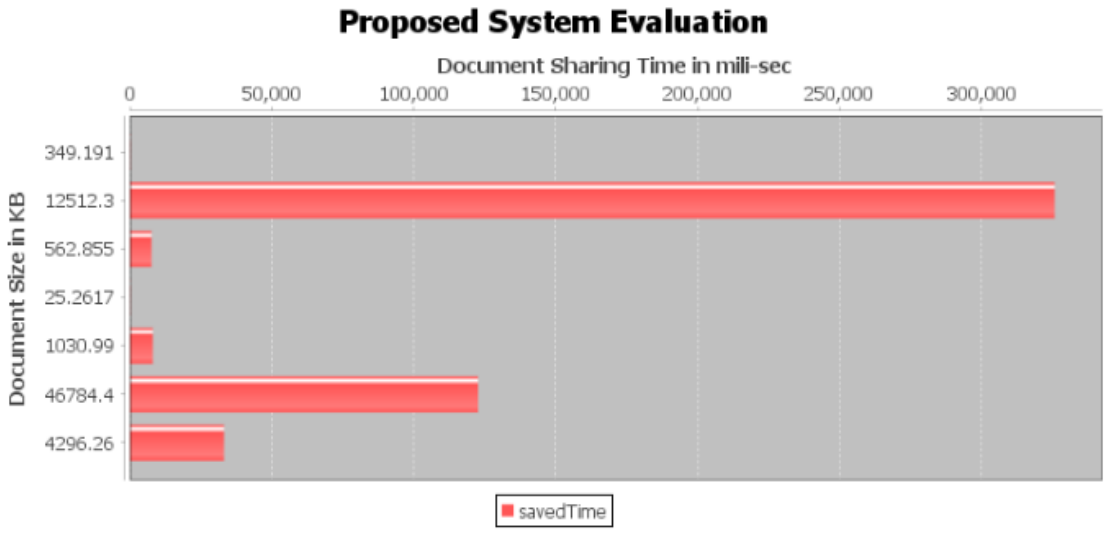

Fig.4.1. Proposed Watermarking Saved Time with Respective Existing System

In an existing system, homomorphism done in watermarking and after that proxy re-encryption of file is done which leads to increase half of the part of size of file. As per shown in figure 4.3., we achieved our objective of maintaining size of file after watermarking.

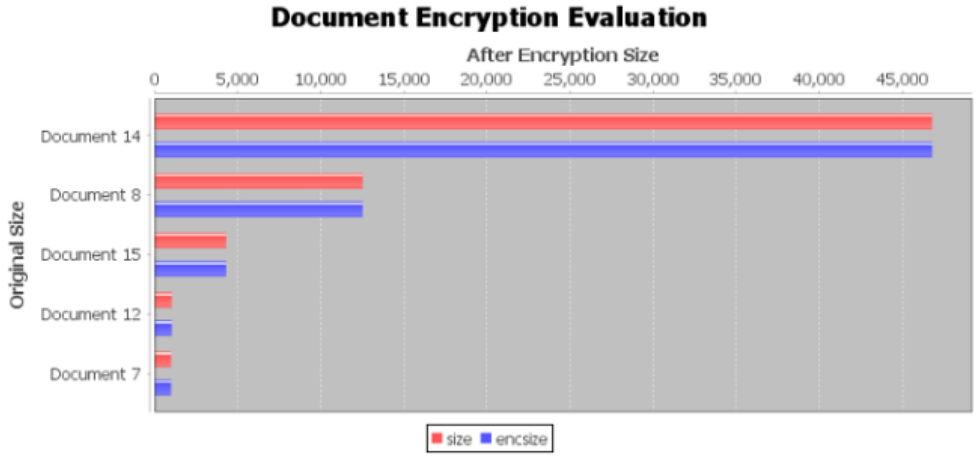

Fig.4.2. Evaluation of size of file.

5. Conclusions

The major focus of our work is to prevent as well as to detect the leakage of multimedia content to unauthorized user. In the existing system all efforts had made for traitor tracing. Also, we prevent the illegal access by using media player. Another factor is the technique used for encryption and watermarking. We used new encryption algorithm which is very secure as it is neither well known and nor increase size of cipher text after encryption and watermarking. Another objective we achieved is to maintain the size of the file after encryption and watermarking. All the prior efforts of watermarking are done on the basis of type of file. In our work we proposed a generalized watermarking for all type of media file. Also, as shown in results our watermarking algorithm requires very less time as compared to existing system. Thus, our system is efficient in terms of security, storage cost and running time complexity.

REFERENCES

[1] Er.Shilpi Harnal and Dr. R. K. Chauhan, "Issues & Perspectives with Multimedia Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 6, Issue 11, November 2016.

[2] Wenwu Zhu, Chong Luo, Jianfeng Wang, and Shipeng Li, "Multimedia Cloud Computing" IEEE Signal Processing Magazine, Volume 28, Issue 3, 2011, pp.59-69.

[3] Prassanna.J, Punitha.K and Neelanarayanan.V, "Towards an analysis of data accountability and auditing for secure cloud data storage", 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), Procedia Computer Science 50 (2015) pp.543 – 550.

[4] Swapnali More and Sangita Chaudhari , "Third Party Public Auditing scheme for Cloud Storage", 7th International Conference on Communication, Computing and Virtualization 2016, Procedia Computer Science 79(2016) pp.69 – 76.

ISBN : 978-93-87793-89-7

[5] Amna Qureshi , Helena Rifa-Pous and David Megias ,“ State-of-the-art, Challenges and Open Issues in Integrating Security and Privacy in P2P Content Distribution Systems”, The Eleventh International Conference on Digital Information Management (ICDIM2016), IEEE, 2016, pp.1-9.

[6] Sameeka Saini, “A survey on watermarking web contents for protecting copyright”, IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems, 2015.

[7] Jaishri Guru, Hemant Damecha, “Digital Watermarking Classification : A Survey”, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 5, Sep-Oct 2014.

[8] Nurul shamimi kamaruddin , amirrudin kamsin, lip yee por, and hameedur rahman, “A Review of Text Watermarking: Theory, Methods, and Applications”, IEEE. Translations and content mining, January, 2018.

[9] Lalit Kumar Saini, Vishal Shrivastava, “A Survey of Digital Watermarking Techniques and its Applications”, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 3, May-Jun 2014.

[10] Dr. Amit Verma, 2Navdeep Kaur Gill, “Analysis of Watermarking Techniques”, InternatIonal Journal of Computer SCIenCe and technology, Vol. 7, ISSue 1, Jan - March 2016.

[11] Chunlin Song, Sud Sudirman, Madjid Merabti, “Recent Advances and Classification of Watermarking Techniques in Digital Images”, ISBN: 978-1-902560-22-9.

[12] Mahsa Boreiry , Mohammad-Reza Keyvanpour, “Classification of Watermarking Methods Based on Watermarking Approaches”, Artificial Intelligence and Robotics (IRANOPEN), 2017.

[13] Ankitha.A.Nayak, Venugopala P. S, Dr. H. Sarojadevi, Dr.Niranjan.N. Chiplunkar, “A Survey and Comparative Study on Video Watermarking Techniques with Reference to Mobile Devices”, IJERA, ISSN : 2248-9622, Vol. 4, Issue 12(Part 6), December 2014, pp.39-44.

[14] D. Usha Nandini, M.E., Divya. S, M.E., “A Literature Survey on Various Watermarking Techniques”, International Conference on Inventive Systems and Control, 2017.

[15] Chin-Laung Lei, Pei-Ling Yu, Pan-Lung Tsai, and Ming-Hwa Chan,“ An Efficient and Anonymous Buyer-Seller Watermarking Protocol,” IEEE Transactions on image processing, vol. 13, no. 12, 2004.

[16] Ritu Gupta, Sarika Jain and Anurag Mishra, “Watermarking System for Encrypted Images at Cloud to check Reliability of Images,” International Conference on Next Generation Computing Technologies, 2015.

[17] Yifeng Zheng, Xingliang Yuan, Xinyu Wang, Jinghua Jiang, Cong Wang, and Xiaolin Gui, “Towards Encrypted Cloud Media Centre with Secure Deduplication”, IEEE Transactions on Multimedia, 2016.

[18] Yi-Jia Peng, Yung-Chen Hsieh, Chih-Wen Hsueh, Ja-Ling Wu “Cloud-based Buyer-Seller Watermarking Protocols,” IEEE Trans. on Smart World, 2017.

[19] Leo Yu Zhang, Yifeng Zheng and Jian Weng, “You Can Access But You Cannot Leak: Defending Against Illegal Content Redistribution in Encrypted Cloud Media Center,” IEEE Transactions on Dependable and Secure Computing, 2018.

ISBN : 978-93-87793-89-7

[20] Priyanka V. Padwal 1, Nilesh P. Sable,"Protection of Multimedia Content in Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 7, July 2016 .

[21] Yoshihiro Kawahara, Liang Wang and Tohru Asami, "Resilient Suppressor Mechanism against Illegal Content Redistribution on Peer-to-Peer Video Sharing Networks", IEEE Communications Society, 210.

[22] S. S. Sudha1 , K. K. Rahini, "Prevention Of Watermarking Attacks Using Cryptography Method", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014 .

[23] Conghuan Ye1, 2 , Ji Li1 ,Zenggang Xiong, "A Secure Content Distribution Based On Chaotic Desynchronization", International Symposium on Computer, Consumer and Control, 2012.

[24] Valer Bocan, M hai Fagadar-Cosma, "Scalable and Secure Architecture for Digital Content Distribution".

[25] S.C. Cheung, Hanif Curreem, "Rights Protection for Digital Contents Redistribution Over the Internet", 26 th Annual International Computer Software and Applications Conference, 2002.

[26] Srijith K. Nair, Bogdan C. Popescu, Chandana Gamage, Bruno Crispo, Andrew S. Tanenbaum, "Enabling DRM-preserving Digital Content Redistribution", 7th IEEE International Conference on E-Commerce Technology, 2005.

[27] Lintian Qiao, Klara Naahrstedt, "Watermarking Schemes and Protocols For Protecting Rightful Ownership And Customer's Right".

[28] Alfredo Rial, Mina Deng, Tiziano Bianchi, Alessandro Piva, and Bart Preneel, Member, "A Provably Secure Anonymous Buyer–Seller Watermarking Protocol", IEEE Transactions On Information Forensics And Security, Vol. 5, No. 4, December 2010.

[29] Birgit Pfitzmann, Matthias Schunteri, "Asymmetric Fingerprinting", Spnnger-Verlag Berlin Heidelberg, , pp. 84-95, 1996.

[30] Baohua Chen1, Na Zhao, "Fully Homomorphic Encryption Application In Cloud Computing".

[31] Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage∗

[32] Shucheng Yu∗, Cong Wang†, Kui Ren †, and Wenjing Lou," Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", IEEE Communications Society,210.

[33] Govinda.K, Divya Joseph , "Dynamic Data Leakage using Guilty Agent Detection over Cloud", International Conference on Intelligent Sustainable Systems, 2017.

[34] Panagiotis Papadimitriou," Data Leakage Detection", IEEE Transactions On Knowledge And Data Engineering, VOL. 23, NO. 1, JANUARY 2011.

[35] Mahsa Boreiry, Mohammad-Reza Keyvanpour, "Classification of Watermarking Methods Based on Watermarking Approaches", IEEE Conference on Artificial Intelligence and Robotics, 2017.