Journal of Computer Engineering and Information Technology

Review Article A SCITECHNOL JOURNAL

Detecting Data Leaks Defending Against Illegal Content Redistribution

Ganesh Kumar P*, K Suthendran, Natrajan NK and Ramprasanna P

Department of Information Technology, Kalasalingam Academy of Research and Institution, Tamilnadu, India

***Corresponding author:** Ganesh Kumar P, Department of Information Technology, Kalasalingam Academy of Research and Institution, Tamilnadu, India; E-mail: vaishuvenkatesan99@gmail.com

Received date: 08 May, 2023, Manuscript No. JCEIT-23-98126;

Editor assigned date: 11 May, 2023, PreQC No. JCEIT-23-98126 (PQ);

Reviewed date: 25 May, 2023, QC No. JCEIT-23-98126;

Revised date: 10 July, 2023, Manuscript No. JCEIT-23-98126 (R);

Published date: 17 July, 2023, DOI: 10.4172/2324-9307.1000293

Abstract

This project will undertake the initial enquiry in safe broadcasting dissemination by reasonable traitorous outlining in secure online server multimedia centre. To begin, we show that a feasible approach exists that utilizes proxy encryption for secure sharing of media with equitable water marking for equitable traitorous monitoring. The supplier of the content publishes encrypted media recordings to the online server. When a user requests this content, the information producer re-encrypts it with an additional key and transmits it to the user. Users that receive information from the online server and subsequently publish that information in the online server anew are considered dishonest users, and this file cannot be posted to the online server. It allows for the secure delivery of subcontracted mass media contented on approved handlers though fairly outlining illegitimate contented redeployment. It investigates the safety features also performs widespread testing for determine the efficacy also applicability of solution. It delivers comprehensive analysis of complexity for content provider efficiency in compute, communication, and storage. The data assets leakage defence system is designed to display the entire list of information assets, confirm the risk evaluation methodology for data resources for centralized cataloging, and exhibit the grade of risk dissemination information visualization exhibit, based on the categorization features of the information safety label of the versatile instances such as the technology application effect, in order to efficiently minimize the possibility of data leakage.

Keywords: Trait tracing; Secure media sharing; Content provider; Plausible design; Re-encrypt; Redistribution

Introduction

Consuming multimedia is increasingly becoming a necessary part of everyday existence in today's big data economy for end users to have access to many devices, services, and programs. With the proliferation of media content, creators of material have begun to look to online figuring aimed at broadcasting storage also distribution, since this may deliver affordable then demanded access to massive archive and processing capabilities [1]. Regardless of the apparent benefits, using an online server media hub divests contented benefactors of straight management concluded contractual mass media assets also increases safekeeping issues. In reality, data vulnerability is frequent among reputable internet storage services [2]. As a result, it is critical to include safety into the design of stored in online server mass media circulation solutions since commencement, establishing admission controller to guarantee which has sanctioned individuals have contact to exported broadcasting contented. In the literature, there are two commonly used methods for providing authority over accessibility and confidential sharing of material in the secured online server media centre. The first technique is attribute based encrypting it in which a content provider provides a related accessible structure over features, and the cipher text saved on the public internet may therefore only be decoded by users who meet that access structure. The latter employs a method known as Proxy Re-En (PRE), in which internet performances as a substitution to aid in delegating decoding civil rights to approved handlers. When compared to ABE, PRE may also be more advantageous since ABE needs the content supplier to receive, evaluate, then re-encrypting statistics once contact laws alteration often [3]. Here study emphases in PRE aimed at protected broadcasting circulation in an online server broadcasting centre. Implementing limited access just for safe multimedia communication, on one hand, would not effectively protect the occupational welfares of contented source. For example, repetition broadcasting gratified is practically permitted, then material suppiliers' financial interests would be compromised if approved users subsequently became traitor and illegally transmitted information from the media to the community after receiving decryption powers. Moving a just-released film from a subscriber to the general public, for example, diminishes the revenues of the linked studio. As a result, it is necessary to provide secure online media distribution platforms with the ability to trace illegal material redistribution. With the rapid growth of technology, the assumption that information is the main source of both the public and private sectors has acquired universal support [4]. As a result, data asset protection has gone up to the highest position on the data protection priority list. The electric power industry is the backbone of the financial system of the nation and one of the most important infrastructures for the expansion of the nation's businesses and people's lives. To address the rising network risk of sensitive data leakage, a private information spillage avoidance strategy based on artificial intelligence technology is being developed.

Literature Review

A new the watermarking process and reviewer encryption approach to prevent unlawful online server data exchange [5-10].

Lower bandwidth cannot coexist. The safety thread is another important issue. A constant internet connection is required for online server computing. Watermarking and re-encrypt methods canister be rummage-sale to tackle the danger thread problem in the online server. In this piece, we are going to look at the above mentioned strategy for overcoming the secrecy problem in online server computing in more detail. The usage of online server is an accumulation of evidence stowed in the online server that can be viewable by the user at any time. The utilisation of an extensive amount of computers linked together is referred to as online server computing. Clod computing is significant because it offers the computing and storage capacity required to run programmes. Any site shall give upon information

[11]. Online server-based technology is also useful in data management. It improves performance.

Using prime ordered collection pairings, safe and effective appeals panel common key cryptography for reviewer constrained environments.

However, the most successful peckd solution relies on internal object encrypting (IPEU), which takes more time and space [12]. By combining a reviewer pair with a premier ordered collection, we provide an effective peckd technique that consumes lower compared length space. The planned system is secure, according to a specified safety definition. In terms of time and space efficiency, theoretical analysis and empirical data reveal that our planned system beats the state of the art technique. A happen to identifying encryption with a public key technique is a crucial tool for keeping data confidentiality in today's online server setting. Encrypting with a public key and conducting independent and linked keyword happen to identifies (PECKD) in particular shall give upon varied happen to identify alternatives not losing key values [13].

A framework for reviewer preserving spatial collaboration. We demonstrate an effective assigning tasks mechanism using encrypted data that may quickly distribute tasks to nearby employees. We employ combined attrib biased encoding besides symmetric-keys cryptography to create safe paths over headwaiters, guaranteeing sure any untrustworthy site delivers the work securely and precisely [14]. Furthermore, we investigate the safety characteristics of our technique. We conducted real world experiments using real world datasets. According on experimental evidence, our technique beats earlier approaches. Privacy leakage is a serious issue with geographical crowdfunding in many scenarios. In this paper, we look on safeguarding privacy in geographical sourcing.

We provide a safe and reliability indexing architecture that allows the client to safely find the candidate selection matching to the image desired for uploading from protected image databases while on the go. Then, utilizing secured candidate selection, we develop two specialized encryption approaches that enable secure image replication. We provide a rigours study of the safety strength of the design. Our testing clearly shows both of which bandwidth and energy consumption at the client device may be decreased while still providing all service requirements and safety assurances. Massive volumeumes of audiovisual data are increasingly being sent to the online server in order to better serve mobile appis [15]. Furthermore, highly connected datasets are becoming increasingly common, as is the rich information.

Methodology

It allows safe media interchange with excellent offender tracing within a protected online server multimedia centre. It provides the safe dissemination of outsourced media content to approved consumers while fairly tracing illegal content redistribution [16]. Using the proxy re-encryption technique and watermark embedding, we can trace and ban unlawful content redistribution, and the cost should be much cheaper than the service offered regionally without online server support. The item's supplier should be prevented from observing the watermarks placed by users during the encrypted media exchange method, avoiding frame attacks on users [17]. Because the above mentioned technique only requires keeping one encrypted copy of each piece of media, the associated cost of storage is kept to the lowest possible level. Ports re-encrypt to a new cipher text using second private key when given a re-encryption key. In this post, we will lay the groundwork for secure media sharing *via* proxy re-encryption techniques. Time a handler requests accessibility to around digital item, CP supply the internet with an admissions committee key and grant that user decryption capabilities [18]. In our system, we will utilize the technique to construct a proxy's recovering primitive (Figure 1).

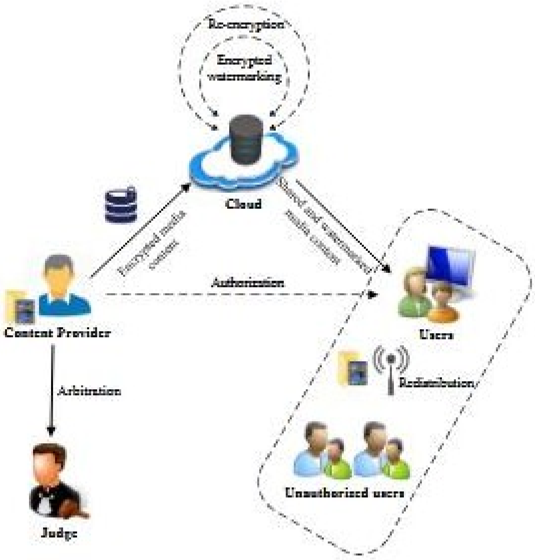


Figure 1: Planned architecture diagram.

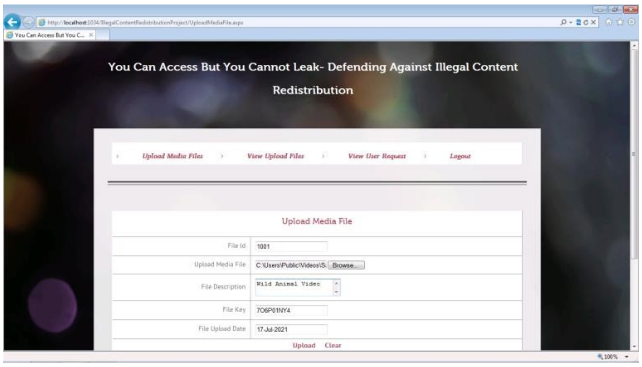
Results and Discussion

ClouBenefactor

A multimedia producer is approved person who possesses a hefty volume of broadcasting then intends to store and distribute it in the online server. Near avoid facts loss also unauthorized contact, CP resolve gather audiovisual reviewer data using encryption. On segment broadcasting contented an approved individual, CP must transmit key for re-encrypt to the online server, granting them the decryption privilege. Furthermore, watermarks must be safely put within shared media files for traitor tracing in accordance with fair watermarking [19].

Users

Online server consumers can contact the mass media gratified the minute being sanctioned also delegated decryption precise of the concrete gratified. Yet, due to monetary incentives or profitable welfares, approved handlers might reallocate the decrypted mass media contented to the public (Figure 2).


http://localhost:1034/IllegalContentRedistributionProject/UploadMediaFile.aspx
You Can Access But You C...
Upload Media Files
View Upload Files
View User Request
Logout
Browse...
Upload
Clear
100%

You Can Access But You Cannot Leak- Defending Against Illegal Content Redistribution

Upload Media File

File Id: 1001
Upload Media File: C:\Users\Public\Videos\S
File Description: Wild Animal Video
File Key: 7O6P01NY4
File Upload Date: 17-Jul-2021

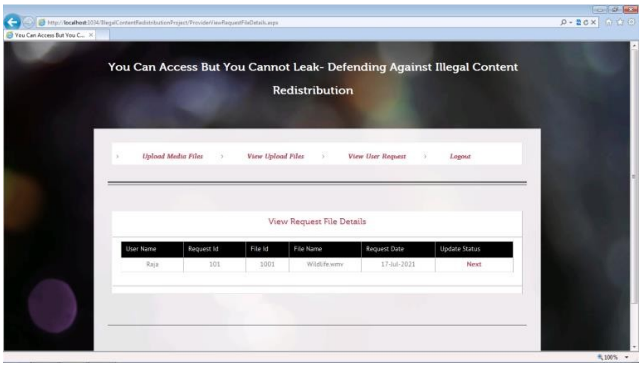
Figure 2: Upload media file by content provider details.

Online server supervision

The organization in charge of operating the server in the online server, which includes the information and files supplied by the service provider, is known as the online server administrator. Administrators have access to information about the system's registered users [20]. He may also view the information of files that have been uploaded and downloaded. Everything of a CP's protected media content is stored on the online server. When it gets an enquiry, it turns as demmitions a proxy, transferring decode privileges to an allowed client whilst secretly embedding both CP's also the client's watered marks in the needed media item.

Uploading file

It enables Fairly track out a traitor It is ideal for the online server to be capable to add CP's marks in cypher text realm on thego-fly during safe allotment in admissions committee-based encrypted media transmission while minimising storage overhead and enabling user dynamics. With this property, the CP is unable to construct N designated variations of each media item ahead of time, minimising storage cost. The CP's watermark, on the other hand, is dynamic in nature since it is manufactured or implanted in real time (Figure 3).


http://localhost:1034/IllegalContentRedistributionProject/ProviderViewRequestFileDetails.aspx
You Can Access But You C...
Upload Media Files
View Upload Files
View User Request
Logout
100%

You Can Access But You Cannot Leak- Defending Against Illegal Content Redistribution

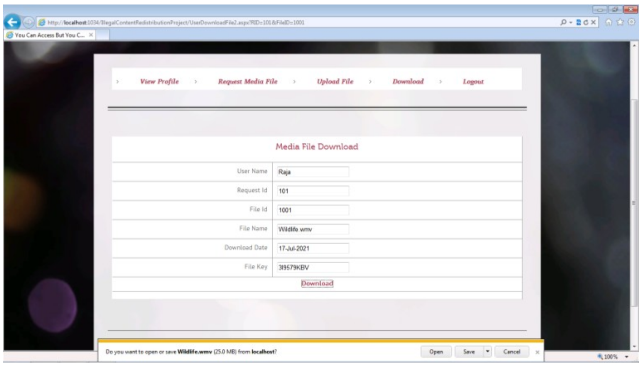
View Request File Details

User Name	Request Id	File Id	File Name	Request Date	Update Status
Raja	101	1001	Wildlife.wmv	17-Jul-2021	Next

Figure 3: View user request by provider.

Downloading file

After receiving an inquiry from the user, the CP will engender a user re-encrypt key, which will subsequently be sent to the online server. At the same time, it creates an image watermark to be included in file toward defend the obvious. By means of the re-encrypt keys, someone else may acquire the required file type *via* the online server. If they attempt to disseminate this content into the online server and a suspect replica is identified, the CP seeks breach identification from the court after submitting evidence to the judge (Figures 4 and 5).

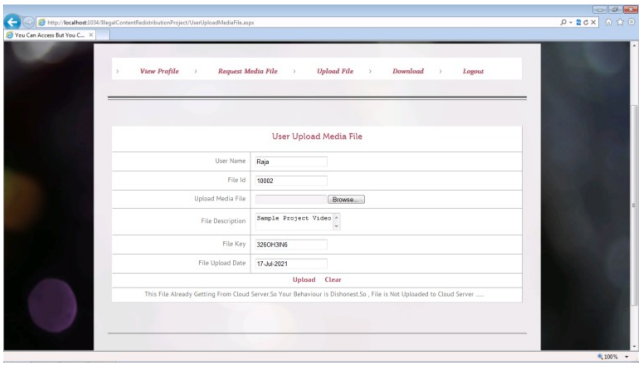

http://localhost:1034/IllegalContentRedistributionProject/UserDownloadFile2.aspx?RID=101&FileID=1001
You Can Access But You C...
View Profile
Request Media File
Upload File
Download
Logout
Download
Open
Save
Cancel
100%

Media File Download

User Name: Raja
Request Id: 101
File Id: 1001
File Name: Wildlife.wmv
Download Date: 17-Jul-2021
File Key: 3I9579KBV

Do you want to open or save **Wildlife.wmv** (25.0 MB) from **localhost**?

Figure 4: Download media file by users.


http://localhost:1034/IllegalContentRedistributionProject/UserUploadMediaFile.aspx
You Can Access But You C...
View Profile
Request Media File
Upload File
Download
Logout
Browse...
Upload
Clear
100%

User Upload Media File

User Name: Raja
File Id: 10002
Upload Media File:
File Description: Sample Project Video
File Key: 326OH3IN6
File Upload Date: 17-Jul-2021

This File Already Getting From Cloud Server.So Your Behaviour is Dishonest.So , File is Not Uploaded to Cloud Server .....

Figure 5: Block uploading of redistribution file.

Conclusion

This purpose of rehappien to identify is to connect re-encrypt of proxy passes and fair watermarked aimed at protected broadcasting communication by reasonable offender monitoring within a secure online multimedia censer, non-strategy an original watered marking that have system. In reality, a handler may attempt to erase watered mark indicators in order to avoid detection (often by performing signal processing steps on his acquired video item replicate, such as bending, examination, noisy furthermore, and so on). Nevertheless should be noted that the fair imprinted technique utilised in our layout provides more than enough resilience to such attacks. This system protects online media exchange while also enabling for accurate traitor tracing. We thoroughly investigated safety strengths and conducted a complexity analysis.

References

1. Chen CP, Zhang CY (2014) Data intensive applications, challenges, techniques and technologies: A survey on big data. Inf Sci 275:314-347.
2. Zhu W, Luo C, Wang J, Li S (2011) Multimedia online server computing. IEEE Signal Process Mag 28:59-69.
3. Xiong H, Zhang X, Yao D, Wu X, Wen Y (2012) Towards end to end secure content storage and delivery with public cloud. Proc Conf Data Appli Secur 257-266.
4. Ren K, Wang C, Wang Q (2012) Safety challenges for the public online server. IEE Int Com 1:69-73.

5. Zheng Y, Cui H, Wang C, Zhou J (2017) Privacy preserving image denoising from external online server databases. IEEE Trans Inf Forensics Secur 12:1285-1298.
6. Shan Z, Ren K, Blanton M, Wang C (2018) Practical secure computation outsourcing: A survey. ACM Comput Surv 51:31:1-40.
7. Bethencourt J, Sahai A, Waters B (2007) Ciphertext policy attribute-based encryption. Proc IEE Symp Secur Priv 321-334.
8. Wu Y, Wei Z, Deng RH (2013) Attribute based access to scalable media in cloud assisted content sharing networks. IEEE Trans Multimed 5:778-788.
9. Liu J, Huang X, Liu JK (2015) Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption. Future Gener Comput Syst 52:67-76.
10. Liang K, Susilo W, Liu JK (2015) Privacy preserving ciphertext multi-sharing control for big data storage. IEEE Trans Inf Forensics Secur. 10:1578-1589.
11. Shao J, Lu R, Lin X, Liang K (2016) Secure bidirectional proxy re-encryption for cryptographic cloud storage. Pervasive Mob Comput 28:113-121.
12. Qin Z, Xiong H, Wu S, Batamuliza J (2016) A survey of proxy re-encryption for secure data sharing in cloud computing. IEEE Tran Ser Comput 1.
13. Cox IJ, Kilian J, Leighton FT, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6:1673-1687.
14. Barni M, Bartolini F, Cappellini V, Piva A (1998) A DCT domain system for robust image watermarking. Signal Process 66:357-372.
15. Pfitzmann B, Schunter M (1996) Asymmetric fingerprinting. Eurocr 84-95.
16. Memon N, Wong PW (2001) A buyer seller watermarking protocol. IEEE Trans Image Process 10:643-649.
17. Lei CL, Yu PL, Tsai PL, Chan MH (2004) An efficient and anonymous buyer-seller watermarking protocol. IEEE Trans Image Process 13:1618-1626.
18. Kuribayashi M, Tanaka H (2005) Fingerprinting protocol for images based on additive homomorphic property. IEEE Trans Image Process 14:2129-2139.
19. Rial A, Deng M, Bianchi T, Piva A, Preneel B (2010) A provably secure anonymous buyer-seller watermarking protocol. IEEE Trans Inf Forensics Secur 5:920-931.
20. Zhang J, Kou W, Fan K (2006) Secure buyer seller watermarking protocol. IEE Process Infor Secur 153:15-18.