iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** II **Month of publication:** February 2023

DOI: https://doi.org/10.22214/ijraset.2023.48812

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue II Feb 2023- Available at www.ijraset.com

Data Leakage Discovery in Cloud Using Watermark Fashion

B. Karthik[1], K. Sai Kumar[2], M. Rajashekar[3]
[1, 2, 3]*JNTUH, ECE, Sreenidhi Institute Of Science and Technology, Hyderabad, Telangana, India*

Abstract: ***Because the data that is kept is so valuable and common, security is a crucial concern in data operations. Although it's a common misconception that hackers cause security breaches, the majority of data loss is really caused by interposers. In a nearly dispersed configuration, the distributor continuously transfers important data to reliable parties. In order to keep the services stable and safe, there is a strong demand, which is based on the growing number of drug users. When a customer leaks sensitive information, the exact consumer who is to blame for the breach should be identified as soon as possible. Consequently, it is necessary to monitor the data flowing from the distributor to the agents. A data leakage discovery system using a watermarking method is proposed. This system investigates data tampering and determines that one or more agents are responsible for the information leak. Additionally, the process is subsequently implemented on design pall***
Keywords: ***Pall, Data, Watermarking, Hackers.***

I. INTRODUCTION

However, it also seriously jeopardises the confidentiality of the files. Although users may not have complete trust in the cloud servers managed by cloud providers, sensitive and confidential data records, such as those pertaining to employees or products, company policies, etc., may be stored there. Data security in cloud computing has therefore drawn a lot of attention. Less control over data can lead to serious security problems and threats that could lead to data leakingThe calibre of the sensitive data disclosed determines the degree of defiling caused by the data leak. If the information that has been Almost every IT business is striving to get into cloud computing, which is a quickly developing and eye-catching technology in the field of information technology. In cloud computing, shared software and information resources are made available to devices as needed. Data storage is one of the basic services offered by cloud computing. By utilising the cloud, staff are completely freed from the aggravating local data storage requirements. If important data is released, the firm could become weak. The leaking might harm the company's operations and bring it to its knees.

Different data leakage detection approaches, such as the fragmentation method and perturbation method, have been developed to address this issue. To deal with identifying data leakage on relational databases, each has been developed. The proposed research is concerned with finding data leaks on clouds that contain vast amounts of data.

II. LITERATURE REVIEW MATERIALS AND METHODOLOGY

A literature review is a complex analysis, not merely a summary, that is closely related to the research issue. In other words, it is a representation of the literature that sets the scene for the subject. The authenticity and vacuum of the funds are necessary for software development. This section aids in finding the information that has been developed and the application and execution of the same in a timely manner. The durability and strength of the product. A literature review is significant because it clarifies the context of exploration on a topic, illustrates why a topic is important to a field of study, unearths connections between ideas from exploration studies, identifies key themes, generalisations, and experimenters on a topic, identifies crucial gaps and points of disagreement, and poses further exploration questions that logically follow from the results of the earlier studies. Techniques and Analysis It suggests a watermark embedding algorithm that is similar to what Sorting is necessary for development, to provide adequate protection for the data contained in the relational database, partitioning used for marker position and bit embedding watermark bits are bedded in the number set. At the time of reacquiring data from the database in its client side, it also generates a watermark discovery technique similar to that which comprises of Sorting, Partitioning utilised for marker position, and bit discovery manner. Cons The main drawback is that this relational database should not address the issue of data security through watermarking in the context of nonnumeric garbling disciplines.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue II Feb 2023- Available at www.ijraset.com

III. ANALYSIS AND MODELING

The distributor and agent are two realities included in the proposed system. Data distribution to third parties will be handled by company labour force as the distributor. The functions of the distributor include adding agents, storing data, spreading data, discovering tampering, and chancying. agents of the bush Third parties participating in the transaction, like a client or an agent Two realities that are part of the suggested system are the distributor and agency. The company's workforce will act as the distributor when distributing data to outside parties. The distributor performs tasks like adding agents, storing data, disseminating data, identifying tampering, and chancying. Bush operatives Participants in the transaction who are not the seller or buyer, such as an agency or client company, are permitted access to data from the distributor, including posting lists, hand hiring, multimedia data, etc. Information recovery and encryption are the first steps in the data transit phase. Data identification information is discovered about the data. Once the data has been recovered, communication (MS1) is made using the customer ID of the benefactor and the recovered data. To prevent any tampering with the information, the connection is additionally translated using symmetric essential encryption, namely the Advanced Encryption Standard (AES) method. The AES algorithm is thought to be more efficient for steganography because it operates faster than triadic DES**.**

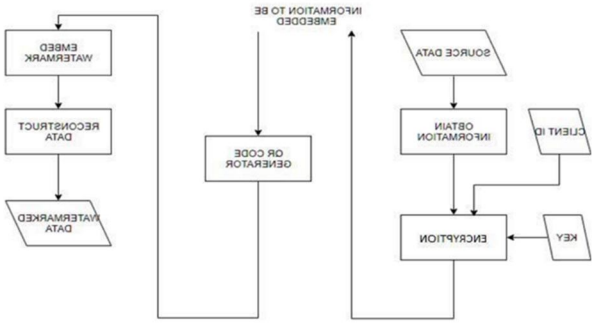


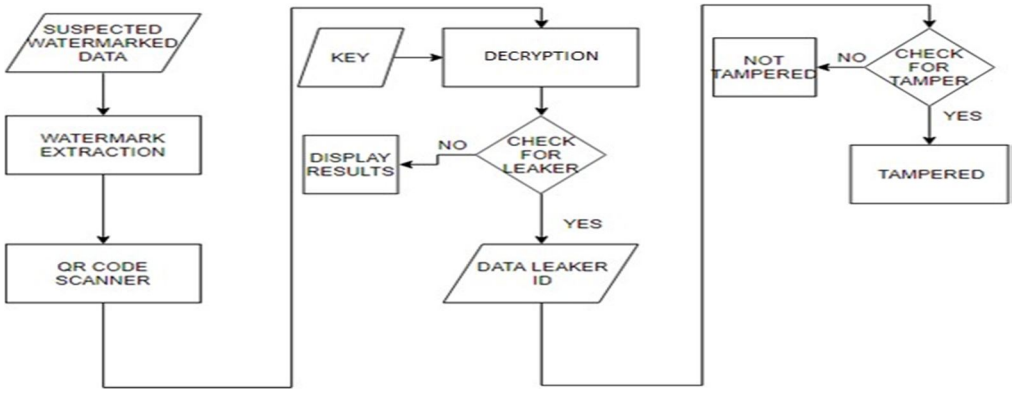
Fig1: embedded algorithm ,

A. Tamper Detection and Detecting Data Leaker

Replace the content after that and fix the mistakes you found. Segment the data codewords, then decode the text according to the mode.

Later, the AES decryption method is used to decode the encrypted data contained in the QR code. Client information obtained from QR codes is compared to the information. In the last step, the watermark is extracted from data that has been leaked but has been watermarked. Later, the extracted QR code is scanned to retrieve the encrypted data. analysing information the The QR code process is the opposite of conversion. Recognizing the dark and light units as an array of 0s and 1s is the first stage in this process.

The following step is to extract the format data, which shows the masking pattern, and to ascertain the QR version. Afterward, XOR the coded region kept in the cloud database. Clients who have leaked important organisational data are presumed guilty if their information matches. Data distortion or manipulation can be found with a tamper detection module. The picture properties are located and then compared to the original data attributes to see if the current image data has been tampered with. If there is a discrepancy between the two, it is declared that the copy in question has been altered or modified.



IV. RESULTS AND DISCUSSION

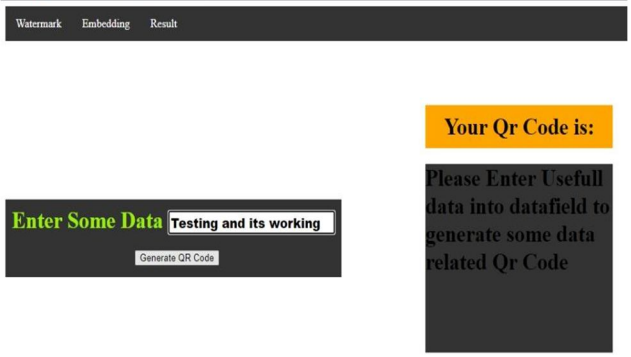


Fig4:qQr generator

Fig5: Output

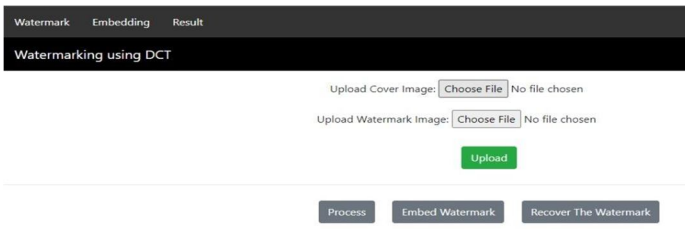
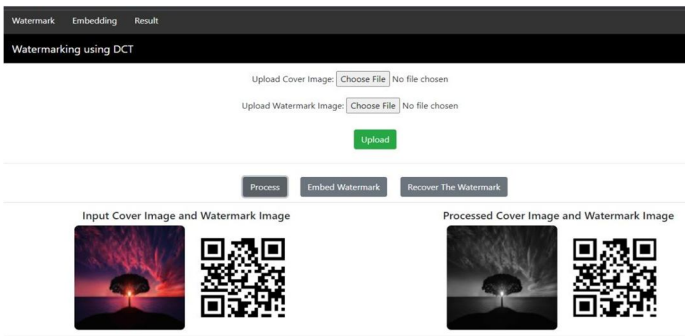


Fig3&4: watermark embedding



V. CONCLUSION

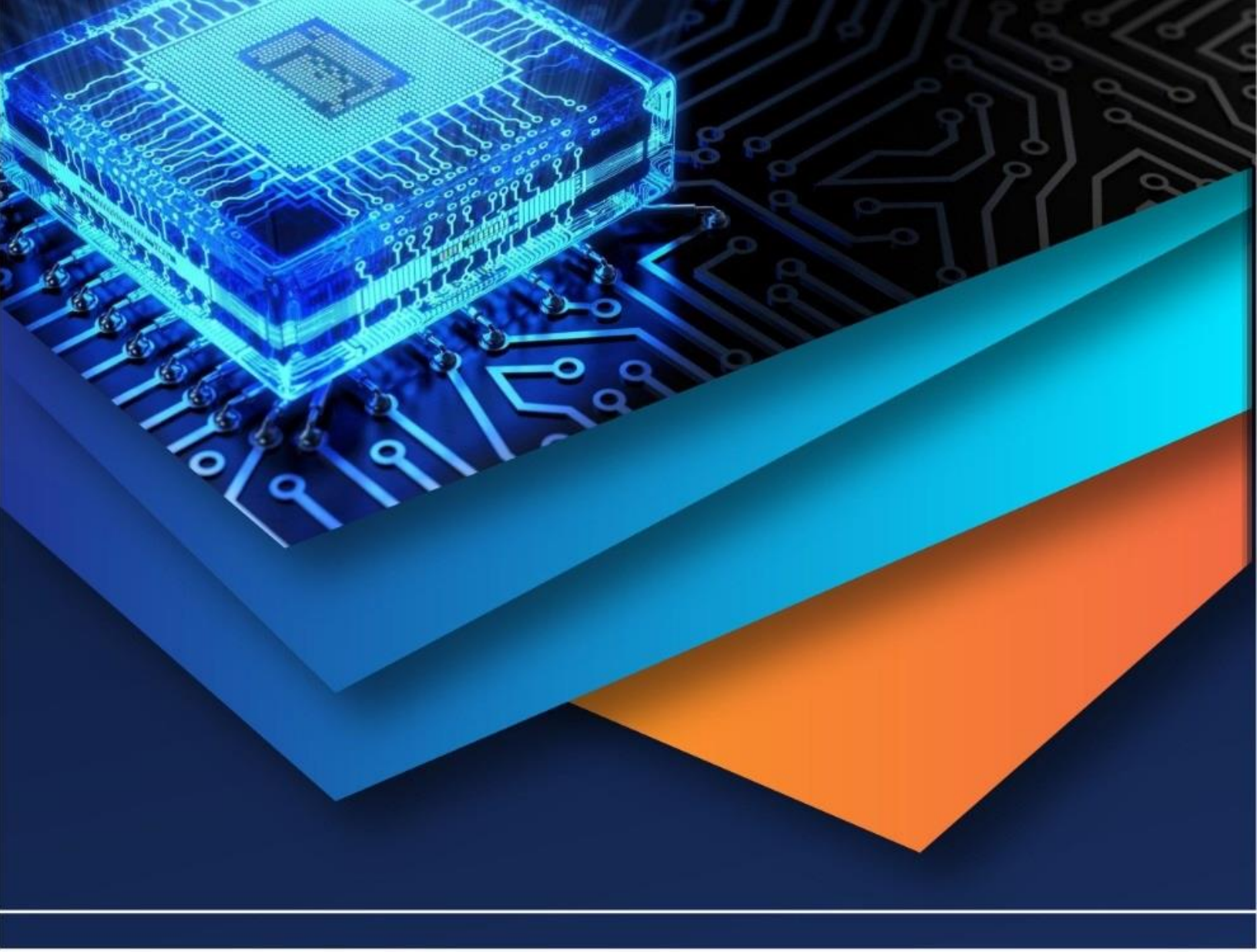
Any industry, group, research community, or institution that frequently shares its data online with any third party may find a data leakage detection model to be of great use. Using a watermarking algorithm, the suggested approach enables the identification of data leaks and data manipulation on cloud data.

The method being shown inserts a Quick Response code, or watermark, made out of the receiving client's information and data together with the image data that needs to be delivered. By removing the watermark from an image and comparing it to the client's information, the data leaker is discovered. Data is additionally examined to identify tampering by contrasting its characteristics with those of the original data.

A data leakage detection system can offer security to the data during transmission, which is a huge benefit. If that data is compromised, it can also identify it. The current system uses encryption to supply security using a variety of techniques, but the suggested model delivers security and detection. Imperceptibility and robustness are incorporated into the model using the hybrid watermarking procedure.

REFERENCES

[1] Molin, "Data Leakage Detection," IEEE Transactions on Knowledge and Data Engineering, Panagiotis Papadimitriou, Hector Garcia, 2011, Volume 23, Issue 1.
[2] "Data Leakage Detection Using Cloud Computing," Abhijeet Singh and Abhineet Anand, International Journal of Engineering and Computer Science, Volume 6, Issue 4, April 2017. Geetha, M.Nishanthini, G.Shanthi, K.Sivabharathi, M.Suganya "Data Leakage Detection and Security Using Cloud Computing", International Journal of Engineering Research and Applications, Volume 6, Issue 3, March 2016.
[3] "Detection of Data Leakage in Cloud Computing Environment," International Conference on Computational Intelligence and Communication Networks, Neeraj Kumar, Vijay Katta, Himanshu Mishra, and Hitendra IEEE Garg 2014.
[4] D.K. Chitre and Rupesh Mishra, "Data Leakage and Detection of Guilty Agent," International Journal of Scientific & Engineering Research, Volume 3, Issue 6, 2012.
[5] Weijun Zhang and Xuetian Meng, "An Improved Digital Watermarking Technology Based on QR code", IEEE 2015 International Conference on Computer Science and Network Technology.
[6] "Advanced Encryption Standard Algorithm: Issues and Implementation Aspects" by Ahmed Fathy, Ibrahim F. Tarrad, Hesham F.A. Hamed, and Ali Ismail Awa1 was published by Springer in 2012.
[7] Sumit Tiwari, "An Introduction to QR Code Technology," 2016 IEEE international information technology conference.
[8] International Conference on Future Computer and Communication, 2009 IEEE, Yanqun Zhang, "Digital Watermarking technology: A Review."
[9] Wang Yanjie and Gu Tianming, "DWT-based Digital Image Watermarking Algorithm," The Tenth International Conference on Electronic Measurement & Instruments, 2011 IEEE.
[10] Sha Wang, Dong Zheng, Jiying Zhao, " An Image Quality Evaluation Method Based on Digital Watermarking" IEEE transactions on circuits and systems for video technology, Volume 17,2007.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY