Vol. 3, Issue III, Jul-Sep, 2020 http://bharatpublication.com/current-issue.php?jID=29/IJAE

A COMPREHENSIVE ANALYSIS OF THE CAUSES AND FACTORS LEADING TO DATA LEAKAGE IN THE CLOUD ENVIRONMENT

Arnav Kakar

Vivekanand Institute of Professional Studies, New Delhi

ABSTRACT

Security is a crucial concern in data operations because the stored data is so valuable and shared. Although it is a common misunderstanding that security breaches are caused by hackers, interposers are responsible for the majority of data loss. In a nearly dispersed configuration, the distributor continuously transfers important data to trustworthy parties. Due to the rising number of drug users, there is a strong demand for the services to remain stable and safe. When a customer leaks sensitive information, it is important to determine who exactly is to blame as soon as possible. As a result, it is necessary to keep an eye on the data that travels from the distributor to the agents. A watermarking-based data leakage discovery system is proposed. Data tampering is looked into by this system, which finds that one or more agents are to blame for the information leak. Additionally, the procedure is then applied to the design plaque.

INTRODUCTION

However, it also poses a serious threat to the confidentiality. Sensitive and confidential data records, such as those about employees or products, company policies, etc., may require more trust from users in the cloud servers managed by cloud providers. It could be kept there. As a result, cloud computing's data security has received a lot of attention. The quality of the disclosed sensitive data determines the degree of defiling caused by the data leak. Less control over data can result in serious security issues and threats that could cause data leaks. According to the information, nearly every IT company is trying to get into cloud computing, a technology in the information technology field that is rapidly evolving and catching attention. In cloud computing, devices can access shared software and information resources whenever they need them. One of the fundamental services provided by cloud computing is data storage. Staff members are completely free of the burdensome local data storage requirements by using the cloud. The business might continue to thrive if crucial information is made public. The leak could have a negative impact on the company's operations and cause it to collapse.

The goal of the proposed study is to find data leaks in clouds that store a lot of data. Various fragmentation and perturbation-based data leakage detection methods have been developed to address this issue. Each was made to find data leaks in relational databases.

ANALYSIS AND MODELLING

The distributor and the agency are two facts included in the suggested system. The proposed system includes the realities of the distributor and agent. The employees of the company will act

as distributors and will be responsible for data distribution to third parties. Adding agents, storing data, spreading data, detecting tampering, and chancying agents of the scrub are all functions of the distributor. Like a client or an agent, third parties are involved in the transaction. When data is distributed to third parties, the workforce of the business will act as the distributor. Adding agents, storing data, disseminating data, spotting tampering, and chancying are all tasks performed by the distributor. Shrubbery agents Members in the exchange who are not the merchant or purchaser, for example, an office or client organization, are allowed admittance to information from the merchant, including posting records, hand recruiting, sight and sound information, and so on. In the data transit phase, the initial steps are data recovery and encryption. The data's identification information is uncovered. The benefactor's customer ID and the recovered data are used in MS1 communication after the data have been recovered. To keep the information safe, the Advanced Encryption Standard (AES) method of symmetric critical encryption is used to translate the connection. Steganography uses the AES algorithm more effectively because it operates faster than triadic DES.

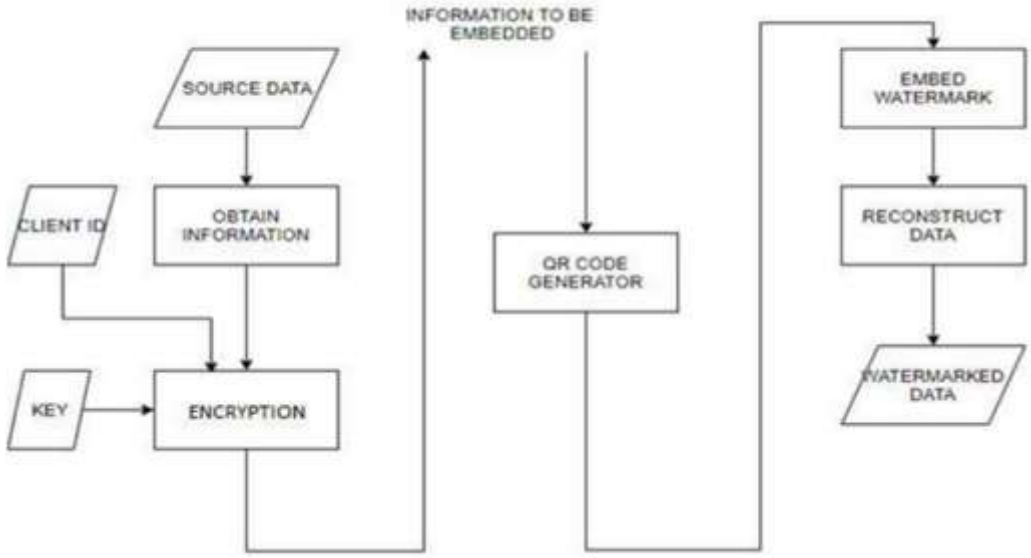
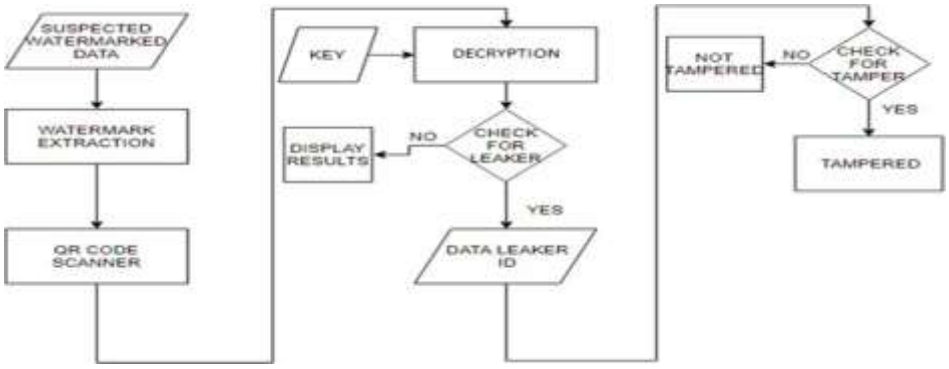


Fig1: Embedded Algorithm

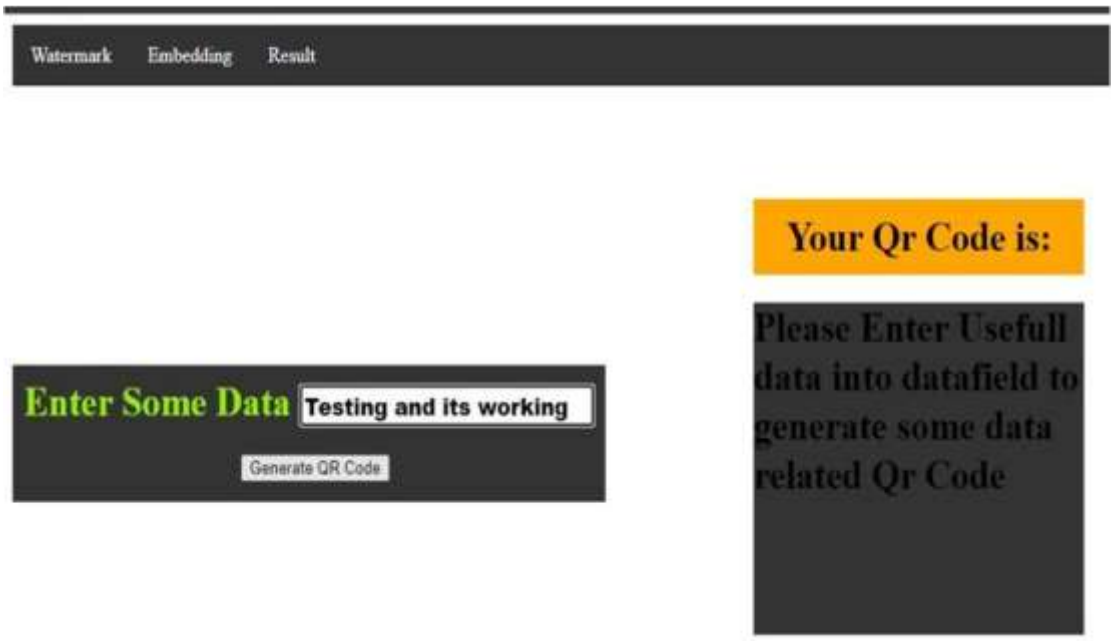
A. Tamper Detection and Data Leaker Detection After that, replace the content and correct any errors you found. Section the information codewords, then, at that point, disentangle the message as indicated by the mode.

The encrypted data contained in the QR code is later decoded using the AES decryption method. The information and the client data obtained from QR codes are compared. The watermark is extracted from data that has been leaked but has been watermarked in the final step. After that, the encrypted data are retrieved by scanning the extracted QR code. In the QR code process, information analysis is the opposite of conversion. The first step in this process is to recognize the dark and light units as an array of zeros and ones.

The next step is to determine the QR version and extract the format data displaying the masking pattern. After that, XOR and the cloud database store the coded region. If the information matches, clients who have leaked important organizational data are presumed guilty. Information mutilation or control can be found with an altered recognition module. In order to determine whether the current image data has been altered, the picture properties are located and compared to the original data attributes. On the off chance that there is an error between the two, it is announced that the duplicate being referred to has been adjusted or changed.



RESULTS AND DISCUSSION



CONCLUSION

A data leakage detection model may be useful for any industry, group, the research community, or institution that frequently shares data online with third parties. The suggested method makes it possible to identify cloud data manipulation and data leaks by employing a watermarking algorithm.

The technique shown embeds a Fast Reaction code, or watermark, made from the accepting client's data and information, furthermore, the picture information that should be conveyed. By

removing the watermark from an image and comparing it to the client's information, the data leak is discovered. Additionally, the characteristics of the tampered data are contrasted with those of the original data in order to identify tampering.

A significant advantage is that a data leakage detection system can provide data transmission security. It is also able to identify that data in the event of a breach. The proposed model provides both security and detection, whereas the current system employs encryption to provide security through a variety of methods. The hybrid watermarking method incorporates imperceptibility and robustness into the model.

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.

[3] 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.