IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10742

Towards privacy preserving content based image retrieval in cloud

Singaravelu M, Roshan K

BE.CSE,Anand Institute of Higher Technology,Affiliated to Anna University,Chennai

ABSTRACT: Privacy-Preserving Content-based image retrieval (CBIR) applications have been rapidly developed along with the increase in the quantity, availability and importance of images in our daily life. However, the wide deployment of the CBIR scheme has been limited by its severe computation and storage requirements. In a privacy- preserving content-based image retrieval scheme, it allows the data owner to outsource the image database and CBIR service to the cloud, without revealing the actual content of the database to the cloud server. Local features are utilized to represent the images, and earth mover's distance (EMD) is employed to evaluate the similarity of images. The EMD computation is essentially a linear programming (LP) problem. The proposed scheme transforms the END problem in such a way that the cloud server can solve it without learning the sensitive information. In Addition, local sensitive hash (LSH) is utilized to improve the search efficiency. The Security analysis and experiments show the security and efficiency of the proposed scheme. In that the encrypted database, secure searchable index and encrypted query will not reveal extra information to the cloud.

Keywords: AES, Advanced Encryption Standard, CBIR, Content-Based Image Retrieval

INTRODUCTION

The first step involved in the development of CBIR project is that the user's requirement was acquired, and the existing system was studied carefully, and the persisting problem faced by the users of the system was analyzed. After analyzing the existing system and its shortcomings, a new system has been developed which satisfies the user's requirements as well as removes the problem due to the existing system.

Problem definition and Analysis Phase is the backbone for the software to be developed. The process of the system analysis involved gathering of facts and figures required in the development of the project. This collection of facts and figures involved the collection of raw data, which includes the basic fields along with type of data. The system study was conducted taking the existing system into mind and evaluating the risk and involved in the development of the project. However, the wide deployment of the CBIR scheme has been limited by its severe computation and storage requirement. Here a privacy-preserving content-based image retrieval scheme is proposed, which allows the data owner to outsource the image database and CBIR service to the cloud, without revealing the actual content of the database to the cloud server.

1.1 SCOPE:

Content Based Image retrieval project allows the data owner to outsource the image database and CBIR service to the cloud, without revealing the actual content of the database to the cloud server. Moreover, these discussed computing resources are not part of on-premises its completely going to be on cloud based one. The proposed scheme transforms the EMD problem in such a way that the cloud server can solve it without learning the sensitive information. Using python script encrypted database, secure searchable index and encrypted query will not reveal extra information to the cloud. So, it can be implemented everywhere where the usage of images is high.

1. 2 OBJECTIVES:

A potential method of solving this problem is to encrypt the whole shared file before sending it to the cloud, and then generate the signatures used to verify the integrity of this encrypted file finally upload this encrypted file and its corresponding signatures to the cloud this method can be realize the sensitive information hiding since only the data owner can be decrypt this file.

Vol. 10, Issue 7, July 2021

DOI 10.17148/IJARCCE.2021.10742

ANALYSIS

- **SYSTEM ANALYSIS**

System analysis is a problem-solving technique that decomposes a system into its component pieces for the purpose of the studying how well those components parts work and interact to accomplish their purpose along with the accurate measurement of the performance delivered by the system.

- **PROBLEM DEFINITION:**

In a day-to-day life with or without knowledge usage of images are growing higher. Images have become a crucial part of life. So, it is important to preserve the privacy of the images. A matter of public concern is how to guarantee the security of data that is outsourced to a remote cloud server and breaks away from the direct control of data owners. Encryption on private data before outsourcing is an effective measure to protect data confidentiality. However, encrypted data make effective data retrieval as a very challenging task. Later, many searchable encryption schemes were proposed based on the symmetric-key and public-key setting to strengthen security and improve query efficiency with the growing popularity of cloud computing and how to securely and efficiently search over the encrypted cloud data becomes a research focus. Cloud server may return incorrect or incomplete query results once he behaves dishonestly for illegal profits. A latent space with lower dimensionality while preserving important discriminative future is the major problem among the users.

3.1.1 DARW BACKS IN EXISTING SYSTEM

- No centralized management for Image retrieval in cloud.
- Traditional On-prem data center.
- Data is not in encrypted format.
- Lagging in data security.
- PROPOSED SYSTEM
- Centralized management for Image retrieval in cloud.
- Virtualized environment in Cloud Computing platform.
- Secure Searchable Index.
- content-based image retrieval.
- Handing user data in virtualized platform.
- Cost Effective, Pay per use.

ADVANTAGE

- User Data Encrypted end to end.
- Secure Searchable Index.
- content-based image retrieval.
- Handing user data in virtualized platform.
- Cost Effective.
- Pay per use.
- Cloud Computing platform.

REQUIREMENT ANALYSIS

3.2.1FUNCTIONAL REQUIREMENTS:

Cloud computing is becoming popular and represents the future of computing. Before it can be embraced by individuals and enterprises, however, the issue of security must be addressed. Early consideration of security in cloud computing systems places it on a par with other functional requirements of the system and significantly improves the security of the system. This work has successfully addressed these security issues, by developing a process to determine security requirements and develop policies for a cloud computing system level-by-level in a structured manner. This methodology analyzes security requirements by identifying threats posed by misusers both external and internal to a system. The process was applied here to typical cloud architecture to demonstrate its function and it was further applied to an actual case study of a cloud service provider in St. Louis, Missouri. In each case, misuse cases at three different were identified. Mal Activity swim lane diagrams for these misuse cases were generated, permitting development of countermeasures for prevention or mitigation. Security requirements were then derived based on the prevention or mitigation options. Finally, security policies were developed to meet at least each requirement.

DOI 10.17148/IJARCCE.2021.10742

3.2.2NON-FUNCTIONAL REQUIREMENTS FEASIBILITY STUDY

The feasibility study is major factor which contributes to analysis of system. In earlier stages of S/W development, it is necessary to check whether system is feasible or not. Detail study was carried out to check workability of proposed system, so the feasibility study is system proposal regarding to its workability, impact on organization, ability to meet user requirements and effective use of resources. Thus, when application progresses it normally goes through a feasibility study and risk analysis.

Feasibility study was carried out considering the following aspects: -

There are different ways of checking whether a system is feasible or not,

but some of the most important tests are the following: -

- Economic Feasibility
- Technical Feasibility
- Operational Feasibility
- Time Feasibility

The last five feasibility studies are made for almost all types of projects and in particular application and system projects. If the five feasibility studies are carried out successfully and properly, a clear picture of the project can be got before developing the project itself. Feasibility studies also analyses various questions and doubts raised during the design phase itself. Feasibility analysis helps in faster development of the project.

Economic Feasibility

The economic feasibility measure the cost effectiveness of the project and judged whether the possible benefit of solving the problem is worthwhile or not

This is a very important aspect to be considered while developing a project. the decided technology based on minimum possible cost factor.It is obvious that one of the main factors to choose Hadoop as a service is its lower price. So, cloud service providers always seek cheaper ways to provide recovery mechanisms by minimizing different types of cost.

Technical Feasibility

Technical feasibility takes care of the technical issues that are to be tested to see whether the system is feasible. Technical feasibility analysis makes s comparison a between the level of technology available and the technology that is needed for the development of the project. The level of technology is determined by the factors such as the software tools available , platform

Technical study is the study of the hardware requirements and software requirements i.e. technical requirements of our project in order to inform the management and user that from particular website designing this much technical resources are required. Considering all below requirements, the project is technically feasible.

Operational Feasibility

The operational scope of the system is verified under operational feasibility.

Operational feasibility deals with the operational requirements of the proposed system if the system is a desktop system then the entire system user access the system only by install the software in each and every system again and again. Hence the operational feasibility of the proposed system is low.The system is operationally feasible because of the benefit of computerized. The total working capacity will be improved due to this proposed system i.e. user need not to install each and every soft-ware at client side. client side is platform independent.

Time Feasibility

A time feasibility study will consider the period in which the project is going to take up to its completion. A project will fail if it takes too long to be completed before it is useful. The client that the system must be completed within 5 or 6 months proposed it. Which is considerable time for development and analysis and it is also feasible with respect to time.

3.2.3 Hardware Requirements:

- 2 GHz core CPU
- 4 GB RAM
- 120 GB HDD

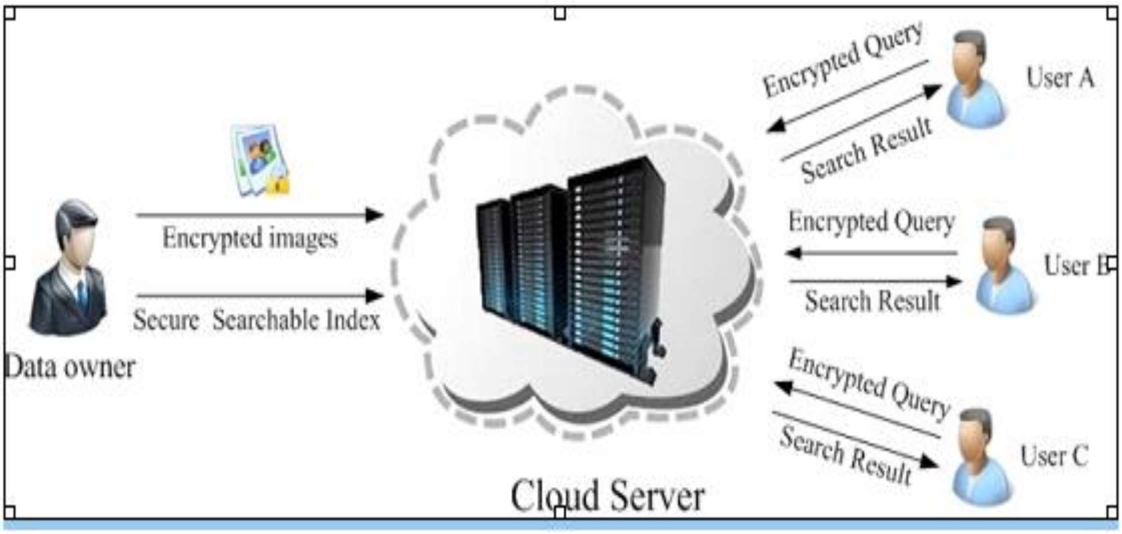
Software Requirements:

- Public Cloud account
- Windows/Linux OS
- Python

DESIGN

ARCHITECTURE DESIGN:

In this design methodology, the system has to construct a secure technique that allows an authorized data user to search over the data owners encrypted data by submitting encrypted query keywords in a privacy preserving manner and is an effective extension of traditional searchable encryption to adapt for the cloud environment.



RESULT AND DISCUSSION

The existing system suffers from the disadvantage that there is no process to encrypt image and retrieve it securely in cloud (i.e., secure searchable index) so there is a possibility of misusing the image. The secure search is thus a technique that allows an authorized data user to search over the data owner's encrypted data by submitting encrypted query keywords in a privacy-preserving manner and is an effective extension of traditional searchable encryption to adapt for the cloud computing environment.

CONCLUSION

A character-based information respectability reviewing plan for secure distributed storage, which bolsters information offering to delicate data covering. In our plan, the record put away in the cloud can be shared and utilized by others depending on the prerequisite that the touchy data of the document is ensured. Moreover, the remote information honestly examining is still ready to be proficiently executed. The security evidence and the exploratory investigation executed. The security evidence and the exploratory investigation exhibit that the proposed plot accomplishes attractive security and productivity.

REFERENCES

[1] C. Pavlopoulou, A. C. Kak, and C. E. Brodley, "Content-based image retrieval for medical imagery," in Medical Imaging 2003. International Society for Optics and Photonics, 2003, pp. 85–96.

[2] A. K. Jain, J.-E. Lee, R. Jin, and N. Gregg, "Content-based image retrieval: An application to tattoo images," in Image Processing (ICIP), 2009 16th IEEE International Conference on. IEEE, 2009, pp. 2745–2748

[3] J. M. Lewin, R. E. Hendrick, C. J. DOrsi, P. K. Isaacs, L. J. Moss, A. Karellas, G. A. Sisney, C. C. Kuni, and G. R. Cutter, "Comparison of full-field digital mammography with screen-film mammography for cancer detection: Results of 4,945 paired examinations 1," Radiology, vol. 218, no. 3, pp. 873–880, 2001.

[4] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE, 2000, pp. 44–55.

[5] E.-J. Goh et al., "Secure indexes." IACR Cryptology ePrint Archive, vol. 2003, p. 216, 2003.

[6] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 79–88.

[7] M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in Data Engineering (ICDE), 2012 IEEE 28th International Conference on. IEEE, 2012, pp. 1156–1167

[8] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, "Achieving usable and privacy-assured similarity search over outsourced cloud data," in INFOCOM, 2012 Proceedings IEEE. IEEE, 2012, pp. 451–459.