IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 5, May 2024

Authorized Keyword Search over Outsourced Encrypted Data in Cloud Environment

Manikanta K. M, A. G Akshay, Aftab Ahmed, Gavi Siddhana Gowda Prof. Shivakeshi Choupiri

Department of Computer Science

Rao Bahadur Y Mahabaleswarappa Engineering College, Bellary, India

Abstract: *This project focuses on developing a secure and efficient mechanism for authorized keyword search over encrypted data outsourced to a cloud environment. With the increasing popularity of cloud computing, data owners are often required to outsource their data to cloud servers for storage and processing. However, the security of outsourced data is a major concern due to the possibility of unauthorized access by cloud providers or malicious attackers. To address this problem, the proposed system introduced a novel expressive authorized keyword search scheme relying on the concept of ciphertext-policy attribute-based encryption. The mechanism also incorporates access control policies to ensure that only authorized users can perform the search operation. Experimental results demonstrate that the proposed mechanism can achieve high search efficiency while maintaining strong security guarantees*

Keywords: authorized keyword

I. INTRODUCTION

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers

II. LITERATURE SURVEY

Recent technological advances have sparked the popularity and success of cloud. This new paradigm is gaining an expanding interest, since it provides cost efficient architectures that support the transmission, storage, and intensive computing of data. However, these promising storage services bring many challenging design issues, considerably due to both loss of data control and abstract nature of clouds. The objective of this survey is to provide a consistent view about both data security concerns and privacy issues that are faced by clients in cloud storage environments. This survey brings a critical comparative analysis of cryptographic defense mechanisms, and beyond this, it explores research directions and technology trends to address the protection of outsourced data in cloud infrastructures.

III. ARCHITECTURE DIAGRAM

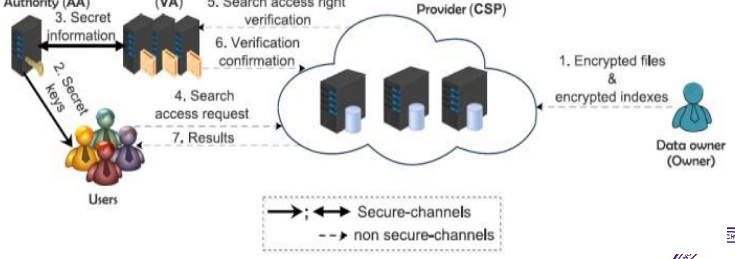

Attribute Authority (AA)
Verification Authorities (VA)
3. Secret information
5. Search access right verification
6. Verification confirmation
Cloud Service Provider (CSP)
2. Secret keys
4. Search access request
7. Results
1. Encrypted files & encrypted indexes
Data owner (Owner)
Users
→; ↔ Secure-channels
- - → non secure-channels

Figure :1

- The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
- The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
- DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
- DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail

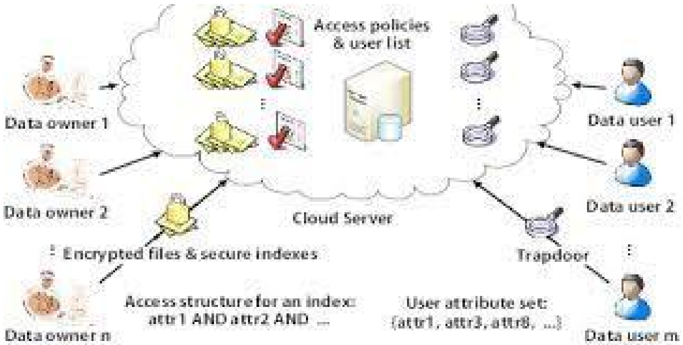
IV. PROPOSED SYSTEM

This project proposes a secure and efficient mechanism for authorized keyword search over encrypted data outsourced to a cloud environment. In this paper, we further investigate the issues of keyword search mechanisms and propose a secure and efficient scheme for authorized keyword search over encrypted data for multi-owner and multi-user cloud environment.

The proposed system uses an expressive fine-grained authorized keyword search scheme for designing for multi- owner and multiuser scenarios using the concept of CP-ABE. The system also develops an interactive protocol is constructed between the user and CSP to avoid overhead involved in establishing secure-channel.

V. METHODOLOGY

A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.


Access policies & user list
Data owner 1
Data owner 2
Data owner n
Data user 1
Data user 2
Data user m
Cloud Server
Encrypted files & secure indexes
Trapdoor
Access structure for an index: attr1 AND attr2 AND ...
User attribute set: {attr1, attr3, attr8, ...}

Problem Definition and Requirements Gathering Identify Stakeholders: Determine who will use the system (data owners, users, and cloud service providers). Define Security Requirements: Specify confidentiality, integrity, and access control requirements.

Performance Criteria: Establish acceptable performance metrics (e.g., search efficiency, encryption/decryption speed).

System Architecture Design

Data Owner Module: Responsible for data encryption, keyword extraction, and generation of search tokens.

User Module: Allows authorized users to generate search queries and decrypt retrieved results.

Cloud Service Provider Module: Stores the encrypted data and processes search queries.

Data Encryption and Indexing

Data Encryption:
Use symmetric encryption (e.g., AES) for data encryption. Encrypt data before outsourcing to the cloud.
Keyword Extraction:
Extract keywords from documents.
Use a consistent method to ensure repeatable extraction (e.g., natural language processing techniques).
Index Creation:
Create an encrypted index of keywords.
Utilize techniques like secure inverted index or bloom filters.

Searchable Encryption Scheme
Preliminary Setup:
Data owner generates cryptographic keys. Share appropriate keys with authorized users. Search Token Generation:
Users generate search tokens using their keys.
Implement techniques like deterministic encryption for token creation

VI. CONCLUSION

In this paper, a fine-grained authorized expressive keyword search scheme has been proposed. The proposed scheme uses the benefits of CP-ABE to perform efficient keyword search over encrypted data and for authorizing users. The security analysis is performed under standard complexity assumptions and it shows that the proposed scheme is semantically secure against the chosen keyword attack. The scheme is also resistant against keyword guessing attacks. Moreover, the performance analysis of the proposed scheme shows that it outperforms the closely-related works in terms of storage, communication overhead, and computational overhead. Security, efficiency, and query expressiveness are the three main factors that define the practical usability of a keyword search scheme. A user expects that the keyword search scheme provides strong security and high efficiency (in terms of computation and communication costs), as high as for normal plaintext search. Further, the query expressiveness will provide the user to make different types of queries. In this paper, we have made an effort to maintain a balance among these three factors. We believe that there is still much work to do for improving the balance among these three factors, i.e., security, efficiency, and query expressiveness. This will lead to the use of the keyword search schemes in privacy-preserving personalized services over the Internet like online advertisements or news.

REFERENCES

[1] N. Kaaniche and M. Laurent, “Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms,” Comput. Commun., vol. 111, pp. 120–141, 2017.
[2] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, “Ensuring security and privacy preservation for cloud data services,” ACM Comput. Survey, vol. 49, no. 1, pp. 13:1–13:39, Jun. 2016.
[3] F. Han, J. Qin, and J. Hu, “Secure searches in the cloud,” Future Generation Comput. Syst.., vol. 62, no. C, pp. 66–75, Sep. 2016.
[4] C. Bosch, P. Hartel, W. Jonker, and A. Peter, “A survey of provably secure searchable encryption,” ACM Comput. Survey, vol. 47, no. 2, pp. 18:1–18:51, Aug. 2014.
[5] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. IEEE Symp. Secur. Privacy, 2000, pp. 44–55.
[6] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: Improved definitions and efficient constructions,” in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 79–88.

DOI: 10.48175/IJARSCT-18468
ISSN 2581-9429 IJARSCT