DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

MAJOR PROJECT - ACADEMIC YEAR 2023-2024

PROJECT TITLE: MULTI-AUTHORITY ATTRIBUTE BASED KEYWORD SEARCH OVER CLOUD DATA

GROUP MEMBERS

S. No	Name	Hall ticket No.
1	L. Sai Kethana	20EG105127
2	M. Uday Sai Kiran	20EG105128
3	N. Meghan Satwik	20EG105134
4	P. Keerthipriya	20EG105141

Project Guide	Mr. Madar Bandu

Signature of the Guide

Problem Statement:

In the current landscape of cloud computing, both organizations and individuals are increasingly reliant on remote storage solutions to handle extensive volumes of sensitive data. However, ensuring the privacy and confidentiality of this data presents notable hurdles, particularly when striving to achieve efficient search capabilities over encrypted data, all while adhering to multi-authority access control policies.

The principal challenge tackled by this project involves creating a resilient system capable of facilitating secure keyword searches over encrypted cloud data while accommodating the demands of multi-authority attribute-based access control. This entails the development of mechanisms that empower authorized users to search for specific information based on keywords or attributes, while concurrently preventing unauthorized access attempts to sensitive cloud-stored data.

Abstract:

To ensure both data security and usability in cloud environments simultaneously, Searchable Encryption (SE) emerges as a crucial technique. Through the utilization of Ciphertext-Policy Attribute-Based Encryption (CP-ABE), the Ciphertext-Policy Attribute-Based Keyword Search (CP-ABKS) scheme accomplishes keyword-based retrieval and fine-grained access control concurrently. However, existing CP-ABKS schemes with a single attribute authority entail costly user certificate verification and secret key distribution, leading to a performance bottleneck in distributed cloud systems. Thus, this study introduces a secure Multi-authority CP-ABKS (MABKS) system to overcome these challenges and alleviate the computation and storage burden on resource-limited devices within cloud systems. Furthermore, the MABKS system extends its functionality to support malicious attribute authority tracing and attribute updates.

Project Objective:

To develop a project that introduces a Searchable Encryption scheme which can simultaneously enable users to search over outsourced encrypted data with only relevant encrypted documents which can only accessed by the authorized users.

Software requirements:

- Java 1.8
- JSP
- Html, CSS
- MySql 5.5
- Tomcat 8

Hardware requirements:

- Updated Processor
- Min 1 GB RAM
- Min 100 GB hard disk

References:

[1] Yinbin Miao, Robert H. Deng, Fellow, IEEE, Ximeng Liu, Kim-Kwang Raymond Choo, Senior Member, IEEE, Hongjun Wu, and Hongwei Li "Multi-authority Attribute-Based Keyword Search over Encrypted Cloud Data" IEEE Transactions on Dependable and Secure Computing (Volume: 18, Issue: 4 01 July-Aug. 2021)

[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symposium on Security and Privacy (SP'00), 2000, pp. 44–55.

[3] D.Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT'04), vol. 3027, 2004, pp. 506–522.

[4] Q. Zheng, S. Xu, and G. Ateniese, "Vabks: verifiable attribute-based keyword search over outsourced encrypted data," in Proc. IEEE Conference on Computer Communications (INFOCOM'14), 2014, pp. 522–530.