Thesis Overview:

Privacy-Preserving Ciphertext-Policy Attribute-Based Search over Encrypted Data in Cloud Storage

Uma Sankararao Varri
National Institute of Technology-Warangal, Telangana, India.
Ph.D. in Computer Science
Thesis Supervisors: Dr. Syam Kumar P and Dr. Kadambari K.V.
umasankararao.varri@gmail.com psyamkumar@idrbt.ac.in kadambari@nitw.ac.in

Introduction

Cloud storage is one of the cloud computing services which allows data users to store their data remotely to the cloud. Thus, most individuals, institutions, and organizations are outsourcing their data to the cloud. Most popular cloud-based storage services are Amazon S3, Google Drive, Microsoft Azure, Apple iCloud, Dropbox, etc. Cloud storage service brings significant benefits to data owners, say, (1) reducing capital and management costs (2) reducing cloud users' burden of storage management and equipment maintenance, (3) avoiding investing a large amount of hardware, (4) accessing data over the Internet from any location from any devices such as desktop computers, laptops, tablets, and smartphones which offers increased flexibility and accessibility.

Motivation

Despite the benefits, outsourcing the sensitive data brings privacy concerns due to the untrusted nature of the cloud and it is treated as honest-but-curious, i.e., it performs all the operations faithfully but may be curious to know the users' sensitive data. This has become a big obstacle for the wide acceptance of cloud storage services in various organizations, such as banking and healthcare. Hence, preserving the privacy of outsourced sensitive data is mandatory. Encrypting the data before outsourcing is one solution to protect the privacy of the data. Although encrypting the data prevents information leakage, it reduces the possibility of computations over ciphertexts, such as searching for keywords or specific items within the data. Searchable encryption (SE) is a solution to achieve data privacy along with keyword search over ciphertexts. In SE, data owners outsource their encrypted data and encrypted keyword index to the cloud. Then, data users issue a trapdoor containing the search keyword to the cloud. The cloud is responsible for searching between the encrypted index and the trapdoor and returning the search results (on successful search) to the data user. Inspired by the concept of SE, several schemes were proposed based on encryption techniques such as symmetric searchable encryption (SSE) and public-key searchable encryption (PKSE). However, SSE and PKSE schemes suffer from issues like the existence of secure channels, and complex key management. Moreover, these schemes do not provide fine-grained access control. With multi-user and multi-owner data usability scenarios, fine-grained access control is essential in controlling the data access privileges. Fine-grained access control allows only legitimate users to decrypt the file and resist unauthorized access.

To achieve fine-grained access control, keyword search over ciphertexts, and data privacy, attribute-based searchable encryption (ABSE) schemes were proposed. In ABSE, a third-party authority (TA) is employed to issue each registered user's secret key (which contains user attributes/policy). The data owner encrypts the documents with access policy/attributes and the index with public parameters. Later, the data user generates the trapdoor and submits it to the cloud by using the secret key. After a successful search, the cloud returns the matched documents to the data user. The data user can decrypt the documents if his attributes satisfy the policy. There are two ABSE variants named key-policy ABSE (KP-ABSE) and ciphertext-policy ABSE (CP-ABSE). CP-ABSE is most suitable for outsourced data retrieval since the data owner controls the access policy. Although previous CP-ABSE schemes achieved significant attention, certain issues need to be addressed to strengthen security and improve efficiency. The issues identified are as follows: 1) Data Authentication, 2) Inefficient encryption and decryption, 3) Inefficient traceability and revocation, 4) Key-escrow problem, 5) Prone to quantum attacks, 6) Lack of semantic search.

The above issues motivated us to design secure and efficient CP-ABSE schemes for the data stored in the cloud.

Contributions

To achieve all the above-mentioned objectives, we proposed privacy-preserving ciphertext-policy attribute-based searchable encryption schemes in cloud storage. The contributions of the thesis are summarized as follows:

1. Practical Verifiable Multi-Keyword Attribute-Based Searchable Signcryption in Cloud Storage

In this contribution, we proposed a practical verifiable multi-keyword attribute-based searchable signcryption scheme in cloud storage. The scheme integrates CP-ABSE with signcryption to achieve data privacy, access control, and data authenticity. Further, we integrate the Multi-dimensional B^{+}-tree with the Merkle tree in index construction to enhance the search efficiency and to verify the search results. The security analysis of the scheme evidences that the scheme achieves data privacy, index privacy, index verifiability, trapdoor unlinkability, access control, and data authenticity.

2. FELT-ABKS: Fog-Enabled Lightweight Traceable Attribute-based Keyword Search Over Encrypted Data

In this contribution, we proposed a FELT-ABKS: fog-enabled lightweight traceable attribute-based keyword search over encrypted data by using ciphertext-policy attribute-based keyword search to realize keyword search and fine-grained access control. FELT-ABKS achieves minimal computation cost at end users by transferring maximum computation to fog nodes. Further, FELT-ABKS traces the malicious users who misuse their secret key. Besides, it supports user revocation and attribute revocation.

3. KEF-ABKSM: Key Escrow Free Attribute-Based Keyword Search in Cloud Storage

In this contribution, we proposed a KEF-ABKSM: key escrow free attribute-based keyword search in the cloud. Key escrow free mechanism prevents the third-party key generation authority from accessing the ciphertexts using users' secret keys. In addition, it demonstrates how to trace malicious users and revoke them from the system

4. CP-ABSEL: Ciphertext-Policy Attribute-Based Searchable Encryption from Lattice in Cloud Storage

In this contribution, we propose a novel ciphertext-policy attribute-based searchable encryption from lattice (CP-ABSEL) in cloud storage, since lattice-based cryptography is quantum attacks free. In CP-ABSEL, we adopted learning with errors (LWE) hardness assumption to resist from quantum attacks.

5. An Efficient Attribute-based Dynamic Multi-Keyword Semantic Search over Encrypted Data in Cloud

In this contribution, we proposed a novel efficient and dynamic attribute-based semantic search scheme that supports multi-keyword semantic search over encrypted data in the cloud. The scheme uses a neural-network-based natural language processing model called the Doc2Vec model to enable semantic-aware multi-keyword search. Further, the scheme integrates the CP-ABSE and lattice-based cryptography to achieve data privacy, access control, and to resist from quantum attacks.

Conclusion

This thesis presents Privacy-Preserving Ciphertext-Policy Attribute-Based Searchable encryption schemes to achieve data privacy, keyword searchability, and fine-grained access control. The works related to this thesis address the issues with the existing related schemes like Data Authentication, Inefficient encryption and decryption, Inefficient traceability and revocation, Key-escrow problems, Prone to quantum attacks, and Lack of semantic search. The performance of all the proposed schemes was evaluated on a local machine.

Future Directions

Although existing CP-ABSE schemes have gotten significant attention, several challenges need to be addressed. In our future work, we will try to work on the following:

- Designing CP-ABSE scheme supporting different functionalities along to resist quantum attacks is necessary. Because the next generation belongs to quantum computing.

- CP-ABSE schemes use a centralized cloud storage system, leading to singlepoint-of-failure. Hence, the designing of secure decentralized CP-ABSE schemes must be explored.

- All our proposed schemes support multi-keyword search. It is necessary to design CP-ABSE schemes to support range queries, temporal queries, and spacial queries for the broad adoption of CP-ABSE schemes.

Publications with this Thesis Work

1) Varri, Uma Sankararao, Sreekanth Kasani, Syam Kumar Pasupuleti, and K. V. Kadambari. "FELT-ABKS: Fog-Enabled Lightweight Traceable Attribute-based Keyword Search Over Encrypted Data." IEEE Internet of Things Journal (2021). DOI: 10.1109/JIOT.2021.3139148.

2) Varri, Uma Sankararao, Syam Kumar Pasupuleti, and K. V. Kadambari. "KEF-ABKSM: Key Escrow Free Attribute-Based Keyword Search for Shared Multi-owner in Cloud Storage." Journal of Systems Architecture

3) Varri, Uma Sankararao, Syam Kumar Pasupuleti, and K. V. Kadambari. "Practical verifiable multi-keyword attribute-based searchable signcryption in cloud storage." Journal of Ambient Intelligence and Humanized Computing (2022): 1-13. DOI: 10.1007/s12652-022-03715-1.

4) Varri, Uma Sankararao, Syam Kumar Pasupuleti, and K. V. Kadambari. "CP-ABSEL: Ciphertext-policy attribute-based searchable encryption from lattice in cloud storage." Peer-to-Peer Networking and Applications 14.3 (2021): 1290-1302. DOI: 10.1007/s12083-020-01057-3.

5) Varri, Umasankararao, Syamkumar Pasupuleti, and K. V. Kadambari. "A scoping review of searchable encryption schemes in cloud computing: taxonomy, methods, and recent developments." The Journal of Supercomputing 76.4 (2020): 3013-3042. DOI: 10.1007/s11227-019-03087-y.

6) Varri, Uma Sankararao, Syam Kumar Pasupuleti, and K. V. Kadambari. ”Key-escrow free attribute-based multi-keyword search with dynamic policy update in cloud computing.” 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID). IEEE, 2020. DOI: 10.1109/CCGrid49817.2020.00-48.

Citation: U. S. Varri. A *Thesis Overview: Privacy-Preserving Ciphertext-Policy Attribute-Based Search over Encrypted Data in Cloud Storage.* Journal of Computer Science & Technology, vol. 23, no. 1, pp. 85-87, 2023.
DOI: 10.24215/16666038.23.e07