Achieving Secure, Universal, And Fine-grained Query Results Verification For Secure Search Scheme Over Encrypted Cloud Data

ABSTRACT

- Secure search techniques over encrypted cloud data allow an authorized user to query data files of interest by submitting encrypted query keywords to the cloud server in a privacy-preserving manner.
- However, in practice, the returned query results may be incorrect or incomplete in the dishonest cloud environment. For example, the cloud server may intentionally omit some qualified results to save computational resources and communication overhead.
- Thus, a well-functioning secure query system should provide a query results verification mechanism that allows the data user to verify results. In this paper, we design a secure, easily integrated, and fine-grained query results verification mechanism, by which, given an encrypted query results set, the query user not only can verify the correctness of each data file in the set but also can further check how many or which qualified data files are not returned if the set is incomplete before decryption.

- The verification scheme is loose-coupling to concrete secure search techniques and can be very easily integrated into any secure query scheme. We achieve the goal by constructing secure verification object for encrypted cloud data. Furthermore, a short signature technique with extremely small storage cost is proposed to guarantee the authenticity of verification object and a verification object request technique is presented to allow the query user to securely obtain the desired verification object. Performance evaluation shows that the proposed schemes are practical and efficient.

EXISTING SYSTEM

- Recently, with the growing popularity of cloud computing, how to securely and efficiently search over encrypted cloud data becomes a research focus.
- Some approaches have been proposed based on traditional searchable encryption schemes in which aim to protect data security and query privacies with better query efficient for cloud computing.
- However, all of these schemes are based on an ideal assumption that the cloud server is an ”honest-but-curious” entity and keeps robust and secure software/hardware environments. server

- As a result, correct and complete query results always be unexceptionally returned from the cloud server when a query ends every time. However, in practical applications, the cloud server may return erroneous or incomplete query results once he behaves dishonestly for illegal profits such as saving computation and communication cost or due to possible software/hardware failure of the

DISADAVANTAGES

- Encrypted data make effective data retrieval a very challenging task.
- Security problem

PROPOSED SYSTEM

- 1)We formally propose the verifiable secure search system model and threat model and design a fine-grained query results verification scheme for secure keyword search over encrypted cloud data.
- 2) We propose a short signature technique based on certificateless public-key cryptography to guaran-tee the authenticity of the verification objects them-selves.
- 3) We design a novel verification object request tech-nique based on Paillier Encryption, where the cloud server knows nothing about what the dat a user is requesting for and which verification objects are returned to the user.

- 4) We provide the formal security definition and proof and conduct extensive performance experiments to evaluate the accuracy and efficiency of our pro-posed scheme

ADAVANTAGES

- our scheme can verify the correctness of each encrypted query result or further accurately find out how many or which qualified data files are returned by the dishonest cloud server.

HARDWARE REQUIREMENTS

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

- Operating system : Windows XP/7.
- Coding Language : ASP.net, C#.net /java

CONCLUSION

- In this paper, we propose a secure, easily integrated, and fine-grained query results verification scheme for secure search over encrypted cloud data. Different from previous works, our scheme can verify the correctness of each encrypted query result or further accurately find out how many or which qualified data files are returned by the dishonest cloud server.
- A short signature technique is designed to guarantee the authenticity of verification object itself. Moreover, we design a secure verification object request technique, by which the cloud server knows nothing about which verification object is requested by the data user and actually returned by the cloud server.