Achieving secure, universal, and fine-grainedquery results verification for secure searchscheme over encrypted cloud data

ABSTRACT:

Secure search techniques over encrypted cloud data allow an authorized user to query data files of interest by submittingencrypted query keywords to the cloud server in a privacy-preserving manner. However, in practice, the returned query results maybe incorrect or incomplete in the dishonest cloud environment. For example, the cloud server may intentionally omit some qualifiedresults to save computational resources and communication overhead. Thus, a well-functioning secure query system should provide aquery results verification mechanism that allows the data user to verify results. In this paper, we design a secure, easily integrated, andfine-grained query results verification mechanism, by which, given an encrypted query results set, the query user not only can verifythe 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 isincomplete before decryption. The verification scheme is loose-coupling to concrete secure search techniques and can be very easilyintegrated 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 verificationobject 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 cloudcomputing, how to securely and efficiently search overencrypted cloud data becomes a research focus. Someapproaches have been proposed based on traditionalsearchable encryption schemes, which aim to protect datasecurity and query privacies with better query efficientfor cloud computing.
- Wang etal. applied hash chain technique to implement the completenessverification of query results by embedding theencrypted verification information into their proposedsecure searchable index.
- Sun et al. used encryptedindex tree structure to implement secure query resultsverification functionality. In this scheme, when thequery ends, the cloud server returns query results alongwith a minimum encrypted index tree, then the datauser searches this minimum index tree using the samesearch algorithm as the cloud server did to finish resultverification.
- Zheng et al. constructed a verifiablesecure query scheme over encrypted cloud data basedon attribute-based encryption technique (ABE) in thepublic-key setting.
- Sun et al. referred to the Merklehash tree and applied Pairing operations to implementthe correctness and completeness verification of queryresults for keyword search over large dynamic encryptedcloud data.

DISADVANTAGES OF EXISTING SYSTEM:

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

- All of these schemes arebased on an ideal assumption that the cloud server is an"honest-but-curious" entity and keeps robust and securesoftware/hardware environments. As a result, correctand complete query results always be unexceptionallyreturned from the cloud server when a query ends everytime. However, in practical applications, the cloud servermay return erroneous or incomplete query results oncehe behaves dishonestly for illegal profits such as savingcomputation and communication cost or due to possiblesoftware/hardware failure of the server.
- These verification mechanisms provide a coarse grained verification, i.e., if the query result set contains all qualified and correct data files, then these schemes reply yes, otherwise reply no. Thus, if the verification algorithm outputs no, a data user has to abort the decryption for all query results despite only one query result is incorrect.
- These verification mechanisms are generally tightly coupled to corresponding secure query constructions and have not universality.

PROPOSED SYSTEM:

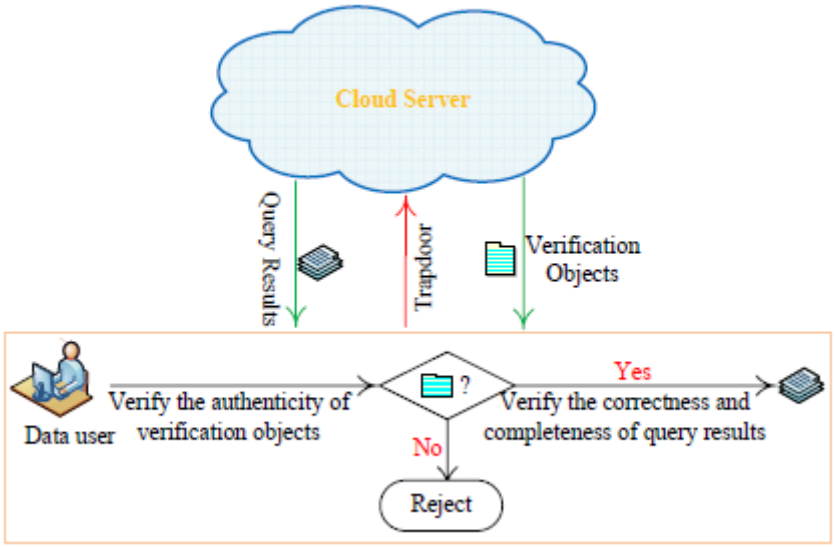
- In this paper, we extend and reinforce our workto make it more applicable in the cloud environment andmore secure to against dishonest cloud server. The maincontributions of this paper are
- We formally propose the verifiable secure searchsystem model and threat model and design a finegrainedquery results verification scheme for securekeyword search over encrypted cloud data.

- We propose a short signature technique based oncertificateless public-key cryptography to guaranteethe authenticity of the verification objects themselves.
- We design a novel verification object request techniquebased on Paillier Encryption, where thecloud server knows nothing about what the datauser is requesting for and which verification objectsare returned to the user.

ADVANTAGES OF PROPOSED SYSTEM:

- We provide the formal security definition and proof and conduct extensive performance experiments to evaluate the accuracy and efficiency of our proposed scheme.
- Our scheme can verify the correctnessof each encrypted query result or further accuratelyfind out how many or which qualified data files arereturned by the dishonest cloud server.
- A short signaturetechnique is designed to guarantee the authenticity ofverification object itself

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.

- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 1 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

REFERENCE:

Hui Yin, Zheng Qin, Jixin Zhang, Lu Ou, and Keqin Li, Fellow, IEEE, "Achieving secure, universal, and fine-grainedquery results verification for secure searchscheme over encrypted cloud data" **IEEE Transactions on Cloud Computing, 2017.**