**Keyword Search over Encrypted Data with Symmetric-Key Based Verification**

**ABSTRACT:-**

Verifiable Searchable Symmetric Encryption, as an important cloud security technique, allows users to retrieve the encrypted data from the cloud through keywords and verify the validity of the returned results. Dynamic update for cloud data is one of the most common and fundamental requirements for data owners in such schemes. To the best of our knowledge, the existing verifiable SSE schemes supporting data dynamic update are all based on asymmetric-key cryptography verification, which involves time-consuming operations. The overhead of verification may become a significant burden due to the sheer amount of cloud data. Therefore, how to achieve keyword search over dynamic encrypted cloud data with efficient verification is a critical unsolved problem. To address this problem, we explore achieving keyword search over dynamic encrypted cloud data with symmetric-key based verification and propose a practical scheme in this paper. In order to support the efficient verification of dynamic data, we design a novel Accumulative Authentication Tag (AAT) based on the symmetric-key cryptography to generate an authentication tag for each keyword. Benefiting from the accumulation property of our designed AAT, the authentication tag can be conveniently updated when dynamic operations on cloud data occur. In order to achieve efficient data update, we design a new secure index composed by a search table ST based on the orthogonal list and a verification list VL containing AATs. Owing to the connectivity and the flexibility of ST, the update efficiency can be significantly improved. The security analysis and the performance evaluation results show that the proposed scheme is secure and efficient.

|  |  |
| --- | --- |
| **EXSISTING SYSTEM** | **PROPOSED SYSTEM** |
| * The first scheme, which adopts the Message Authentication Code (MAC) to verify the search results, works fine with static cloud data. * In order to solve this problem, the second scheme uses the timestamp functionality of the RSA accumulator to obtain the verifiability of search results. * The follow-up schemes utilize RSA accumulator to achieve the verification for search results and the dynamic update for cloud data | * In this paper, we explore how to achieve keyword search over dynamic encrypted cloud data with symmetric-key based verification. * In order to support the efficient verification of dynamic data, we design a novel symmetric-key based Accumulative Authentication Tag (AAT) to generate an authentication tag for each keyword. * For each keyword, we construct a linked list with the same length aiming at hiding the frequency of each keyword |
| **EXISTING ALGORITHM**  RSA accumulator to achieve the verification  for search results and the dynamic update for cloud data | **PROPOSED ALGORITHM:-**  Accumulative Authentication Tag (AAT) based on the symmetric-key cryptography |
| **ALGORITHM DEFINITION:-**  This scheme and scheme [9] both leverage RSA accumulator to realize the results verification and the data dynamics. The verification techniques used in above verifiable and dynamic schemes are all based on asymmetric-key cryptography, which involves time-consuming operations. As a result, the verification efficiency is very low in these schemes. | **ALGORITHM DEFINITION:-**  Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both the encryption of plaintext and the decryption of ciphertext. ... The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. |
| **DRAWBACKS:-**   * Meanwhile, with the rise of IoT, * low-performance terminals are deployed for receiving and uploading patient data to the server. | **ADVANTAGES:-**   * When the data needs to be updated, the cloud server might not perform the update operation for saving computation. * It cost or software/ hardware failures. |

**System model with a cloud server, a data owner and**

**data users.**

****

**MINIMUMSYSTEM REQUIREMENTS**

**HARDWARE REQUIREMENTS**

* PROCESSOR : DUAL CORE 2 DUO.
* RAM : 2GB DD RAM
* HARD DISK : 250 GB

**SOFTWARE REQUIREMENTS**

* FRONT END : J2EE (JSP, SERVLET)
* BACK END : MY SQL 5.5
* OPERATING SYSTEM : WINDOWS 7
* IDE : ECLIPSE