A Secure and Dynamic Multi Keyword Ranked Search over Encrypted Cloud Data

R. Prema[1], K.S.D. Narendra Gupta[2], K. Teja[3]

[1]Assistant Professor, Department of CSE, SCSVMV (Deemed to be University), Tamilnadu
[2]Student, Department of CSE, SCSVMV (Deemed to be university), Tamilnadu.
[3]Student, Department of CSE, SCSVMV (Deemed to be university), Tamilnadu

---

Abstract: - *Due to the growing recognition of cloud computing, an increasing number of facts proprietors are stimulated to outsource their facts to cloud servers for outstanding comfort and decreased fee in facts management. However, touchy facts need to be encrypted earlier than outsourcing for privateness requirements, which obsoletes facts usage like key-word-primarily based totally file retrieval.In this paper, we present a consistent multi-key-phrase ranked are seeking scheme over encrypted cloud facts, which simultaneously allows dynamic update operations like deletion and insertion of files.. Specifically, the vector area version and the widely-used TF_IDF version are mixed withinside the index production and question generation. We assemble a unique tree-primarily based totally index shape and endorse a "Greedy Depth-first Search" set of rules to offer green multi-key-word ranked seek. The steady KNN set of rules is applied to encrypt the index and question vectors, and in the meantime make certain correct relevance rating calculation among encrypted index and question vectors. In order to withstand statistical attacks, phantom phrases are brought to the index vector for blinding seek results. Due to using our unique tree-primarily based totally index shape, the proposed scheme can gain sub-linear seek time and address the deletion and insertion of files flexibly.*

1. INTRODUCTION

Cloud computing is using computing assets (hardware and software program) which can be introduced as a provider over a network (commonly the Internet). The call comes from the not unusualplace use of a cloud-fashioned image as an abstraction for the complicated infrastructure it incorporates in gadget diagrams. Cloud computing entrusts faraway offerings with a user's records, software program and computation. Cloud computing includes hardware and software program assets made to be had at the Internet as controlled third-celebration offerings. These offerings commonly offer get admission to to superior software program programs and high-cease networks of server computers. The purpose of cloud computing is to use conventional supercomputing, or high-overall performance computing energy, generally utilized by army and studies facilities, to carry out tens of trillions of computations in keeping with second, in purchaser-orientated programs along with monetary portfolios, to supply customized information, to offer records garage or to energy massive, immersive laptop games. The cloud computing makes use of networks of massive businesses of servers commonly strolling low-value purchaser PC generation with specialised connections to unfold records-processing chores throughout them. This shared IT infrastructure incorporates massive swimming pools of structures which can be related together. Often, virtualization strategies are used to maximise the energy of cloud

2. Literature Survey

1) Security challenges for the public cloud

Cloud computing represents today's maximum interesting computing paradigm shift in statistics technology. However, protection and privateness are perceived as number one boundaries to its huge adoption. Here, the authors define numerous important protection demanding situations and inspire in addition research of protection answers for a straightforward public cloud environment.

2) A fully homomorphic encryption scheme

We endorse the primary completely homomorphic encryption scheme, fixing an antique open problem. Such a scheme permits one to compute arbitrary features over encrypted records with out the decryption key—i.e., given encryptions E(m1), ..., E(mt) of m1, ..., m t, you can still correctly compute a compact ciphertext that encrypts f(m1, ..., mt) for any correctly computable feature f.Fully homomorphic encryption has severa applications. For example, it allows encrypted seek engine queries—i.e., a seek engine can come up with a succinct encrypted solution to your (boolean) question with out even understanding what your question was. It additionally allows looking on encrypted records; you may keep your encrypted records on a faraway server, and later have the server retrieve handiest documents that (while decrypted) fulfill a few boolean constraint, despite the fact that the server can't decrypt the documents on its very own. More broadly, it improves the performance of steady multipartycomputation. In our solution, we start with the aid of using designing a fairly homomorphic "boostrappable" encryption scheme that works while the feature f is the scheme's very own decryption feature. We then display how, thru recursive self-embedding, bootstrappable

Implementation

MODULES

 Data Owner Module

 Data User Module

 Cloud server and Encryption Module

 Rank Search Module

MODULES DESCRIPTION

Data Owner Module

This module facilitates the proprietor to sign in the ones information and additionally consist of login information. This module facilitates the proprietor to add his record with encryption the usage of RSA algorithm. This guarantees the documents to be covered from unauthorized user. Data proprietor has a set of files F = that he desires to outsource to the cloud server in encrypted shape whilst nevertheless preserving the functionality to look on them for powerful utilization. In our scheme, the records proprietor first of all builds a stable searchable tree index I from file series F, after which generates an encrypted file series C for F. Afterwards, the records proprietor outsources the encrypted series C and the stable index I to the cloud server, and securely distributes the important thing statistics of trapdoor era and file decryption to the legal records users. Besides, the records proprietor is accountable for the replace operation of his files saved withinside the cloud.

Data User Module

This module consists of the person registration login information. This module is used to assist the consumer to look the report the use of the a couple of key phrases idea and get the correct end result listing primarily based totally at the person question. The person goes to pick out the specified report and sign up the person information and get activation code in mail e mail earlier than input the activation code. After person can down load the Zip report and extract that report. Data customers are legal ones to get admission to the files of information owner. With t question keywords, the legal person can generate a trapdoor TD consistent with seek manage mechanisms to fetch okay encrypted files from cloud server. Then, the information person can decrypt the files with the shared mystery key.

Cloud Server and Encryption Module:

This module is used to assist the server to encrypt the record the usage of RSA Algorithm and to transform the encrypted record to the Zip report with activation code after which activation code ship to the consumer for download. Cloud server shops the encrypted record series C and the encrypted searchable tree index I for facts owner. Upon receiving the trapdoor TD from the facts consumer, the cloud server executes seek over the index tree I, and sooner or later returns the corresponding series of top-okay ranked encrypted documents. Besides, upon receiving the replace statistics from the facts owner, the server wishes to replace the index I and record series C in keeping with the obtained statistics. The cloud server withinside the proposed scheme is taken into consideration as "honest-but-curious", that's hired through masses of works on stable cloud facts seek

Rank Search Module

These modules make certain the consumer to go looking the documents which can be searched regularly the use of rank search. This module permits the consumer to down load the document the use of his mystery key to decrypt the downloaded data. This module permits the Owner to view the uploaded documents and downloaded documents. The proposed scheme is designed to offer now no longer simplest multi-key-word question and correct end result ranking, however additionally dynamic replace on report collections. The scheme is designed to save you the cloud server from mastering extra facts approximately the report collection, the index tree, and the question.

CONCLUSION:

In this paper, a stable, green and dynamic seek scheme is proposed, which helps now no longer handiest the correct multi-key-word ranked seek however additionally the dynamic deletion and insertion of files. We assemble a unique key-word balanced binary tree because the index, and recommend a "Greedy Depth-first Search" set of rules to reap higher performance than linear seek. In addition, the parallel seek method may be accomplished to in addition lessen the time cost. The protection of the scheme is included towards risk fashions via way of means of the usage of the stable kNN set of rules. Experimental effects reveal the performance of our proposed scheme. There are nevertheless many mission troubles in symmetric SE schemes. In the proposed scheme, the records proprietor is liable for producing updating records and sending them to the cloud server. Thus, the records proprietor desires to shop the unencrypted index tree and the records which might be essential to recalculate the IDF values. Such an energetic records proprietor might not be very appropriate for the cloud computing model. It may be a significant however tough destiny paintings to layout a dynamic searchable encryption scheme whose updating operation may be finished via way of means of cloud server handiest, in the meantime booking the cappotential to guide multi-key-word ranked seek. In addition, because the maximum of works approximately searchable encryption, our scheme in particular considers the mission from the cloud server. Actually, there are many stable demanding situations in a multi-consumer scheme. Firstly, all of the customers commonly preserve the equal stable key for trapdoor technology in a symmetric SE scheme. In this case, the revocation of the consumer is large mission. If it's miles had to revoke a consumer on this scheme, we want to rebuild the index and distribute the brand new stable keys to all of the legal customers. Secondly, symmetric SE schemes commonly anticipate that every one the records customers are trustworthy. It isn't always realistic and a bent records consumer will lead to many stable troubles. For example, a bent records consumer can also additionally seek the files and distribute the decrypted files to the unauthorized ones. Even more, a bent records consumer can also additionally distribute his/her stable keys to the unauthorized ones. In the destiny works, we are able to try and enhance the SE

REFERENCES

[1] K. Ren, C.Wang, Q.Wang et al., “Security challenges for the public cloud,”IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[2] S. Kamara and K. Lauter, “Cryptographic cloud storage,” in FinancialCryptography and Data Security. Springer, 2010, pp. 136–149.

[3] C. Gentry, “A fully homomorphic encryption scheme,” Ph.D. dissertation,Stanford University, 2009.

[4] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, “Fuzzy keywordsearch over encrypted data in cloud computing,” in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–5.

[5] M. Kuzu, M. S. Islam, and M. Kantarcioglu, “Efficient similarity search overencrypted data,” in Data Engineering (ICDE), 2012 IEEE 28th International Conference on. IEEE, 2012, pp. 1156–1167.

[6] C. Wang, K. Ren, S. Yu, and K. M. R. Urs, “Achieving usable and privacy-assured similarity search over outsourced cloud data,” in INFOCOM, 2012 Proceedings IEEE. IEEE, 2012, pp. 451–459.