International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Achieving Secure, Universal, and Fine-Grainedquery Results Verification for Secure Searchscheme Over Encrypted Cloud Data

S. Priya, N. Nandhini

Assistant Professor, Department of Information Technology,
GKM College of Engineering and Technology, Affiliated Under, Anna University, Chennai, Tamil Nadu, India

How to cite this paper: S. Priya | N. Nandhini "Achieving Secure, Universal, and Fine-Grainedquery Results Verification for Secure Searchscheme Over Encrypted Cloud Data" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.1997-1999, **https://doi.org/10.31142/ijtsrd26620**

IJTSRD26620

ABSTRACT

Secure pursuit strategies over encoded cloud information enable an approved client to inquiry information documents of enthusiasm by submitting scrambled question catchphrases to the cloud server in a protection safeguarding way. In any case, practically speaking, the returned question results might be mistaken or deficient in the exploitative cloud condition. For instance, the cloud server may deliberately preclude some qualified outcomes to spare computational assets and correspondence overhead. In this manner, a well-working secure inquiry framework ought to give a question comes about check system that enables the information client to confirm comes about. In this paper, we outline a protected, effectively incorporated, and fine-grained question comes about confirmation instrument, by which, given an encoded inquiry comes about set, the question client not exclusively can check the rightness of every information record in the set yet in addition can additionally check what number of or which qualified information documents are not returned if the set is inadequate before unscrambling.

INTRODUCTION

In a search process, for a returned query results set that contains multiple encrypted data files, a data user may wish to verify the correctness of each encrypted data file (thus, he can remove incorrect results and retain the correct ones as the ultima query results) or wants to check how many or which qualified data files are not returned on earth if the cloud server intentionally omits some query results. These information can be regarded as a hard evidence to punish the cloud server.

This is challenging to achieve the fine-grained verifications since the query and verification are enforced in the encrypted environment. We proposed a secure and fine-grained query results verification scheme by constructing the verification object for encrypted outsourced data files. When a query ends, the query results set along with the corresponding verification object are returned together, by which the query user can accurately verify: 1) the correctness of each encrypted data file in the results set; 2) how many qualified data files are not returned and 3) which qualified data files are not returned. Furthermore, our proposed verification scheme is lightweight and loose-coupling to concrete secure query schemes and can be very easily equipped into any secure query scheme for cloud computing.However, some necessary extensions and importantworks need to be further supplied to perfect our original scheme such as detailed performance evaluation and formal security definition and proof. More importantly, in the dishonest cloud environment, the scheme suffers from the following two important security problems: 1) Just as possibly tampering or deleting query results, the dishonest cloud server may also tamper or forge verification objects themselves to make the data user impossible to perform verification operation. Specially, once the cloud server knows that the query results verification scheme is provided in the secure search system, he may return inveracious verification object to escape responsibilities of misbehavior. 2) When a data user wants to obtain the desired verification object, some important information will be revealed such as which verification objects are being or have been requested before frequently, etc. These information may leak query user's privacy and expose some useful contents about data files. More importantly, these exposed information may become temptations of misbehavior for the cloud server.

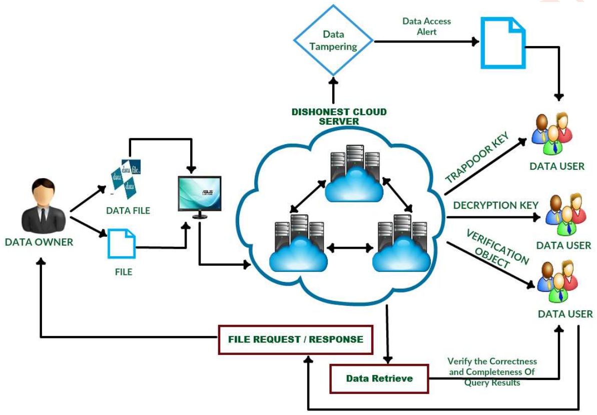
Proposed System

A secure and fine-grained query results verification scheme by constructing the verification object for encrypted outsourced data files. When a query ends, the query results set along with the corresponding verification object are returned together, by which the query user can accurately verify: 1) the correctness of each encrypted data file in the results set; 2) how many qualified data files are not returned and 3) which qualified data files are not returned. Furthermore, our proposed verification scheme is lightweight and loose-coupling to concrete secure query schemes and can be very easily equipped into any secure query scheme for cloud computing. Just as possibly tampering or deleting query results, the dishonest cloud server may also tamper or forget verification objects themselves to make the data user impossible to perform verification operation. Specially, once the cloud server knows that the query results verification scheme is provided in the secure search system, this information may leak query user's privacy and expose some useful contents about data files. More importantly, this exposed information may become temptations of misbehavior for the cloud server.

Advantages

- 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.
- We propose a short signature technique based on certificate less public-key cryptography to guarantee the authenticity of the verification objects themselves.
- We design a novel verification object request technique based on Parlier Encryption, where the
- Cloud server knows nothing about what the data user is requesting for and which verification objects are returned to the user.
- We provide the formal security definition and proof and conduct extensive performance experiments to evaluate the accuracy and efficiency of our proposed scheme.

ARCHITECTURE DIAGRAM



MODULES

- Query results verification
- Outsourcing Encrypted File
- Verification object construction
- Verification object signature and authentication
- Unauthorized access data alert
- File Recovery

MODULES DESCRIPTION

QUERY RESULTS VERIFICATION

The query result verification mechanism allows the data user to verify the results. In this project, we designed a safe, easy to integrate Fine-grained query results validation mechanism, by giving a given query result set, the query user can not only verify The correctness of each data file in the collection can also be further checked if the collection does not return how many or which qualified data files

OUTSOURCING ENCRYPTED FILE

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services that can be rapidly provisioned and released with minimal management effort or service provider interaction. The data owner will outsource the encrypted file to the cloud server, automatically three different keys will be generated for the file.

VERIFICATION OBJECT CONSTRUCTION

To maximize reduce storage and communication cost and achieve privacy guarantee of the verification objects. Trapdoor key, verification object key and decryption key is automatically constructed. The trapdoor key is basically differentiate the data owner and hacker

VERIFICATION OBJECT SIGNATURE AND AUTHENTICATION

When a query ends, the query results set and corresponding verification object are together returned to the query user, who verifies the correctness and completeness of query results based on the verification object. Our proposed query results verification scheme not only allows the query user to easily verify the correctness of each encrypted data file in the query results set, but also enables the data user to efficiently perform completeness verification before decrypting query results

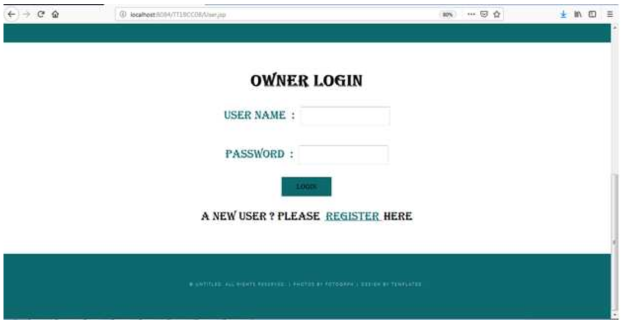
UNAUTHORIZED DATA ACCESS ALERT

When the cloud server or unauthorized person gains the access of the information or data which is stored by the user. The data user will get alert whenever anyone try to access the data or information. We can prevent from accessing the user information or data by verifying the verification object.

FILE RECOVERY

Data recovery is a process of salvaging (retrieving) inaccessible, lost, corrupted, damaged or formatted data from secondary storage, removable media or files, when the data stored in them cannot be accessed in a normal way. Even the hacker will access the data or even hacker does the tampering we can still recover the whole document.

RESULTS AND DISCUSSION



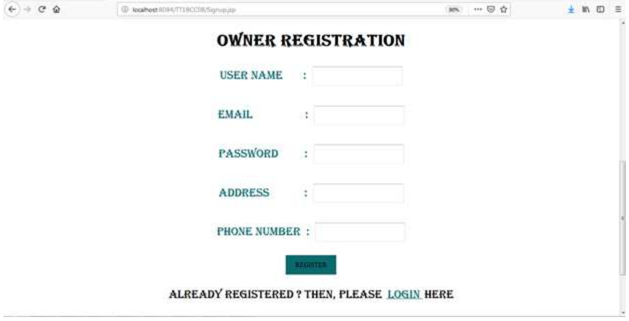
OWNER LOGIN

USER NAME :

PASSWORD :

A NEW USER ? PLEASE REGISTER HERE

OWNER REGISTRATION



OWNER REGISTRATION

USER NAME :

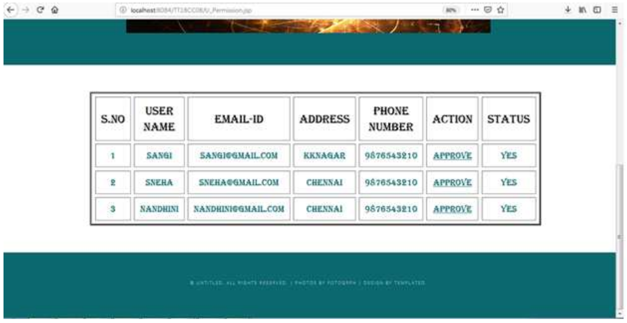
EMAIL :

PASSWORD :

ADDRESS :

PHONE NUMBER :

ALREADY REGISTERED ? THEN, PLEASE LOGIN HERE



S.NO	USER NAME	EMAIL-ID	ADDRESS	PHONE NUMBER	ACTION	STATUS
1	SANGI	SANGI@GMAIL.COM	KKNAGAR	9876543210	APPROVE	YES
2	SNEHA	SNEHA@GMAIL.COM	CHENNAI	9876543210	APPROVE	YES
3	NANDHINI	NANDHINI@GMAIL.COM	CHENNAI	9876543210	APPROVE	YES

Conclusion

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. Performance and accuracy experiments demonstrate the validity and efficiency of our proposed scheme.

FUTURE ENHANCEMENT

In future of outsource data -Search method is not efficient since the cloud needs to search through the whole database, which is very inefficient. In future we have some work in this line that will be enhancements for efficient verification for large-scale outsourced data. This system works on semi trusted cloud but in future it will be extended up to all types of cloud environment and can provide better security. Furthermore in future we can extend our search scheme to use external storage more carefully while maintaining privacy.

References

[1] N. Park and D. J. Lilja, "Characterizing datasets for data dedupli- cation in backup applications," in Proc. IEEE Int. Symp. Workload Characterization (IISWC), 2010, pp. 1–10.

[2] A. ODriscoll, J. Daugelaite, and R. D. Sleator, "Big data, hadoop and cloud computing in genomics," J. Biomed. Inform. vol. 46, no. 5, pp. 774–781, 2013.

[3] P. C. Zikopoulos, C. Eaton, D. DeRoos, T. Deutsch, and G. Lapis, Understanding Big Data. New York, NY, USA: McGraw-Hill, 2012.

[4] M. Dong, H. Li, K. Ota, and H. Zhu, "HVSTO: Efficient privacy preserv- ing hybrid storage in cloud data center," in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), 2014, pp. 529–534.

[5] J. Li, Y. K. Li, X. Chen, P. P. Lee, and W. Lou, "A hybrid cloud approach for secure authorized deduplication," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 5, pp. 1206–1216, May 2015.

[6] M. Dutch. (2008, Jun.). SNIA: Understanding Data De-Duplication Ratios [Online]. Available: Understanding_Data_De-duplication_Ratios-20080718.pdf

[7] M. Dong, H. Li, K. Ota, L. T. Yang, and H. Zhu, "Multicloud-based evacuation services for emergency management," IEEE Cloud Comput., vol. 1, no. 4, pp. 50–59, Nov. 2014.

[8] J. Long, A. Liu, M. Dong, and Z. Li, "An energy-efficient and sink- location privacy enhanced scheme for WSNS through ring based rout- ing," J. Parallel Distrib. Comput., vol. 81, pp. 47–65, 2015.

[9] M. Wen, R. Lu, K. Zhang, J. Lei, X. Liang, and X. Shen, "PaRQ: A privacy-preserving range query scheme over encrypted metering data for smart grid," IEEE Trans. Emerging Topics Comput., vol. 1, no. 1, pp. 178–191, Jun. 2013.