A SECURE SEARCHABLE ENCRYPTION FRAMEWORK FOR PRIVACY-CRITICAL CLOUD STORAGE SERVICES

JALLIPALLI SRI BHAVYA Student[CSE], SRI VANI EDUCATIONAL SOCIETY GROUP OF INSTITUTIONS, A.P., India.

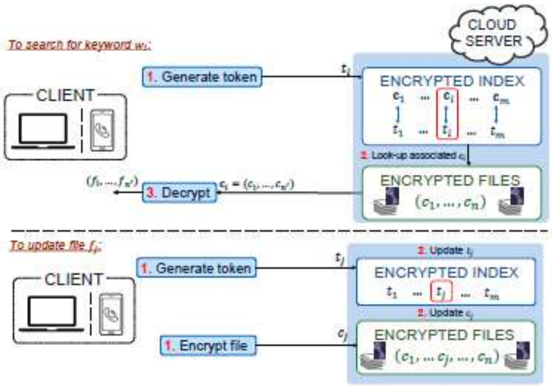
V.BABU RAO ASSISTANT PROFESSOR , Dept of CSE, SRI VANI EDUCATIONAL SOCIETY GROUP OF INSTITUTIONS, A.P., India.

ABSTRACT:

Searchable encryption has received a significant attention from the research community with various constructions being proposed, each achieving asymptotically optimal complexity for specific metrics (e.g., search, update). Despite their elegance, the recent attacks and deployment efforts have shown that the optimal asymptotic complexity might not always imply practical performance, especially if the application demands a high privacy. In this article, we introduce a novel Dynamic Searchable Symmetric Encryption (DSSE) framework called Incidence Matrix (IM)-DSSE, which achieves a high level of privacy, efficient search/update, and low client storage with actual deployments on real cloud settings. We harness an incidence matrix along with two hash tables to create an encrypted index, on which both search and update operations can be performed effectively with minimal information leakage. This simple set of data structures surprisingly offers a high level of DSSE security while achieving practical performance. Specifically, IM-DSSE achieves forward-privacy, backward-privacy and size-obliviousness simultaneously. We also create several DSSE variants, each offering different trade-offs that are suitable for different cloud applications and infrastructures. We fully implemented our framework and evaluated its performance on a real cloud system (Amazon EC2). We have released IM-DSSE as an open-source library for wide development and adaptation.

INTRODUCTION:

One of the most important cloud services is data Storage-as-a-Service (SaaS), which can significantly reduce the cost of data management via continuous service, expertise and maintenance for resource-limited clients such as individuals or small/medium businesses. Despite its benefits, SaaS also brings significant security and privacy concerns to the user. That is, once a client outsource his/her own data to the cloud, sensitive information (e.g., email) might be exploited by a malicious party (e.g., malware). Although standard encryption schemes such as Advanced Encryption Standard (AES) can provide confidentiality, they also prevent the client from querying encrypted data from the cloud. This privacy versus data utilization dilemma may significantly degrade the benefits and usability of cloud systems. Therefore, it is vital to develop privacy-enhancing technologies that can address this problem while retaining the practicality of the underlying cloud service. Searchable Symmetric Encryption (SSE) [1] enables a client to encrypt data in such a way that they can later perform keyword searches on it. These encrypted queries are performed via “search tokens” [2] over an encrypted index which represents the relationship between search token (keywords) and encrypted files. A prominent application of SSE is to enable privacy-preserving keyword search on the cloud (e.g., Amazon S3), where a data owner can outsource a collection of encrypted files and perform keyword searches on it without revealing the file and query contents [3].



Preliminary SSE schemes (e.g., [1], [4]) only provide searchonly functionality on static data (i.e., no dynamism), which strictly limits their applicability due to the lack of update capacity. Later, several Dynamic Searchable Symmetric Encryption (DSSE) schemes (e.g., [3], [5]) were proposed thatpermit the user to add and delete files after the system is set up. To the best of our knowledge, there is no single DSSE scheme that outperforms all the other alternatives in terms of all the aforementioned metrics: privacy (e.g., information leakage), performance (e.g., search, update delay), storage efficiency and functionality.

LITERATURE SURVEY

TITILE: Searchable symmetric encryption: improved definitions and efficient constructions.

AUTHOR: L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner.

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions.

TITLE: Practical dynamic searchable encryption with small leakage

AUTHOR: D. X. Song, D. Wagner, and A. Perrig.

Dynamic Searchable Symmetric Encryption (DSSE) enables a client to encrypt his document collection in a way that it is still searchable and efficiently updatable. However, all DSSE constructions that have been presented in the literature so far come with several problems: Either they leak a significant amount of information (e.g., hashes of the keywords contained in the updated document) or are inefficient in terms of space or search/update time (e.g., linear in the number of documents).

In this paper we revisit the DSSE problem. We propose the first DSSE scheme that achieves the best of both worlds, i.e., both small leakage and efficiency. In particular, our DSSE scheme leaks significantly less information than any other previous DSSE construction and supports both updates and searches in sublinear time in the worst case, maintaining at the same time a data structure of only linear size. We finally provide an implementation of our construction, showing its practical efficiency.

TITLE: Dynamic searchable symmetric encryption

AUTHOR: Z. Xia, X. Wang, X. Sun, and Q. Wang.

Dynamic Searchable Symmetric Encryption (DSSE) enables a client to perform keyword queries and update operations on the encrypted file collections. DSSE has several important applications such as privacy-preserving data outsourcing for computing clouds. In this paper, we developed a new DSSE scheme that achieves the highest privacy among all compared alternatives with low information leakage, efficient updates, compact client storage, low server storage for large file-keyword pairs with an easy design and implementation. Our scheme achieves these desirable properties with a very simple data structure (i.e., a bit matrix supported with two hash tables) that enables efficient yet secure search/update operations on it. We prove that our scheme is secure and showed that it is practical with large number of file-keyword pairs even with an implementation on simple hardware configurations.

PROPOSED APPROACH:

The existing multi-keyword search schemes can realize many multi-keyword search related functions such as conjunctive keyword search, disjunctive keyword search and subset search. Ballardetal. proposed two different conjunctive keyword search schemes, which only return the files containing all the searched keywords, on the basis of Shamir secret sharing and bilinear pairings, respectively. Their scheme is proven secure in the standard model. And disjunctive keyword search scheme was proposed in later, which can return files containing the subset of query keywords. Meanwhile predicate encryption schemes were also presented in order to support both conjunctive keyword search and disjunctive keyword search.

DIS-ADVANTAGES

1. The data owner has to rebuild the search index tree, which is time-consuming.
2. Traditional solutions have to suffer high computational costs.

PROPOSED SYSTEM:

We will propose a secure and effective multi-keyword ranked search scheme supporting update operations efficiently. The index tree based on Bloom filter will be designed to improve the search efficiency. And our scheme utilizes vector space model to build an index vector for every file in the outsourcing dataset. The cosine similarity measure is used to compute the similarity score of one file to the search query and TF×IDF weight will be used to improve the search accuracy.

Advantage

- ❖ Support dynamic operation properly and effectively.
- ❖ This scheme updates the lower computational cost.
- ❖ Supports dynamic operations that contain deletions or insertions in a document

MODULES DESCRIPTION:

- **Data Owner**

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the data file and then store in the cloud. The Data owner can have capable of manipulating the encrypted data file. And the data owner can set the access privilege to the encrypted data file.

- **Cloud Server**

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. It is responsible for authorizing all end users.

- **Key Distribution centre**

KDC who is trusted to store verification parameters and offer public query services for these parameters such as generating secret key based on the file and send to the corresponding end users. It is responsible for capturing the attackers.

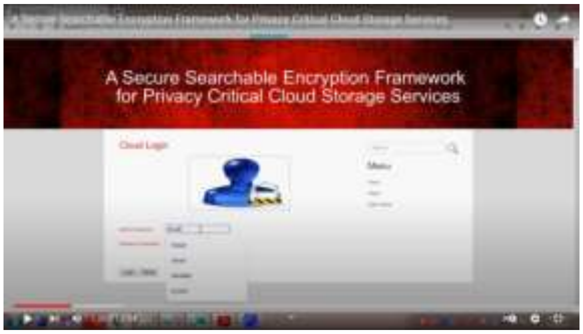
- **Data Consumer/End User**

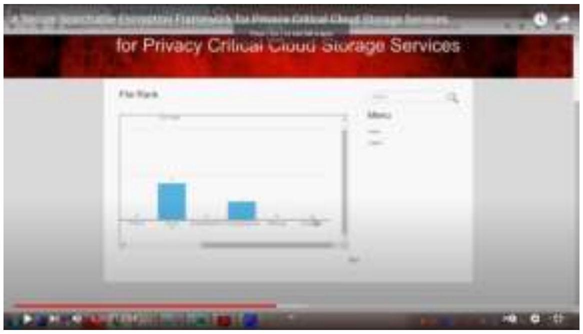
In this module, the user can only access the data file with the encrypted key if the user has the privilege to access the file. For the user level, all the privileges are given by the Data owner and the Data users are controlled by the data owner only. Users may try to access data files either within their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. He is sending request to KDC to generate secret key and KDC will generate the skey and send to corresponding end user.

- **Attacker (Unauthorized User)**

Attacker adds the malicious data to a block in cloud server. Then the Unauthorized user will considered as a attacker.

SAMPLE RESULTS


A Secure Searchable Encryption Framework for Privacy Critical Cloud Storage Services
Cloud Login
Menu



A Secure Searchable Encryption Framework for Privacy Critical Cloud Storage Services
A Secure Searchable Encryption Framework
for Privacy Critical Cloud Storage Services
Delete Files
Menu

CONCLUSION:

Our framework offers various DSSE constructions, which are specifically designed to meet the needs of cloud infrastructure and personal usage in different applications and environments. All of our schemes in IM-DSSE framework are proven to be secure and achieve the highest privacy among their counterparts. We conducted a detailed experimental analysis to evaluate the performance of our schemes on real Amazon EC2 cloud systems. Our results showed the high practicality of our framework, even when deployed on mobile devices with large datasets. We have released the full-fledged implementation of our framework for public use and analysis.

REFERENCES:

[1] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” in Proc. 13th ACM Conf. Comput. Commun. security, ser. CCS ’06. ACM, 2006, pp. 79–88.

[2] E. Stefanov, C. Papamanthou, and E. Shi, “Practical dynamic searchable encryption with small leakage,” in 21st Annu. Network and Distributed System Security Symp. — NDSS 2014. The Internet Soc., February 23-26, 2014.

[3] S. Kamara, C. Papamanthou, and T. Roeder, “Dynamic searchable symmetric encryption,” in Proc. 2012 ACM Conf. Comput. Commun. security. New York, NY, USA: ACM, 2012, pp. 965–976.

[4] D. X. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in Proc. 2000 IEEE Symp. Security and Privacy, 2000, pp. 44–55.

[5] D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawcyk, M.-C. Rosu, and M. Steiner, “Dynamic searchable encryption in very-large databases: Data structures and implementation,” in 21th Annu. Network Distributed System Security Symp. — NDSS 2014. The Internet Soc., February 23-26, 2014.

[6] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, “Privacy-preserving multi-keyword ranked search over encrypted cloud data,” IEEE Trans. Parallel Distributed Syst., vol. 25, no. 1, pp. 222–233, 2014.

[7] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, “Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking,” IEEE Trans. Parallel Distributed Syst., vol. 25, no. 11, pp. 3025–3035, 2014.

[8] S. Kamara and C. Papamanthou, “Parallel and dynamic searchable symmetric encryption,” in Financial Cryptography and Data Security (FC), ser. Lecture Notes in Comput. Sci. Springer Berlin Heidelberg, 2013, vol. 7859, pp. 258–274.

[9] M. Naveed, M. Prabhakaran, and C. A. Gunter, “Dynamic searchable encryption via blind storage,” in 35th IEEE Symp. Security Privacy, May 2014, pp. 48–62.

[10] S. Kamara and T. Moataz, “Boolean searchable symmetric encryption with worst-case sub-linear complexity,” EUROCRYPT 2017, 2017.