Journal of Engineering Sciences

Vol11,Issue2,FEB/2020
ISSN NO:0377-9254

PRIVILEGED ACCESS MANAGEMENT FOR CLOUD STORAGE

Dr.SYED SADAT ALI (M.Tech.,Ph.D)[1], SK.SUBHANI[2], K.REVATHI KRISHNA KUMARI[3], G.PRIYANKA[4], P.NAGA PAVANI[5]

[1]Associate Professor & H.O.D, Dept. of Computer Science & Engineering, LINGAYAS INSTITUTE OF MANAGEMENT AND TECHNOLOGY, A.P., India.

[2,3,4,5] Student, B. Tech (CSE), LINGAYAS INSTITUTE OF MANAGEMENT AND TECHNOLOGY, A.P., India.

ABSTRACT: The major feature of cloud computing is that it allows sharing and scalable deployment of services as needed by the users from any location. Cloud computing saves time and money during software up-gradation; cloud services are updated by the provider; so users are always working on the latest platform. 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.

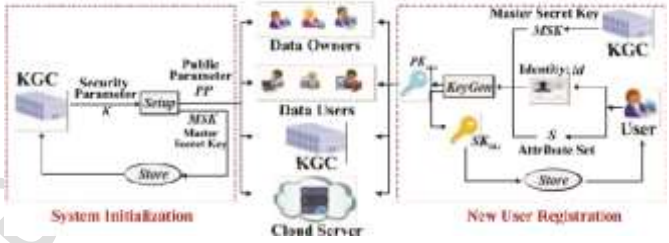
Keywords: Cloud Computing; Cloud Users; Cloud Providers; Security;

INTRODUCTION

Cloud Computing is the hottest topic in information technology(IT). However, it is not so much that the term „Cloud Computing" representsa host of new technologies, but rather that these technologies are combinedand effectively upgraded and enable new IT services and newbusiness models [1].The major feature of cloud computing is that it allows sharing and scalable deployment of services as needed by the users from any location. Cloud computing saves time and money during software up-gradation; cloud services are updated by the provider; so users are always working on the latest platform [2]. Cloud minimizes the amount of wasted computing resources and can also reduce energy consumption significantly. cloud computing becomes the most notable one, which provides convenient, on-demand services from a shared pool of configurable computing resources. Therefore, an increasing number of companies and individuals prefer to outsource their data storage to cloud server. Despite the tremendous economic and technical advantages,

unpredictable security and privacy concerns become the most prominent problem that hinders the widespread adoption of data storage in public cloud infrastructure. Encryption is a fundamental method to protect data privacy in remote storage .However, how to effectively execute keyword search for plaintext becomes difficult for encrypted data due to the unreadability of ciphertext. Searchable en-cryption provides mechanism to enable keyword search over encrypted data For the file sharing system, such as multi-owner multiuser scenario, fine-grained search authorization is a desirable function for the data owners to share their private data with other authorized user. However, most of the available systems require the user to perform a large amount of complex bilinear pairing operations. These overwhelmed computations become a heavy burden for user's terminal, which is especially serious for energy constrained devices. The outsourced decryption method allows user to recover the message with ultra lightweight decryption. However, the cloud server might return wrong half-decrypted information as a result of malicious attack or system malfunction. Thus, it is an important issue to guarantee the correctness of outsourced decryption in public key encryption with keyword search (PEKS) system. The authorized entities may illegally leak their secret key to a third party for profits. Suppose that a patient someday suddenly finds out that a secret key corresponding his electronic medical data is sold on e-Bay. Such despicable behavior seriously threatens the patient's data privacy. Even worse, if the private electronic health data that contain serious health disease is abused by the insurance company or the patient's employment corporation, the patient would be declined to renew the medical insurance or labor contracts. The intentional secret key leakage seriously undermines the foundation of authorized access control and data privacy protection. Thus, it is extremely urgent to identify the malicious user or even prove it in a court of justice.

in the following algorithms.



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.

Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries. We formally define SSE in this multi-user setting, and present an efficient construction.

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 METHOD

Searchable Symmetric Encryption (SSE) 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” over an encrypted dex 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 that permit 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. In the following, we first provide an overview on DSSE research and then, outline our research objectives and contributions toward addressing some of the limitations of the state-of-the-arts.

Proposed System:

Although a number of DSSE schemes have been introduced the literature, most of them only provide a theoretical asymptotic analysis1 and, in some cases, merely a prototyp implementation. The lack of experimental performanc evaluations on real platforms poses a significant difficulty I assessing the application and practicality of proposed DSS schemes, as the impacts of security vulnerability, hidden computation costs, multi-round communication delay and storage blowup might be overlooked. For instance, most efficient DSSE schemes (e.g., [5], [10]) are vulnerable to file-injection attacks, which have been shown to be easily conducted even by a semi-honest adversary in practice, especially in the personal email scenario. Although several forward-secure DSSE schemes with an optimal asymptotic complexity have been proposed, they incur either very high delay due to public-key operations (e.g., [11]), or significant storage blow-up at both client and server side (e.g., [2]), and therefore, their ability to meet actual need of real systems in practice is still unclear.

RELATED WORK

The rise of cloud storage and computing services provides vast benefits to the society and IT industry. 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. In the following, we first provide an overview on DSSE research and then, outline our research objectives and contributions toward addressing some of the limitations of the state-of-the-arts.

CONCLUSION

In this project analyse the Security is ensured by different parameter such as authentication, authorization, confidentiality, integrity and availability. Among these parameters, confidentiality and integrity should protect the data in cloud storage. Data stored in cloud storage is controlled and monitored by the cloud providers. To protect them, it is needed that an efficient confidentiality technique for cloud data storage. Thus, it is necessary to propose a new security mechanism to protect the outsourced data in public cloud storage environment.

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] F. Hahn and F. Kerschbaum, "Searchable encryption with secure and efficient updates," in Proc. 2014 ACM SIGSAC Conf. Comput. and Commun. Security. ACM, 2014, pp. 310–320.

[11] R. Bost, "Sophos – forward secure searchable encryption," in Proc. 2016 ACM Conf. Comput. Commun. Security. ACM, 2016.

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