RELIABLE AND RESEARCHABLE CRYPTOGRAPHY FRAMEWORK

[1] Mrs. B. Gouthami,[2] K. Lavanya,[3] J. Sindhu,[4] J. Raju,[5] K. Rama Krishna
[1] Assistant Professor,[2345] B.Tech Students
Department Of Computer Science & Engineering
Sri Indu College Of Engineering & Technology,Sheriguda, Ibrahimpatnam

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

I. INTRODUCTION

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 outsources 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

search only 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 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.

II. LITERATURE SURVEY

TITLE: Searchable symmetric encryption: improved definitions and efficient construction

AUTHORS: R. Curtmola, J. Garay,

ABSTRACT: 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 review existing security definitions, pointing out their short- comings, and propose two new stronger definitions which we prove equivalent. 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 ecient 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 ecient construction.

TITLE: Practical dynamic searchable encryption with small leakage

AUTHORS: S. Kamara, and R. Ostrovsk

ABSTRACT: 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 line.

TITLE: Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

AUTHORS: N. Cao, C. Wang, M. Li, K. Ren, and W. Lou

ABSTRACT: With the advent of cloud computing, data owners are motivated to outsource their complex data management systems from local sites to the commercial public cloud for great flexibility and economic savings. But for protecting data privacy, sensitive data have to be encrypted before outsourcing, which obsoletes traditional data utilization based on plaintext keyword search. Thus, enabling an encrypted cloud data search service is of paramount importance. Considering the large number of data users and documents in the cloud, it is

necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. In this paper, for the first time, we define and solve the challenging problem of privacy-preserving multi-keyword ranked search over encrypted data in cloud computing (MRSE). We establish a set of strict privacy requirements for such a secure cloud data utilization system. Among various multi-keyword semantics, we choose the efficient similarity measure of "coordinate matching," i.e., as many matches as possible, to capture the relevance of data documents to the search query. We further use "inner product similarity" to quantitatively evaluate such similarity measure. We first propose a basic idea for the MRSE based on secure inner product computation, and then give two significantly improved MRSE schemes to achieve various stringent privacy requirements in two different threat models. To improve search experience of the data search service, we further extend these two schemes to support more search semantics. Thorough analysis investigating privacy and efficiency guarantees of proposed schemes is given. Experiments on the real- world data set further show proposed schemes indeed introduce low overhead on computation and communication.

TITLE: Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking

AUTHORS: W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li

ABSTRACT: With the growing popularity of cloud computing, huge amount of documents are outsourced to the cloud for reduced management cost.

III. SYSTEM ANALYSIS

EXISTING SYSTEM

Lai et al. modeled the relationship between keywords and files in DSSE as bipartite graphs. The authors also proposed a novel data structure called cascaded triangles, which offers parallelism and efficient update (add/delete). Kim et al. leveraged two hash tables to integrate forward index and inverted index together in the form of encrypted index, which offers efficient update with direct deletion. Bost et al. proposed some (single-keyword) DSSE schemes that achieve both forward-privacy and backward-privacy with optimal asymptotic complexity using asymmetric primitives.

DISADVANTAGES

- 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.
- Most of the existing system only provide a theoretical asymptotic analysis and, in some cases, merely a prototype implementation.
- The lack of experimental performance evaluations on real platforms poses a significant difficulty in assessing the application and practicality of proposed DSSE schemes, as the impacts of security vulnerability, hidden computation costs, multi-round communication delay and storage blowup might be overlooked.
- Most efficient DSSE schemes 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, or significant storage blow-up at both client and server side and therefore, their ability to meet actual need of real systems in practice is still unclear.

PROPOSED SYSTEM

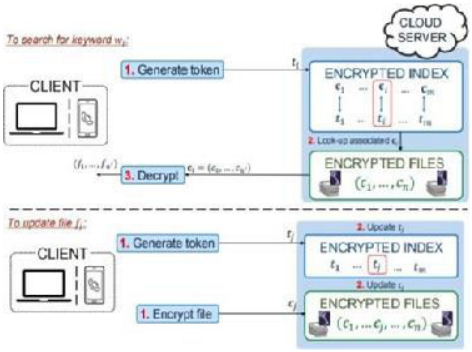
In this project, towards filling the gaps between theory and practice in DSSE research community, we introduce IM-DSSE, a fully-implemented Incidence Matrix-based DSSE framework which favors desirable properties for realistic privacy-critical cloud systems including high security against practical attacks and low end-to-end delay.

In this framework, we provide the full-fledged implementation of our preliminary DSSE scheme proposed, as well as extended schemes, which are specially designed to meet various application requirements and cloud data storage as- a-service infrastructures in practice.

ADVANTAGES

- Highly secure against File-Injection Attacks
- Updates with Improved Features
- Fully Parallelizable

SYSTEM ARCHITECTURE



IV. IMPLEMENTATION

MODULES

1. Data User
2. Data Owner
3. Cloud

MODULE DESCRIPTION

DATA USER

The user is one of the module, here the user should register with the application and should authorized by the cloud then only the user can able to search for the file, if you find the file then you should get the decryption key to view the file . To get the decryption key, the user should request for that key to the cloud .after getting the decrypt key from the cloud the user can view the decrypted file and if the user want to download the file here also the user should get the file token from the owner, after verifying file token the user can able to download the file.

DATA OWNER

Here the data owner is the module, the data owner should register with our application and the owner can perform the following action such as upload the file into the clouds, view uploaded files and the owner can able to check his transaction and the owner give the token to the user.

CLOUD

The cloud is module who manage everything about the project like authorizing the users and authoring the owner, view decrypt key request, view uploaded files, view secure data details, view file attackers and view transactions.

SCREENSHOTS

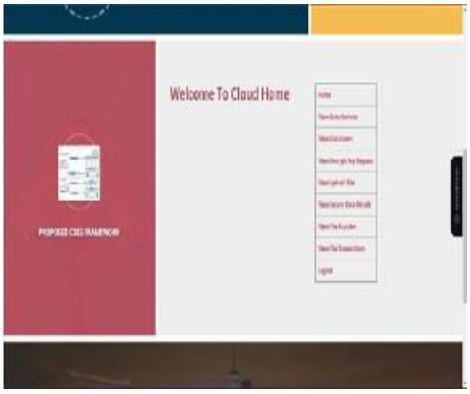


Fig 1 : Project Home Page

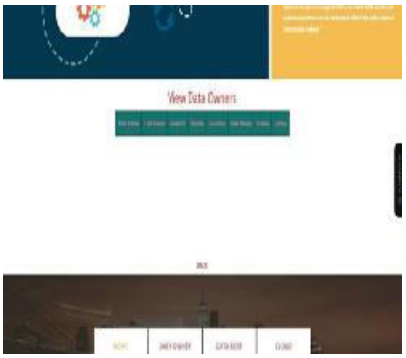


Fig 2 : View Data Owners Page

Fig 4 : View Decrypt Key Request Status

Fig 5 : View Uploaded Files

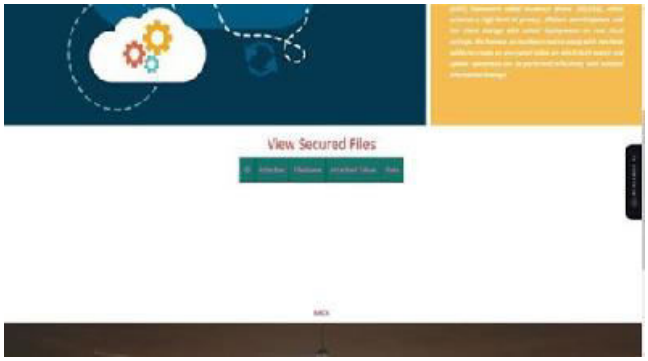


Fig 6 : View Secured Files Page

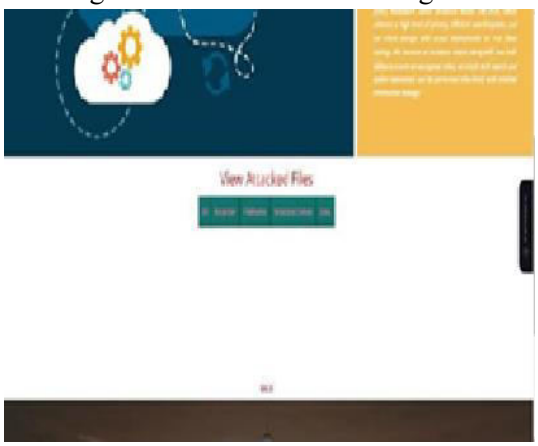


Fig 7 : View Attacked Files Page

Fig 8 : View all Transactions Page

Fig 9 : Data Owner Login

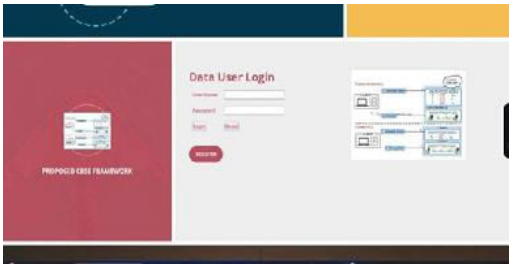


Fig 10 : Data User Login Screen

VI CONCLUSION

In this article, we presented IM-DSSE, a new DSSE framework which offers very high privacy, efficient updates, low search latency simultaneously. Our constructions rely on a simple yet efficient incidence matrix data structure in combination with two hash tables that allow efficient and secure search and update operations. 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.

FUTURE SCOPE

The future scope for the project "RELIABLE AND RESEARCHABLE CRYPTOGRAPHY FRAMEWORK" is vast and promising, given the increasing significance of data security and privacy in our digital age. This framework can be pivotal in enhancing the robustness and transparency of cryptographic systems. It can serve as a foundation for developing more secure communication protocols, protecting sensitive information across various sectors such as finance, healthcare, and government. Additionally, the framework's researchable aspect opens avenues for continuous improvement and innovation, fostering academic and practical advancements in cryptography. This project could also play a crucial role in addressing emerging threats posed by quantum computing, ensuring that cryptographic methods evolve to meet future security challenges. Moreover, the framework can facilitate standardized practices in cryptographic implementations, promoting interoperability and trust in digital systems globally.

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.
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. 25.
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. 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.
13. D. Cash, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner, "Highly- scalable searchable symmetric encryption with support for boolean queries," in Advances in Cryptology, CRYPTO 2013, ser. Lecture Notes in Comput. Sci., vol. 8042, 2013, pp. 353–373.
14. Z. Fu, X. Wu, C. Guan, X. Sun, and K. Ren, "Toward efficient multi-keyword fuzzy search over encrypted outsourced data with accuracy improvement," IEEE Trans. Inform. Forensics Security, vol. 11, no. 12, pp. 2706–2716, 2016.
15. Q. Wang, M. He, M. Du, S. S. Chow, R. W. Lai, and Q. Zou, "Searchable encryption over feature-rich data," IEEE Trans. Dependable Secure Computing, 2016.