Framework for Secure Searchable Encryption for Flexible Data Sharing in Cloud Storage Services

Mr.M.Dhamodaran M.E., A. Avinash, A. Anbalagan, S. Hariharan

[1]Assistant Professor and Head, [2]Student

Department of Information Technology, Muthayammal Engineering College (Autonomous),
Rasipuram - 637 408, Tamil Nadu, India

Article Info
Volume 8, Issue 7
Page Number: 76-80

Publication Issue :
May-June-2022

Article History
Accepted: 01June2022
Published: 20June2022

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.

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, 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 might be exploited by a malicious party.

Although standard encryption schemes such as Advanced Encryption Standard can provide confidentiality, they also prevent the client from querying encrypted data from the cloud.

Cloud 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. Proxy re-encryption could be useful to address the dilemma for sharing encrypted data.

II. PUBLIC-KEY OPERATIONS

Although a number of DSSE schemes have been introduced in the literature, most of them only provide a theoretical asymptotic analysis1 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.

For instance, 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.

There is a significant need for a DSSE scheme that can achieve a high level of security with a well quantified information leakage, while maintaining a performance and functionality balance between the search and update operations.

More importantly, it is critical that the performance of proposed DSSE should be experimentally evaluated in a realistic cloud environment with various parameter settings, rather than merely relying on asymptotic results.

The investigation of alternative data structures and their optimized implementations on commodity hardware seem to be the key factors towards achieving these objectives.

SECURE SEARCHABLE ENCRYPTION

With the rapid development of cloud computing, cloud storage has enabled the provision of high data availability, easy access to data, and reduced infrastructure costs from outsourcing of data to remote servers. Many users prefer cloud storage services to relieve the burden of maintenance costs as well as the overhead of storing data locally. Moreover, users are able to access their data from anywhere and at any time instead of having to use dedicated machines.

FORWARD-PRIVATE DSSE SCHEMES

The proposed a DSSE scheme, which leaked less information than that of and it was parallelizable. Recently, a series of new DSSE schemes have been proposed which offer various trade-offs between security, functionality and efficiency properties such as small leakage, scalable searches with extended query types ,or high efficiency .

Inspired by the work from,. in proposed a new sublinear DSSE scheme which supports more complex queries such as disjunctive and Boolean queries.

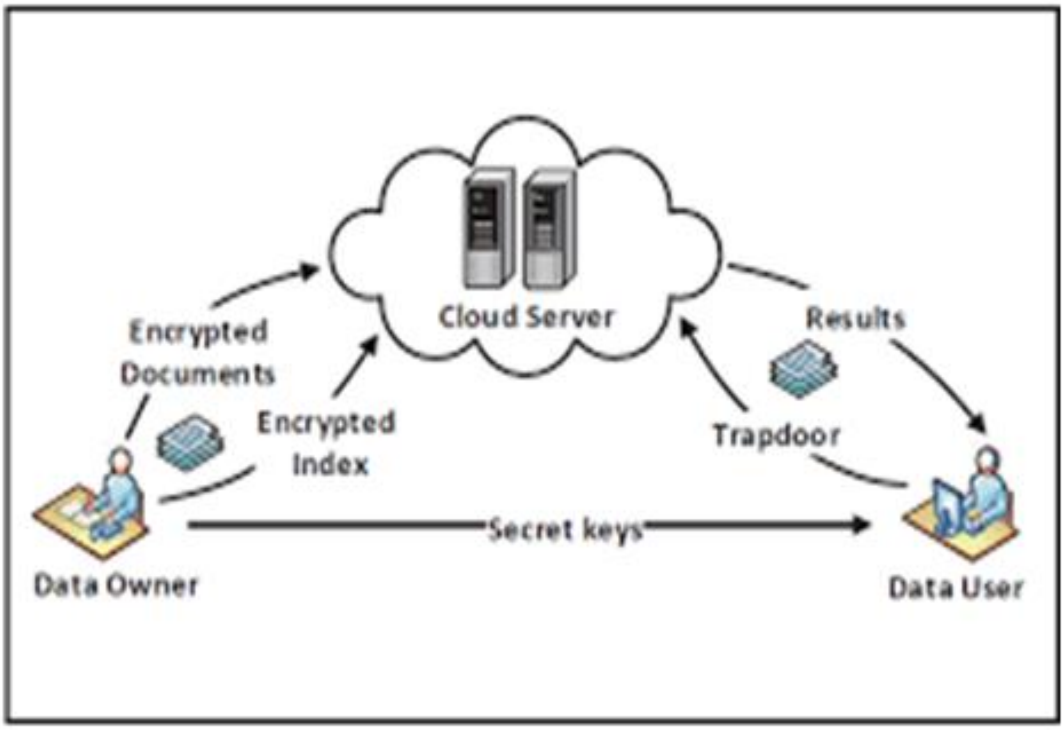
III. PROPOSED SYSTEM

In this paper, Despite a number of DSSE schemes have been introduced in the literature, most of them only provide a the oretical a symptotic analysis and in some cases, merely a prototype implementation. The lack of a rigorous actual experimental performance evaluation on real platforms poses a signcant diculty 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. 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.

ADVANTAGES

- The highly practical and mostly dominated by the clientserver communication opportunities for broad adaptation and testing

IV. SYSTEM ARCHITECTURE



MODULES

- Data owner to Share the data
- Data user to deploy the data
- Cloud server

V. MODULES DESCRIPTION

DATA OWNER TO SHARE THE DATA

Data owner register their own details. Login their account. Upload the files to cloud in encrypted format by using DSSE.At the time of file uploading we calculate(TF/IDF) term frequency and pre processing(stemming,stopwords) for every files. For key generation (Private and Trapdoor key) we are using random key generator and bloom filter technics. Owner can view all files uploaded by own and download the file. Data owner logout their account.

DATA USER TO DEPLOY THE DATA

Data user registers their own details. user login their account. User can search the files by using keyword and k-value. User can send the request for secret key to cloud for download the files in decrypt format. Using private and trapdoor key users can download the files. Data user logout their account.

CLOUD SERVER

- Cloud server login their account. View data owner and data user details. accept the user key request and send the key user' s registered mail.

Finally graph will show based on between number of files and rank of those files, between number of files and request count of those files. Cloud server logout their account.

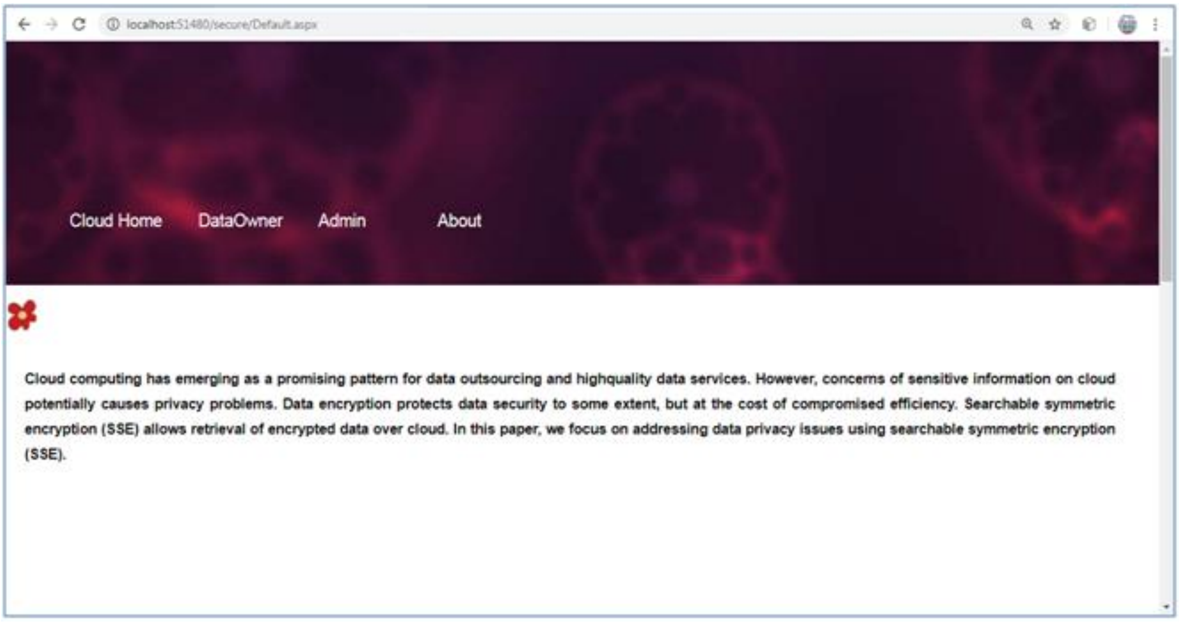
VI. CONCLUSION

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

VII. FUTURE ENHANCEMENT

Future work will focus on experiments with. 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. This model is exported with a low-level API allowing clients to implement new access protocols and to add them to the system on-line. The API has been validated with an implementation of the file system interface. The critical factor for meeting the design targets has been the selection of proper data organization based on redundant chains of data containers. We present this organization in detail and describe how it is used to deliver required data services.

VIII. RESULTS



Cloud computing has emerging as a promising pattern for data outsourcing and highquality data services. However, concerns of sensitive information on cloud potentially causes privacy problems. Data encryption protects data security to some extent, but at the cost of compromised efficiency. Searchable symmetric encryption (SSE) allows retrieval of encrypted data over cloud. In this paper, we focus on addressing data privacy issues using searchable symmetric encryption (SSE).

IX. REFERENCES

[1]. Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin, and H. Wang, "Privacypreserving cloud-based road condition monitoring with source authentication in vanets," IEEE Trans. Information Forensics and Security, vol. 14, no. 7, pp. 17791790, 2019.

[2]. H. Yin, Z. Qin, J. Zhang, L. Ou, F. Li, and K. Li, "Secure conjunctive multi-keyword ranked search over encrypted cloud data for multiple data owners," Future Generation Computer Systems, vol. 100, pp. 689700, 2019.

[3]. http://www.healthvault.com. cloud-based road condition monitoring with source authentication in vanets," IEEE Trans. Information

[4]. https://www.google.com/health.

[5]. M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in EUROCRYPT 1998. Springer Berlin Heidelberg, 1998, pp. 127144.

[6]. M. Green and G. Ateniese, "Identity-based proxy re-encryption," in ACNS 2007. Springer Berlin Heidelberg, 2007, pp. 288306.

[7]. H. Deng, Z. Qin, Q. Wu, Z. Guan, R. H. Deng, Y. Wang, and Y. Zhou, "Identity-based encryption transformation for flexible sharing of encrypted data in public cloud," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 31683180, 2020.

[8]. S. Yin, H. Li, and L. Teng, "A novel proxy re-encryption scheme based on identity property and stateless broadcast encryption under cloud environment," International Journal of Network Security, vol. 21, no. 5, pp. 797803, 2019.

[9]. P. Xu, T. Jiao, Q. Wu, W. Wang, and H. Jin, "Conditional identity-based broadcast proxy re-encryption and its application to cloud email," IEEE Transactions on Computers, vol. 65, no. 1, pp. 6679, 2015.