International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

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

M.Dhamodaran[1],A.Anbalagan[2],A.Avinash[3],S.Hariharan[4],

[1]AssistantProfessor,[2,3,4,]Student(B.TECH)
Department of Information Technology, Muthayammal Engineering College(Autonomous) ,Rasipuram,Tamil Nadu, India.
chocolateanbu143@gmail.com,soloavi143@gmail.com,hariharanmass11@gmail.com.dhamu2k@gmail.com.

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

Keywords: Distance Measurement, Indoor Navigation, Particle Filter, Ultrasonic Transducers.

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.

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.

LITERATUREREVIEW

According to research journal “Framework for Secure Searchable Encryption for Flexible Data Sharing in Cloud Storage Services”Shoulin Yin, Hang Li-2019 public key that can reduce the processA Secure Fine-Grained Micro-Video Subscribing System in Cloud Computing CHUNPENG GE-2019 vulnerability in the cloud and the hardware computing

PROPOSEDSYSTEM:

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 signcantdiculty 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.

5.ALGORITHM

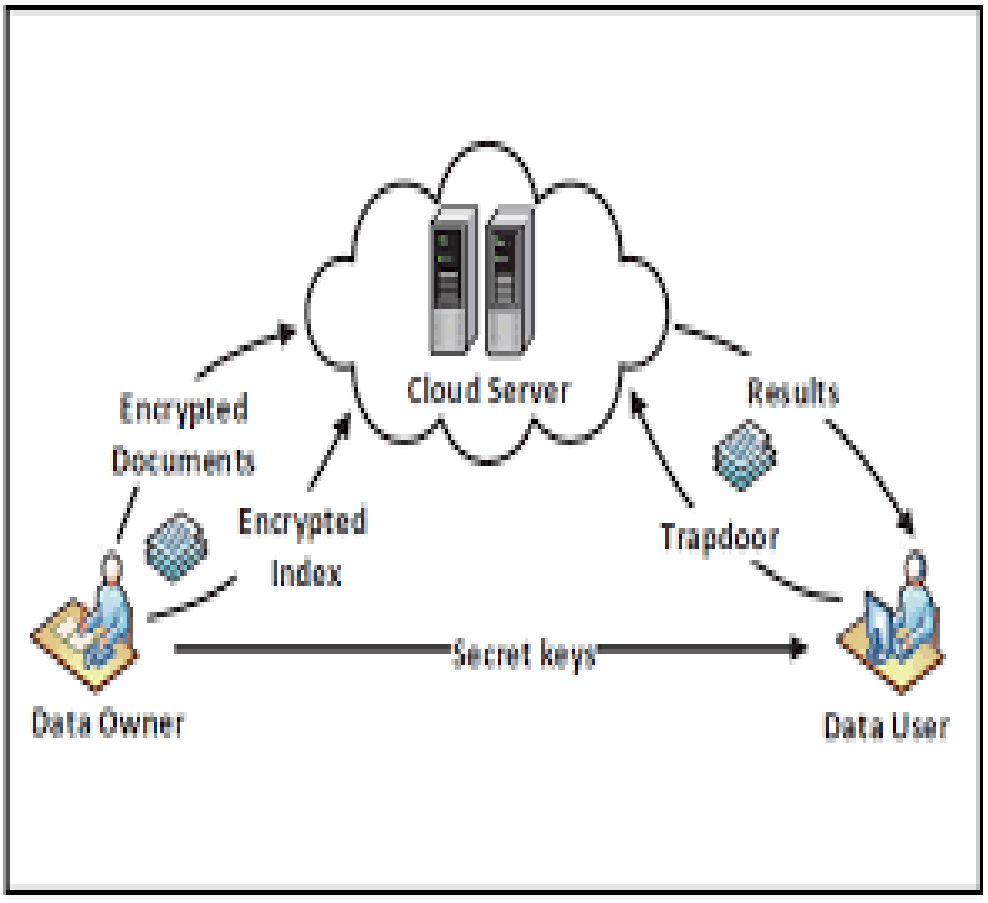
Incidence Matrix -dynamic searchable symmetric encryption

- 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 sizeobliviousness simultaneousl

ADVANTAGES:

- It is suitable for different cloud applications and infrastructures.
- The more efficient searchable technique
- Backup service and security.
- Data privacy and combating unsolicited accesse

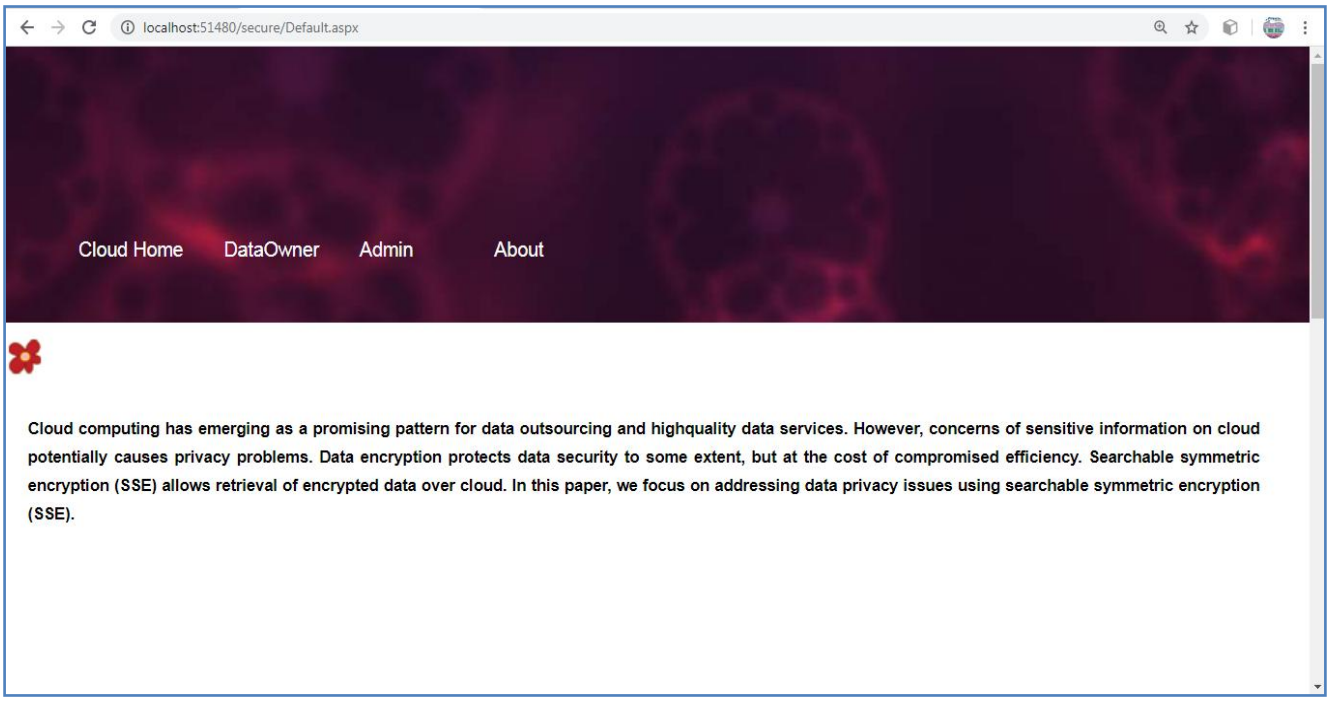
SYSTEMARCHITECTURE:



HARDWARE REQUIREMENTS

• System	:	Pentium Dual Core
• HardDisk	:	120 GB
• RAM	:	1 GB
• Monitor	:	15 " LED
• Input devices	:	Keyboard,Mouse

1. RESULT



IMPLEMENTATION

• 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.

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 .

BIBLIOGRAPHY

[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. 1779– 1790, 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. 689– 700, 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.