Journal of
Sensor and
Actuator Networks

Article

Fast Multi-User Searchable Encryption with Forward and Backward Private Access Control

Salim Sabah Bulbul [1], Zaid Ameen Abduljabbar [2,*], Duaa Fadhel Najem [3], Vincent Omollo Nyangaresi [4], Junchao Ma [5,*] and Abdulla J. Y. Aldarwish [2]

[1] Directorate General of Education Basra, Ministry of Education, Basra 61004, Iraq; pgs2185@uobasrah.edu.iq
[2] Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
[3] Department of Cyber Security, College of Computer Science and Information Technology, University of Basrah, Basrah 61004, Iraq
[4] Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo 40601, Kenya
[5] College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
* Correspondence: zaid.ameen@uobasrah.edu.iq (Z.A.A.); majunchao@sztu.edu.cn (J.M.)

Abstract: Untrusted servers are servers or storage entities lacking complete trust from the data owner or users. This characterization implies that the server hosting encrypted data may not enjoy full trust from data owners or users, stemming from apprehensions related to potential security breaches, unauthorized access, or other security risks. The security of searchable encryption has been put into question by several recent attacks. Currently, users can search for encrypted documents on untrusted cloud servers using searchable symmetric encryption (SSE). This study delves deeply into two pivotal concepts of privacy within dynamic searchable symmetric encryption (DSSE) schemes: forward privacy and backward privacy. The former serves as a safeguard against the linkage of recently added documents to previously conducted search queries, whereas the latter guarantees the irretrievability of deleted documents in subsequent search inquiries. However, the provision of fine-grained access control is complex in existing multi-user SSE schemes. SSE schemes may also incur high computation costs due to the need for fine-grained access control, and it is essential to support document updates and forward privacy. In response to these issues, this paper suggests a searchable encryption scheme that uses simple primitive tools. We present a multi-user SSE scheme that efficiently controls access to dynamically encrypted documents to resolve these issues, using an innovative approach that readily enhances previous findings. Rather than employing asymmetric encryption as in comparable systems, we harness low-complexity primitive encryption tools and inverted index-based DSSE to handle retrieving encrypted files, resulting in a notably faster system. Furthermore, we ensure heightened security by refreshing the encryption key after each search, meaning that users are unable to conduct subsequent searches with the same key and must obtain a fresh key from the data owner. An experimental evaluation shows that our scheme achieves forward and Type II backward privacy and has much faster search performance than other schemes. Our scheme can be considered secure, as proven in a random oracle model.

Keywords: symmetric encryption; cloud computing; access control; multiple user; backward privacy

check for updates

Citation: Bulbul, S.S.; Abduljabbar, Z.A.; Najem, D.F.; Nyangaresi, V.O.; Ma, J.; Aldarwish, A.J.Y. Fast Multi-User Searchable Encryption with Forward and Backward Private Access Control. *J. Sens. Actuator Netw.* **2024**, *13*, 12. https://doi.org/10.3390/jsan13010012

Academic Editors: Donald Elmazi, Elis Kulla and Hakima Chaouchi

Received: 7 December 2023
Revised: 10 January 2024
Accepted: 18 January 2024
Published: 2 February 2024

1. Introduction

Following the rapid emergence of cloud computing, individuals and enterprises can now outsource storage and computation to the cloud [1–3]. The encryption of outsourced data before uploading to the cloud can prevent privacy leaks; however, data availability will be reduced if traditional encryption is used, as querying outsourced data is impossible in this case [4].