PLOS ONE

RESEARCH ARTICLE

# A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client

**Salim Sabah Bulbul[1], Zaid Ameen Abduljabbar[2], Rana Jassim Mohammed[2], Mustafa A. Al Sibahee[3,4]*, Junchao Ma[5]*, Vincent Omollo Nyangaresi[6,7], Iman Qays Abduljaleel[8]**

**1** Directorate General of Education Basra, Ministry of Education, Basra, Iraq, **2** Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah, Iraq, **3** National Engineering Laboratory for Big Data System Computing Technology, Shenzhen University, Shenzhen, PR China, **4** Computer Technology Engineering Department, Iraq University College, Basrah, Iraq, **5** College of Big Data and Internet, Shenzhen Technology University, Shenzhen, China, **6** Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science & Technology, Bondo, Kenya, **7** Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai, Tamil Nadu, India, **8** Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq

* majunchao@sztu.edu.cn (JM); mustafaalsibahee@szu.edu.cn (MAAS)





**Citation:** Bulbul SS, Abduljabbar ZA, Mohammed RJ, Al Sibahee MA, Ma J, Nyangaresi VO, et al. (2024) A provably lightweight and secure DSSE scheme, with a constant storage cost for a smart device client. PLoS ONE 19(4): e0301277. https://doi.org/10.1371/journal.pone.0301277

**Editor:** Sathishkumar Veerappampalayam Easwaramoorthy, Sunway University, MALAYSIA

**Received:** November 4, 2023

**Accepted:** March 13, 2024

**Published:** April 25, 2024



**Data Availability Statement:** The data underlying the results presented in the study are available from (https://www.kaggle.com/datasets/wcukierski/enron-email-dataset).

**Funding:** This work is supported by the Natural Science Foundation of Top Talent of SZTU (to M. Li); grant no.GDRC202132.

**Competing interests:** The authors have declared that no competing interests exist

## Abstract

Outsourcing data to remote cloud providers is becoming increasingly popular amongst organizations and individuals. A semi-trusted server uses Searchable Symmetric Encryption (SSE) to keep the search information under acceptable leakage levels whilst searching an encrypted database. A dynamic SSE (DSSE) scheme enables the adding and removing of documents by performing update queries, where some information is leaked to the server each time a record is added or removed. The complexity of structures and cryptographic primitives in most existing DSSE schemes makes them inefficient, in terms of storage, and query requests generate overhead costs on the Smart Device Client (SDC) side. Achieving constant storage cost for SDCs enhances the viability, efficiency, and easy user experience of smart devices, promoting their widespread adoption in various applications while upholding robust privacy and security standards. DSSE schemes must address two important privacy requirements: forward and backward privacy. Due to the increasing number of keywords, the cost of storage on the client side is also increasing at a linear rate. This article introduces an innovative, secure, and lightweight Dynamic Searchable Symmetric Encryption (DSSE) scheme, ensuring Type-II backward and forward privacy without incurring ongoing storage costs and high-cost query generation for the SDC. The proposed scheme, based on an inverted index structure, merges the hash table with linked nodes, linking encrypted keywords in all hash tables. Achieving a one-time O(1) storage cost without keyword counters on the SDC side, the scheme enhances security by generating a fresh key for each update. Experimental results show low-cost query generation on the SDC side (6,460 nanoseconds), making it compatible with resource-limited devices. The scheme outperforms existing ones, reducing server-side search costs significantly.