IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

Privacy-Preserving Searchable Encryption with Access Control Using Secret Sharing for Secure Cloud Data Outsourcing

P. Dinesh[1], S. Dhineshkumar[2], B. Gowtham[3], T. Kalaiselvan[4]
Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2-4]
Anjalai Ammal Mahalingam Engineering College, Thiruvarur, Tamilnadu, India

Abstract: *Searchable encryption allows users to perform search operations on encrypted data without revealing its content. While many existing methods use public key and symmetric key encryption, public key approaches often involve high computational costs, making them less suitable for large databases in cloud environments. To overcome this issue, this paper proposes a privacy-preserving searchable encryption method based on secret sharing, known for its lower computational complexity. Secret sharing divides confidential data into multiple independent shares, improving both security and efficiency. Previous work introduced a searchable encryption method using secret sharing but did not support user access control. In this study, we present a searchable encryption framework with integrated user access control, using a (k, n) threshold secret sharing scheme. In the proposed system, each data item stored in the cloud has an owner, who can control access permissions for different users. A client-server model is used to perform secure computations between the data owner, authorized users, and $n \geq k$ cloud servers. We analyze the security of our system in terms of data distribution, query generation, and search processes, proving its resistance to honest-but-curious adversaries with knowledge of up to $k - 1$ servers. Additionally, we propose an improved method using an (n, n) additive secret sharing scheme for cases where $n = k$. The performance of the proposed methods is evaluated using Python, with comparisons made against existing secret sharing-based searchable encryption schemes. Results show that our approach offers better computational and communication efficiency while maintaining strong security guarantees.*

Keywords: Searchable Encryption, Secret Sharing, Access Control, Cloud Data Outsourcing, (k, n) Threshold Scheme, Additive Secret Sharing, Secure Computation, Honest-but-Curious Adversary, Privacy Preservation

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-26053