IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, November 2024

Efficient Access Control for Cloud-Based User Data Storage and Sharing

SK. Pujitha[1], Chintala Harish[2], Ganesh Gangishetty[3], Chimmula Shruthi Reddy[4], Arpan Butti[5]
Assistant Professor, Department of CSE[1]
Students, Department of CSE[2,3,4,5]
Guru Nanak Institute of Technology, Hyderabad, Telangana, India

Abstract: *Cloud computing provides flexible data management and ubiquitous data access. However, the storage service provided by cloud server is not fully trusted by customers. Searchable encryption could simultaneously provide the functions of confidentiality protection and privacy-preserving data retrieval, which is a vital tool for secure storage. In this paper, we propose an efficient large universe regular language searchable encryption scheme for the cloud, which is privacy-preserving and secure against the off-line keyword guessing attack (KGA). A notable highlight of the proposal over other existing schemes is that it supports the regular language encryption and deterministic finite automata (DFA) based data retrieval. The large universe construction ensures the extend ability of the system, in which the symbol set does not need to be predefined. Multiple users are supported in the system, and the user could generate a DFA token using his own private key without interacting with the key generation center. Furthermore, the concrete scheme is efficient and formally proved secure in standard model. Extensive comparison and simulation show that this scheme has function and performance superior than other schemes*

Keywords: Cloud Computing, Searchable Encryption, Privacy-Preserving, Deterministic Finite Automata (DFA), Keyword Guessing Attack (KGA).