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, September 2024

Matching Free Open Key Checked Encryption With Articulation Search

V. Poojitha[1], V. Shiva Kumar[2], Shivansh[3], Dr. Rishi Sayal[4]
CSE, Guru Nanak Institutions Technical Campus, Hyderabad, Telangana, India[1,2,3,4]
vaiadalapoojitha69@gmail.com[1], vilasagarapushivakumar@gmail.com[2]
bandralshivansh5@gmail.com[3], ad.rs@gniindia.org[4]

Abstract: *The Industrial Internet of Things (IIOT) demands robust encryption solutions for cloud-based data storage to uphold user privacy. Existing Public Key Encryption with Keyword Search (PEKS) systems suffer from vulnerabilities like Inside Keyword Guessing Attacks (IKGA) and operational hurdles such as certificate management and key escrow. To address these challenges, this paper proposes a novel Certificateless Public Key Authenticated Encryption with Keyword Search (CLPEKS) scheme.By eliminating costly bilinear pairings, our approach enhances computational efficiency while mitigating IKGA vulnerabilities and circumventing certificate management and key escrow issues. Validation within the random oracle model demonstrates improved computational efficiency, reduced communication overhead, and enhanced security properties. Furthermore, our scheme introduces salted trapdoors and conceals keyword search frequencies to fortify data privacy for resource-constrained IIOT devices. Additionally, it empowers data owners to encrypt keywords and verify data user identities, thereby reinforcing overall cloud security.*

Keywords: Public Key Encryption with Keyword Search (PEKS), Inside Keyword Attack (IKGA), Key escrow, Trapdoor ,cloud security