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 5, June 2025
Impact Factor: 7.67

Secure Data Transfer in Cloud Computing Using the Elliptic Curve Diffie–Hellman (ECDH) Algorithm

Mr. Pradeep Nayak*[1], Lohit M Patgar*[2], Farhan*[3], Pranam*[4], Ravikumar*[5]
Department of Information Science and Engineering[1-5]
Alva's Institute of Engineering and Technology, Mijar, Karnataka, India-

Abstract: *Cloud computing provides flexible and scalable data storage and processing, but ensuring secure data transfer remains a critical challenge. Traditional RSA-based cryptographic key exchange systems, while reliable, are increasingly burdened by lengthy key generation times and large key sizes. Elliptic Curve Diffie–Hellman (ECDH) has emerged as a powerful alternative, offering equivalent security with smaller key sizes, lower computational overhead, and substantially faster execution—often 10× faster in shared-secret calculations and ~60× faster in key generation compared to RSA kumarasenau.medium.com.Comparative benchmarks showing ECDH-based schemes outperform RSA counterparts in encryption latency and resource use .Hybrid encryption frameworks (e.g., ChaCha20+ECDH) achieving 2 ms encryption time and 15.8 ms key generation, far surpassing RSA/AES and Blowfish/ECC alternatives researchgate.net.We also evaluate curve selection strategies, security enhancements like perfect forward secrecy, public key validation, and the integration of ECDH with advanced symmetric encryption in large-scale cloud environments. Finally, we explore future directions involving post-quantum integration and blockchain-based integrity mechanisms, making a compelling case for ECDH as a modern, efficient, and secure protocol for protecting cloud data in transit*

Keywords: *Cloud computing*

DOI: 10.48175/568