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: 7.301
Volume 3, Issue 2, July 2023

Strengthening Cloud Security: A Comprehensive Review of Modern Cryptography Methods and Emerging Trends

Saifuddin Ansari
Student, Department of Masters of Computer Applications
Late Bhausaheb Hiray S.S Trust's Hiray Institute of Computer Application, Mumbai, India
ansarisaifuddin9325@gmail.com

Abstract: *To protect data and communication in cloud environments, this article examines the foundations, methods, and protocols of cryptography in the context of cloud computing. Asymmetric and symmetric key cryptography is introduced, with a focus on the difficulties in key distribution and the significance of strong cryptographic algorithms. The paper discusses several cloud cryptography strategies, demonstrating their value in enabling safe data sharing and compute outsourcing while maintaining secrecy. These techniques covered include homomorphic encryption, proxy re-encryption, attribute-based encryption, and searchable encryption. The relevance of cryptographic protocols for cloud security in terms of authentication, access control, and data sharing is examined. Examples include SSL/TLS for secure communication and KMIP for key management. Furthermore, the paper highlights privacy-preserving computation techniques and the usage of cryptographic standards and frameworks provided by NIST, CSA, and TCG in ensuring secure cryptographic practices. The paper concludes by addressing current challenges and future directions, including performance optimization, trust in cloud providers, and post-quantum cryptography, to enhance the security of data in cloud computing.*

Keywords: Cryptography, Cloud computing, Data, Security, Key, Algorithms, Cloud cryptography, Privacy

REFERENCES

[1]. Proceedings of the 43rd ACM Symposium on Theory of Computing (pp. 309-318). ACM
[2]. Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof-Systems. SIAM Journal on Computing, 18(1), 186-208
[3]. Rane, S., & Apte, V. (2013). Searchable Symmetric Encryption: Approaches, Challenges, and Future Directions. International Journal of Computer Applications, 73(13), 15-20.
[4]. Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120-126.
[5]. Bellare, M., Rogaway, P., & Steinfeld, R. (2003). Keying Hash Functions for Message Authentication. In CRYPTO 2003: Advances in Cryptology (pp. 1-15). Springer.