CERTIFICATE NO : NCISETH/2023/C0723531

AN EVALUATION OF SECURITY ALGORITHMS FOR ENHANCED CLOUD COMPUTING PROTECTION

AJITESH KUMAR SAHA

Research Scholar, Ph. D. in Computer Science & Engineering
Mansarovar Global University, Bilkisganj, M.P.

ABSTRACT

Due to expanding understanding and concerns about data security, encryption techniques are becoming more vital for securing authentication access, user sessions, system applications, and most crucially data in transit over the insecure Internet when using Cloud services. Cloud Service Providers are putting a premium on data security for their clients, however this comes at the cost of Cloud Performance due to variations in the encryption and encoding methods used. The evaluation of security algorithms is critical for enhancing protection in cloud computing, where data and applications are highly vulnerable to sophisticated cyber threats. As cloud adoption grows, the need for robust encryption algorithms, secure key management, and authentication protocols has become paramount. Security algorithms such as Advanced Encryption Standard (AES), RSA, and Elliptic Curve Cryptography (ECC) are being scrutinized for their effectiveness in safeguarding cloud environments. AES, known for its speed and efficiency, is widely used for encrypting data at rest and in transit, while RSA and ECC are favored for secure key exchanges and digital signatures. Evaluating these algorithms involves assessing their resilience against attacks, computational efficiency, and compatibility with cloud architectures. Furthermore, emerging algorithms leveraging quantum cryptography and homomorphic encryption are being explored for their potential to offer even stronger security in cloud computing. Through rigorous evaluation, organizations can implement the most appropriate algorithms to ensure data confidentiality, integrity, and availability, thereby fortifying their cloud infrastructures against evolving cyber threats.