ABSTRACT

Abstract—Cloud computing transformed data storage and retrieval with scalable, cost-efficient, and flexible approaches. Data leakage is one of the most critical security threats that exposes confidential information to unauthorized users and cyber attacks. This paper introduces a full security framework based on AES-256 encryption, watermarking, and fake object insertion to safeguard cloud data.AES-256 encryption ensures data confidentiality, watermarking ensures traceability with identifiers, and insertion of simulated objects ensures a decoy to detect unauthorized access attempts. The system architecture, workflow, and algorithms suggested are compared to determine its utility to prevent data breaches.

A comparative study of existing approaches is also carried out to study their feasibility and limitations. The results establish that encryption, watermarking, and decoy-based detection greatly enhance cloud security with insider threat prevention and accountability. This research is significant through the introduction of a robust and viable solution to data leakage prevention, thus supporting further development in cloud security solutions.