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 2, November 2025
Impact Factor: 7.67

A Systematic Review of Cryptographic Approaches in Privacy-Preserving Data Mining

Jitendra Shrivastav[1] and Dr. Sanmati Kumar Jain[2]
[1]Research Scholar, Department of Computer Science and Engineering
[2]Research Guide, Department of Computer Science and Engineering
Vikrant University, Gwalior (M.P.)

Abstract: *Privacy-Preserving Data Mining is an interdisciplinary field that addresses the challenge of extracting meaningful patterns and knowledge from data while ensuring the confidentiality and privacy of sensitive information. Cryptographic techniques have emerged as fundamental enablers of PPDM by providing formal security guarantees during data analysis. This paper systematically reviews major cryptographic approaches used in PPDM, including Secure Multiparty Computation, Homomorphic Encryption, Differential Privacy, and Zero-Knowledge Proofs. We examine their underlying mathematical principles, present key formulas, evaluate their performance in terms of computational and communication overhead, and discuss their practical applications. The review also highlights current challenges, such as scalability and real-world deployment, and suggests future research directions, including hybrid models and post-quantum cryptographic adaptations. This synthesis aims to serve as a comprehensive reference for researchers and practitioners navigating the landscape of privacy-preserving analytics.*

Keywords: Privacy-Preserving Data Mining, Secure Multiparty Computation

DOI: 10.48175/568