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 9, March 2025
Impact Factor: 7.67

# Differential Privacy in AI Models for Cyber-Security Applications

**Anil B. Thenge**
Dept. of Mathematics
Shivaji Mahavidyalaya, Renapur, Latur, MS
anilthenge@gmail.com

**Abstract:** *Artificial Intelligence (AI) has become an essential tool in modern cyber-security applications such as intrusion detection, malware detection, and network monitoring. However, AI models require large amounts of data, often containing sensitive personal or organizational information. Differential Privacy (DP) offers a mathematical framework to ensure that individual data remains confidential while enabling effective AI model training. This paper presents a simplified mathematical explanation of differential privacy and explores its role in AI-driven cybersecurity systems.*

**Keywords:** Artificial Intelligence (AI), Differential Privacy (DP), Clipped Gradient, Laplace Mechanism, Cyber-security, Gradient Noise Addition