Abstract

In the realm of complex industrial processes, optimizing e ciency through distributed algorithms is pivotal, yet vulnerable to adversarial attacks that aim to compromise the integrity and e ectiveness of optimization processes. Adversarial attacks encompass various malicious strategies, including data poisoning, model evasion, and privacy breaches, which pose signiýcant threats to the reliability and security of distributed optimization systems. To mitigate these risks, di erential privacy emerges as a crucial safeguarding mechanism. By incorporating di erential privacy into distributed optimization algorithms, sensitive data can be protected without compromising the accuracy of optimization outcomes. This abstract explores the role of di erential privacy in countering adversarial threats, discusses implementation strategies such as noise injection and secure aggregation, and highlights real-world applications in smart manufacturing and energy grid management. Despite challenges in performance and integration complexity, the adoption of di erential privacy promises to fortifvaV , ẹ m ᴀ V ʊ 𝘛

computation. In distributed optimization, this means algorithms can operate on aggregated data without revealing sensitive information about any individual data contributor.

Implementing di erential privacy in distributed optimization

Incorporating di erential privacy into distributed optimization algorithms involves several key strategies