File name: FID-028.txt

Result: PLAGIARISM NOT DETECTED

Plagiarism percentage: 0%

Text to analyze:

The recent advances in machine learning (ML) and Artificial Intelligence (AI) have resulted in widespread application of data-driven learning algorithms. Rapid growth of AI/ML and their penetration within a plethora of civilian and military applications, while successful, has also opened new vulnerabilities. It is now clear that ML algorithms for AI systems are viable targets for malicious attacks. Therefore, there is a pressing need for better understanding of adversarial attacks against ML models, in order to secure them against such malicious attacks. In this paper, we present a survey of adversarial machine learning and some associated countermeasures. We also present a taxonomy of ML/AI system attacks that follow the same properties and characteristics, allowing them to be linked with different defensive approaches. A taxonomy is given for both attack and defense, and attacks proposed in the literature are categorized according to our taxonomy.

Sentence analysis:

Original sentence (file FID-028.txt):
'The recent advances in machine learning (ML) and Artificial Intelligence (AI) have resulted in widespread application of data-driven learning algorithms.'

Original sentence (file FID-028.txt):
'Rapid growth of AI/ML and their penetration within a plethora of civilian and military applications, while successful, has also opened new vulnerabilities.'

Original sentence (file FID-028.txt):
'It is now clear that ML algorithms for AI systems are viable targets for malicious attacks.'

Original sentence (file FID-028.txt):
'Therefore, there is a pressing need for better understanding of adversarial attacks against ML models, in order to secure them against such malicious attacks.'

Original sentence (file FID-028.txt):
'In this paper, we present a survey of adversarial machine learning and some associated countermeasures.'

Original sentence (file FID-028.txt):
'We also present a taxonomy of ML/AI system attacks that follow the same properties and characteristics, allowing them to be linked with different defensive approaches.'

Original sentence (file FID-028.txt):
'A taxonomy is given for both attack and defense, and attacks proposed in the literature are categorized according to our taxonomy.'