DP-LSSGD: A Stochastic Optimization Method to Lift the Utility in Privacy-Preserving ERM

Tech ID: 31895 / UC Case 2019-884-0

SUMMARY

UCLA researchers in the Department of Mathematicshave developed a method to maintain data privacy.

BACKGROUND

Companies use machine learning (ML) algorithms to analyze their user base for information to improve targeted advertisements and customer tracking. However, with many parameters in the accumulated data sets, the algorithms can memorize the training data, making it possible to recover sensitive user information and break privacy. Current methods to overcome this privacy issue, such as adding 'noise' (artificial data), improve security but decrease data accuracy. Therefore, there is a need for improved ML algorithms that maintain user privacy without decreasing data analysis accuracy.

INNOVATION

UCLA researched have developed a ML algorithm that produces models with improved data protection without decreasing user data accuracy. The algorithm reduces training and validation loss and improves the generalization of the trained private models. The algorithm has been successfully tested to create models that were 10% more accurate and equal/better data privacy than models created by existing methods. Additionally, the method was easier to implement and required negligible additional computational power and memory cost compared to existing methods.

APPLICATIONS

- Cybersecurity
- Internet Privacy

ADVANTAGES

- 10% faster than current methods used
- Can be implemented on current hardware
- Negligible extra computational complexity and memory cost

STATE OF DEVELOPMENT

The method has been tested and developed.

CONTACT

UCLA Technology Development Group
ncd@tdg.ucla.edu
tel: 310.794.0558.

INTRODUCING
UC TechAlerts
New technology matches delivered to your email at your preferred schedule
SEARCH SAVE SEARCH
Learn More

INVENTORS

- Osher, Stanley J.

OTHER INFORMATION

KEYWORDS

Digital Privacy, Advertisement, Data Safety, Algorithms, Data sets, Internet Security

CATEGORIZED AS

- **Computer**
  - Other
  - Security

RELATED CASES

2019-884-0

UCLA Technology Development Group
10889 Wilshire Blvd., Suite 920,Los Angeles,CA 90095
https://tdg.ucla.edu
Tel: 310.794.0558 | Fax: 310.794.0638 | ncd@tdg.ucla.edu

© 2020, The Regents of the University of California
Terms of use
Privacy Notice