Meenakshi Nagarajan

Detecting Violations of Differential Privacy

Research problem and its importance

With increasing number of databases which contains our personal information, differential privacy algorithms are essential to make an effective use of data while preserving privacy. However, large number of existing differential privacy algorithms are fraught with errors and complications which affects novices and experts as well who attempts to design an error-free algorithm to accurately learn the data without compromising privacy. This paper talks about developing a method to find how the algorithms violate differential privacy.

Technical challenges of the problem

There are two main challenges when working with sensitive data. Their privacy should be maintained and verification of results should be done without original data. While there are tools and verification techniques to assist developers to create an error free algorithm and can verify the results of the model respectively, it cannot be done at the cost of privacy and integrity.

Proposed approach

In this paper, they adopted a new approach which uses statistical tests to find errors in the algorithm that affects the differential privacy guarantee. While the existing programming tools and techniques, helps to create and verify a correct algorithm and discards the incorrect one, the counterexample generation approach, identifies the bugs in the program that violates the privacy and generate examples to practically illustrate why the algorithm is false.

Strengths of the approach

- Counter examples can advise developers of errors in the algorithm help them fix the issues
- This approach can be useful to novices who are new to differential privacy to understand why an algorithm fails and they can use this knowledge in the design of more sophisticated algorithms
- It is not restricted to a specific programming language
- False positive error is minimal

Possible weaknesses

- Fails to identify violations that happens very rarely
- Lacks theoretical guarantee