Bachelor Project on Local Differential Privacy

Johan Ringmann Fagerberg (jofag17) - 1996-09-24

Motivation

Differential privacy is a recently proposed measure of the level of privacy provided by random functions. It provides a formal measure for how much information a potential attacker can achieve from a perturbed data set, when the data perturbation consists of random noise.

In global differential privacy, a global aggregator has access to the real data prior to perturbing it. This differs from local differential privacy, where users perturb their data before sending it to the aggregator.

I aim to gain an understanding of differential privacy in general, with a particular focus on local differential privacy, and attempt to use that to produce an architecture for a trust-less and privacy-respecting web analytics solution.

Product

Description of a web analytics system, à la [Akk+12], but using local differential privacy (or potentially ESA, depending on whether that'd be relevant - requires better understanding) to remove the need for users to trust a potentially malicious third party. Report should include an evaluation of the pros and cons of this implementation vs.

Experiments

Current proposal mostly involves analyzing a theoretical solution. It would definitely be important to analyze real world applications, i.e. how much the added noise from differential privacy would impact usability of the analytics, but actual experiments would require an implementation which I am unlikely to achieve in 10 ECTS.

Risks

Potentially not possible to generate an actually useful trust-less web analytics solution (e.g. due to increased noise from local differential privacy). Could still produce report and evaluate why it doesn't work.

Research entry points

[Des19] Reading list of key papers in differential privacy. Part of a semi-technical blog series on differential privacy. Probably the most useful entry point.

[Yan+20] Recent survey on local different privacy methods for various use cases. Primarily useful as a source of articles through its citations.

References

[Akk+12] Istemi Ekin Akkus et al. "Non-tracking web analytics". In: *Proceedings of the 2012 ACM conference on Computer and communications security*. CCS '12. Raleigh, North Carolina, USA: Association for Computing Machinery, Oct. 2012, pp. 687–698. ISBN: 9781450316514. DOI: 10.1145/2382196.2382268. URL: https://doi.org/10.1145/2382196.2382268 (visited on 11/25/2020).

[Des19] Damien Desfontaines. *A reading list on differential privacy*. 2019. URL: https://desfontain.es/privacy/differential-privacy-reading-list.html (visited on 11/25/2020).

[Yan+20] Mengmeng Yang et al. "Local Differential Privacy and Its Applications: A Comprehensive Survey". In: *arXiv:2008.03686 [cs]* (Aug. 2020). arXiv: 2008.03686. URL: http://arxiv.org/abs/2008.03686 (visited on 11/25/2020).