A trustless, privacy-preserving recommendation system

Practical, verifiable secure multi-party computation for decentralized collaborative sys.
(Draft of Proposal paper)

David Aparicio

February 12, 2016

1 Motivation

Imagine that you go to an amusement park, get out of one of the many attractions, and exclaim in front of your whole family, because you really enjoyed the ride. Your connected watch transmits, anonymously, the animation of your arms to the Cloud, which analyzes them and deduces that you had a great time in that particular part of the theme park. On the other hand, the absence of gestures could show a lassitude or lack of opinion about the attraction. This would be the future of a reputation system without any notice or form to fill.

Or we can give the example that a camera analyzes the emotions that your face at the exit of your plane, or train, to know your level of happiness, satisfaction. The study could also be done by analyzing social networks with textual analysis.

This would be a good solution, instead of being spammed with emails and notifications, to fill the satisfaction formulation. The data is out-sourced to a cloud[2] because the producers of this data are smart-devices and don't have the capacity (nor the will from a mobility/battery point of view) to do these expensive calculations. Moreover, they want to be online/offline quite regularly.

Figure 1: Theme park attraction

1.1 Reputation

Reputation allows to evaluate the services that a company provides. It can also be used to evaluate the users of a service. Indeed, Waze, the social GPS uses the information provided by users' smartphones (current speed, average speed) to evaluate the congestion of a road. Moreover, it can add the reports made by the latter, to signal the presence of works, objects on the road, potholes or current weather conditions (dense fog, heavy rain or snowstorm). They can also contribute to the updating of the maps by adding new roads or altering them. Nevertheless, users must be honest if Waze wants to provide the best possible route.

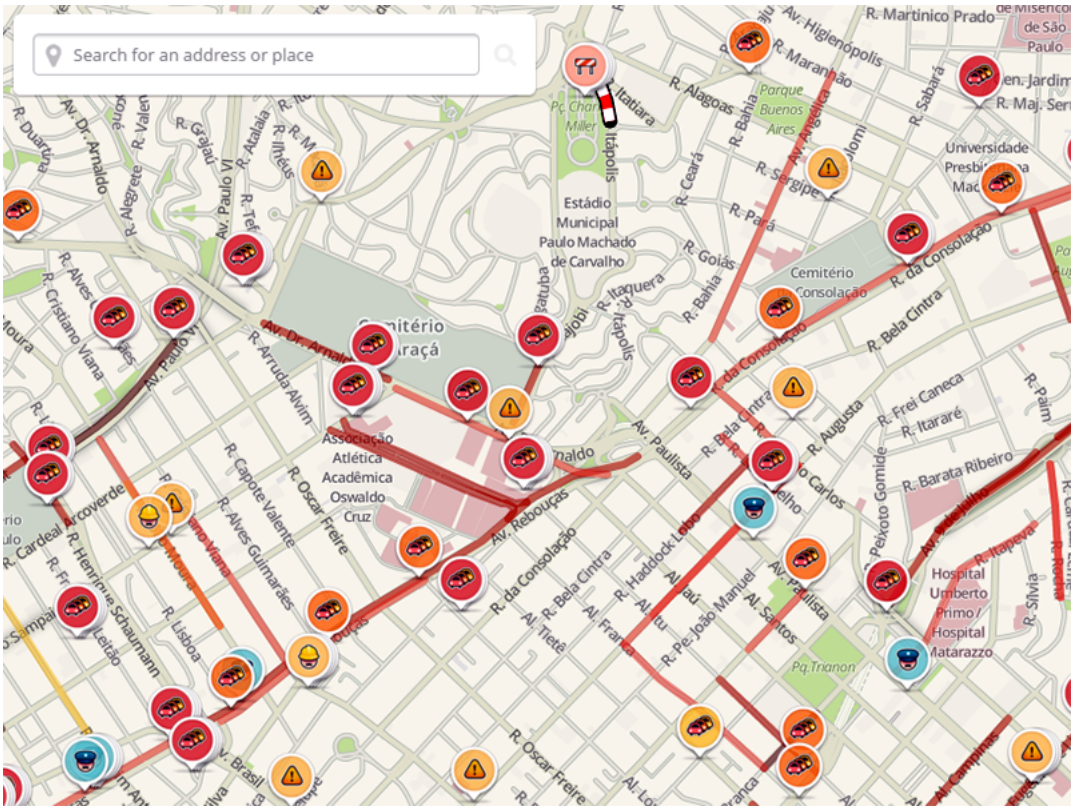

Figure 2: Waze, the social GPS is based on all the reports made by users

1.2 Problems

For reasons of Single Point of Failure (SPOF) and data integrity in case of attacks on the central server, it is better to use a decentralized solution. The solution proposed by Hasan et al. [3] is very interesting but suffers from some drawbacks. The first one is that the clusters must remain online in order to compute the reputation of a node. In the recent work of Schaud et al. [4], this problem has been corrected by adding a data structure, decentralized and distributed, like the Blockchain. But this raises another problem, customers have to solve the puzzle in order to be able to publish their feedback, and this can be very expensive for small devices like smartphones or connected bracelets.

2 Model

One proposal would be to combine the two works to solve the problems raised in the given examples.

We use the same concept as the article [1]

3 State of the Art

Cf. Hasan's survey

4 Objectives

- Practical - Robustness - Decentralization - Suitability for distributed applications - Trustlessness - Anonymity preservation

References

[1] David W Archer, Dan Bogdanov, Benny Pinkas, and Pille Pullonen. Maturity and performance of programmable secure computation. 2015.

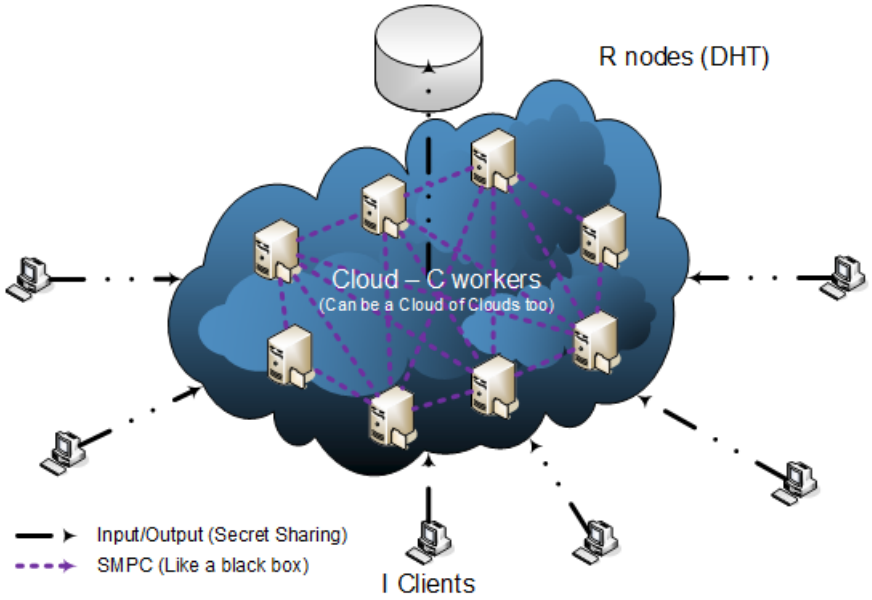

Figure 3: Model with I clients, C workers, R nodes in the multi-cloud

[2] Yao Chen and Radu Sion. To cloud or not to cloud?: musings on costs and viability. In *Proceedings of the 2nd ACM Symposium on Cloud Computing*, page 29. ACM, 2011.

[3] Omar Hasan. *Privacy preserving reputation systems for decentralized environments*. PhD thesis, 2010.

[4] Alexander Schaub, Rémi Bazin, Omar Hasan, and Lionel Brunie. A trustless privacy-preserving reputation system. Cryptology ePrint Archive, Report 2016/016, 2016.