Système de réputation distribué

Proposal paper

David Aparicio

February 12, 2016

1 Motivation

Imaginez que vous vous rendiez dans un parc de loisirs, que vous sortiez de l'une des nombreuses attractions, et vous vous exclamiez devant toute votre famille, car vous avez réellement apprécié le manège. Votre montre connectée transmets, de manière anonyme, l'animation de vos bras au Cloud qui les analyse et en déduit que vous avez savouré un très moment dans cet endroit précis du parc à thème. A l'opposé, l'absence de gestes pourrait montrer une lassitude ou sans-avis par rapport à l'attraction. Ainsi serait le futur d'un système de réputation sans avis ou formulaire à remplir.

Ou bien nous pouvons donner l'exemple qu'une caméra analyse les émotions que votre visage à la sortie de votre avion, ou train, pour connaître votre niveau de bonheur, de satisfaction. L'étude pourrait également se faire en analysant les réseaux sociaux avec de l'analyse textuelle.

Ceci serait une bonne solution, au lieu d'être spammé d'e-mails et de notifications, afin de remplir le formulation de satisfaction. Les données sont out-sourcés vers un cloud[2] car les producteurs de ces données sont des smart-devices et n'ont pas la capacité (ni la volonté du point de vue mobilité/batterie) de faire ces calculs coûteux. De plus, ils veulent être online/offline assez régulièrement.

Figure 1: Attraction dans un Parc à thème

1.1 Réputation

La réputation permet d'évaluer les services qu'une entreprise fournis. Elle permet également d'évaluer les utilisateurs d'un service, en effet, Waze, le GPS social utilise les informations fournis par les smartphones des utilisateurs (vitesse actuelle, vitesse moyenne) pour évaluer l'engorgement d'une route. De plus, il peut s'ajouter les rapports réalisés par ces derniers, pour signaler la présence de travaux, d'objets sur la route, de nids de poules ou bien des conditions actuelles climatiques (brouillard dense, pluie forte ou tempête de neige). Ils peuvent également contribuer sur la mise à jour des cartes en y ajoutant de nouvelles routes ou en les altérant. Néanmoins, les utilisateurs doivent être honnêtes si Waze souhaite fournir le meilleur itinéaire possible.

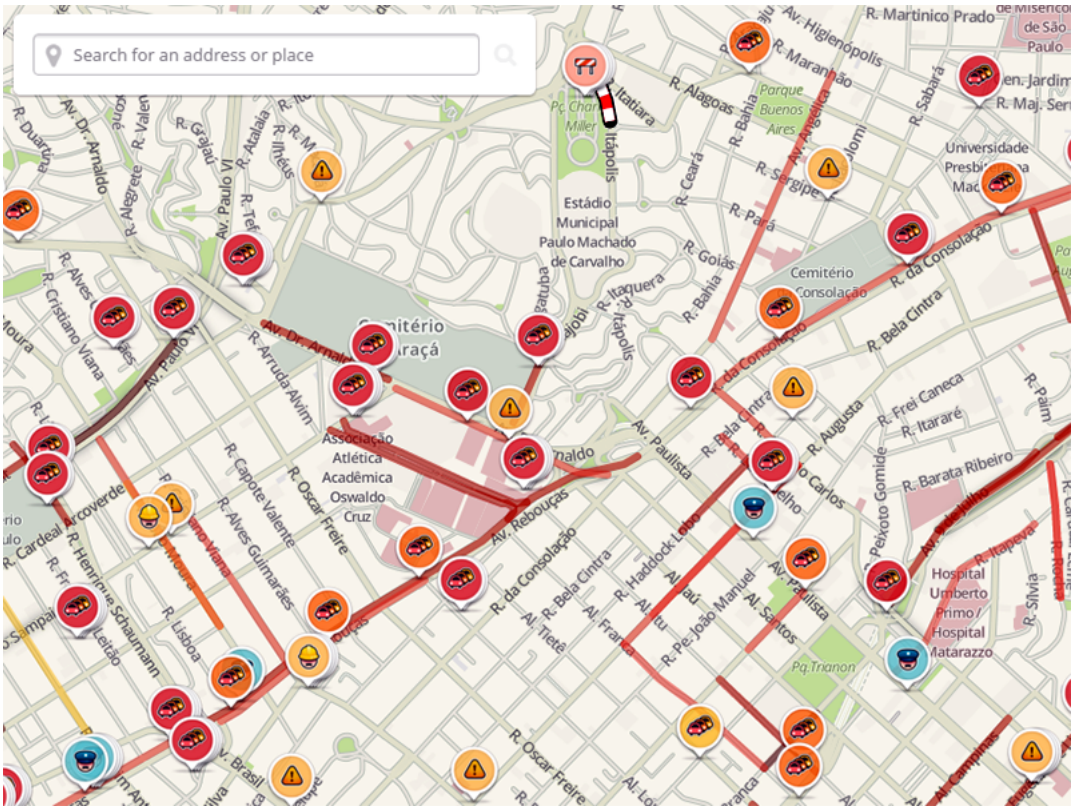

Figure 2: Waze, le GPS social se base sur l'ensemble des reports faits par les utilisateurs

1.2 Problèmes

Pour des raisons de Point individuel de défaillance (SPOF) et d'intégrité des données en cas d'attaques sur le serveur central, il est préférable d'utiliser une solution décentralisée. La solution proposée par Hasan et al. [3] est fort intéressante mais souffre de quelques inconvénients. La première est que les clusters doivent rester en ligne pour pouvoir calculer la réputation d'un noeud. Dans le récent travail de Schaud et al. [4], ce problème a été corrigé par le rajout d'une structure de données, décentralisée et distribuée, comme la Blockchain. Mais cela lève un autre problème, les clients doivent résoudre le puzzle afin de pouvoir publier leur retour d'expérience (feedback), et cela peut-être très coûteux pour des petits devices comme les smartphones ou des bracelets connectés.

2 Modèle

Une proposition serait de combiner les deux traveux pour résoudre les problèmes soulevés dans les exemples donnés.

Nous utilisons la même notion que l'article [1]

3 État de l'Art

Cf. Hasan's survey

4 Objectifs

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

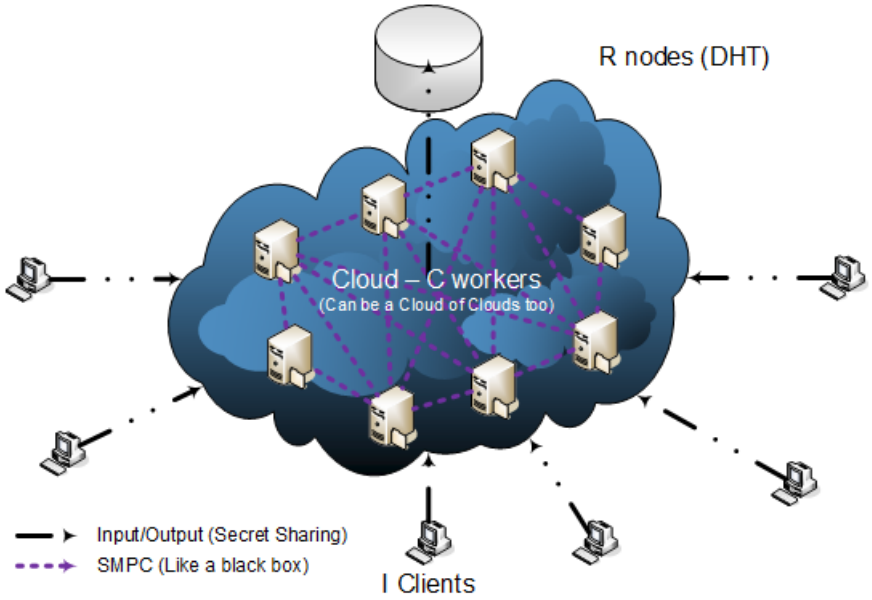

Figure 3: Modèle avec I clients, C workers, R noeuds dans le cloud

References

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

[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.