Chapter 9

A P2P Architecture for Social Networking

Michele Tomaiuolo
https://orcid.org/0000-0002-6030-9435
University of Parma, Italy

Monica Mordonini
https://orcid.org/0000-0002-5916-9770
University of Parma, Italy

Agostino Poggi
https://orcid.org/0000-0003-3528-0260
University of Parma, Italy

ABSTRACT

Social networking systems are usually huge centralized systems owned by a single company. However, this solution has many drawbacks (e.g., lack of privacy, lack of anonymity, risks of censorship, and operating costs). This chapter proposes a novel P2P system that leverages existing, widespread, and stable technologies such as DHTs and BitTorrent. In particular, it introduces a key-based identity system and a model of social relations for distributing content efficiently among interested readers. The proposed system, called Blogracy, is a micro-blogging social networking system focused on (1) anonymity and resilience to censorship, (2) authenticatable content, and (3) semantic interoperability using activity streams. This chapter presents the model and the implementation of the Blogracy system, discusses the experimentations to study its behavior, and presents their results regarding (1) communication delays for some simulations of node churn, (2) delays measured in test operations over PlanetLab in direct communication, and (3) through the I2P anonymizing network.

DOI: 10.4018/978-1-5225-8295-3.ch009
INTRODUCTION

After the huge success of the early social networking systems, many other players came into the social networking market and nowadays hundreds of different social networking systems exist. Even if these social networking systems are greatly dissimilar in their user base and functionality, they are almost always centralized systems. The centralized nature allows a simple browser-based user experience and, moreover, many algorithms, e.g., friend suggestion, are far easier and more efficient to implement in this setting.

A drawback is that scaling centralized systems to tens or hundreds of millions of users is not an easy task. Certainly, existing systems demonstrate that the problem can be solved providing enough resources. However, the huge operative costs of supporting the infrastructure necessary to provide the service to millions of users can only be justified with robust business plans. While some social networking services have extremely differentiated business models (Hobart, 2011; McGrath, 2010), for most of them the primary source of income is advertisement and consequently they have a strong motive for: (i) using user provided data to increase performance for that purpose and (ii) even giving access to authorized commercial third parties to the data. This behavior poses serious threats to privacy and data protection issues and there are virtually no specific legislation or explicit guarantees.

Another problem is that many social networking systems have very demanding terms of service, essentially asking their users a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use content that they submit. Arguably, social networking sites tend to guide their users into “walled gardens,” without giving users full control over their own information because such information constitutes much of the company value (Berners-Lee, 2010; Shankland, 2010).

The last problem with centralized social networking systems is that service providers are in the position to perform a-priori or a-posteriori censorship and may be forced for legal reason: (i) to perform such actions, and (ii) to disclose all the information they have, no matter how private (Franchi, Poggi & Tomaiuolo, 2013). In fact, the recent clamor about the PRISM program and the release of classified documents by Edward Snowden (Greene, 2014) has raised many questions about the privacy issues of current social networking applications.

Thus, we believe that an approach based on peer-to-peer (P2P) or distributed technologies not only is viable but also highly desirable. First of all, P2P systems essentially achieve simpler resource scalability, in the sense that the availability of resources is roughly proportional to the number of users.
The Dynamic Data Privacy Protection Strategy Based on the CAP Theory
www.igi-global.com/chapter/the-dynamic-data-privacy-protection-strategy-based-on-the-cap-theory/224589?camid=4v1a