Chapter 36
Blogracy:
A Peer-to-Peer Social Network

Enrico Franchi
University of Parma, Italy

Agostino Poggi
University of Parma, Italy

Michele Tomaiuolo
University of Parma, Italy

ABSTRACT

The current approach to build social networking systems is to create huge centralized systems owned by a single company. However, such strategy has many drawbacks, e.g., lack of privacy, lack of anonymity, risks of censorship and operating costs. In this paper the authors propose a novel P2P system that leverages existing, widespread and stable technologies such as DHTs and BitTorrent. In particular, they introduce a key-based identity system and a model of social relations for distributing content efficiently among interested readers. The system they propose, Blogracy, is a micro-blogging social networking system focused on: (i) anonymity and resilience to censorship; (ii) authenticatable content; (iii) semantic interoperability using activity streams. The authors have implemented the system and conducted various experiments to study its behaviour. The results are presented here, regarding (i) communication delays for some simulations of node churn, (ii) delays measured in test operations over PlanetLab, in direct communication, and (iii) through the I2P anonymizing network.

1. INTRODUCTION

After the huge success of the early social networking systems, many other players came in 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.

DOI: 10.4018/978-1-5225-7113-1.ch036

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

A drawback is that scaling centralized systems to tens or hundreds of million 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 and 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. This property is especially desirable for media sharing social networking systems, considering the exceptionally high amount of resources needed. Secondly, the popularity over time of most content on such systems exhibits either a power-law or an exponential behavior (Avramova et al., 2009) and is consequently well suited for P2P distribution (Zink et al., 2009), possibly with fallback strategies for less popular content. Regarding censorship issues, a P2P system essentially solves them by design. Without a central entity, nobody is in the position of censoring data systematically nor may be held legally responsible for the diffusion of censurable data: the sole owners and responsible of the data are the users themselves.

Attacks to distributed and P2P social platforms are yet possible, for example by introducing sybil nodes in the network, i.e., nodes with forged identities created to subvert the reputation system in a P2P network. However, analyzing these kinds of attacks is not the focus of the article. A comprehensive list of such attacks and countermeasures is presented in (Franchi and Tomaiuolo, 2013).

The main objective of this article is to present Blogracy, a new P2P system for social networking that we implemented and tested on the PlanetLab infrastructure. Thus, some results will be presented about the feasibility and limitations encountered in the realization of a distributed social networking system layered upon a widespread file sharing network such as BitTorrent. The system is modular in the approach to the core problems of (*i*) data availability and resilience to censorship, (*ii*) content authenticability, (*iii*) data confidentiality, (*iv*) network anonymity, and (*v*) semantic interoperability. All these aspects are kept as much orthogonal as possible in the system. For both its architecture and its level of implementation, to our knowledge it is quite unique. Being available as open source software, it can be freely used for conducting further analysis and evaluations in the larger research area of distributed social platforms, exploring alternative architectural choices and implementations along each axis.

20 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/blogracy/213827

Related Content

Airplane Health Surveillance System: For Connected World
N. B. Rachana, K. G. Srinivasaand S. Seema (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 1259-1272).*
www.irma-international.org/chapter/airplane-health-surveillance-system/213853

Gender, Translation, and Censorship: The Well of Loneliness (1928) in Spain as an Example of Translation in Cultural Evolution
Gora Zaragoza (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 1868-1892).*
www.irma-international.org/chapter/gender-translation-and-censorship/213889

Public-Private Partnerships in Support of Critical Infrastructure and Key Resources
Martin A. Negrónand Doaa Taha (2019). *National Security: Breakthroughs in Research and Practice (pp. 633-646).*
www.irma-international.org/chapter/public-private-partnerships-in-support-of-critical-infrastructure-and-key-resources/220905

A Surveillance and Spatiotemporal Visualization Model for Infectious Diseases Using Social Network
Younsi Fatima-Zohra, Hamdadou Djamilaand Boussaid Omar (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 1027-1046).*
www.irma-international.org/chapter/a-surveillance-and-spatiotemporal-visualization-model-for-infectious-diseases-using-social-network/213842

Utilization Pattern and Privacy Issues in the Use of Health Records for Research Practice by Doctors: Selected Nigerian Teaching Hospitals as Case Study
Eunice Olubunmi Omidoyin, Rosaline Oluremi Opekeand Gordon Kayode Osagbemi (2019). *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications (pp. 1179-1190).*
www.irma-international.org/chapter/utilization-pattern-and-privacy-issues-in-the-use-of-health-records-for-research-practice-by-doctors/213849