

GEMSTONE: A Generic Middleware for Social Networks

David Koll
Institute of Computer Science
University of Goettingen,
Germany
koll@cs.uni-goettingen.de

Florian Tegeler
Institute of Computer Science
University of Goettingen,
Germany
tegeler@cs.uni-goettingen.de

Xiaoming Fu
Institute of Computer Science
University of Goettingen,
Germany
fu@cs.uni-goettingen.de

1. INTRODUCTION

Online Social Networks like Facebook or Flickr have seen a boost in popularity over the past years and have recently started to extend their reach to mobile consumer devices. Still, the centralized nature of their architectures raises privacy concerns with respect to external attacks as well as internal data misuse. Moreover, direct connectivity to a central server is required, preventing participation from intermittently connected mobile devices. We present GEMSTONE, a fully decentralized, privacy preserving socio-aware middleware, that enables any application on top of it to use social information.

2. GEMSTONE

GEMSTONE is developed to perform the following common functionality required by most social applications and thus allows easy development:

- Social graph maintenance, including friend lists and group membership/leading.
- Privacy preservation and security mechanisms via attribute based encryption (following [1]) to protect personal data and provide access control to profile information. Privacy is additionally supported by fully decentralized data storage on preferably socially related nodes, which are specifically selected to ensure high availability with minimal replication.
- Data dissemination and network participation even via intermittently connected links using MobiClique-like [4] DTN forwarding in case of non-present infrastructure.

3. NODE SELECTION IN GEMSTONE

Our main contribution is a holistic approach to select suitable nodes for decentralized data storage that ensures a high availability of data with minimal replicas in the system, even if the data owner is disconnected. As shown in **Figure 1**, nodes are selected based on the following criteria:

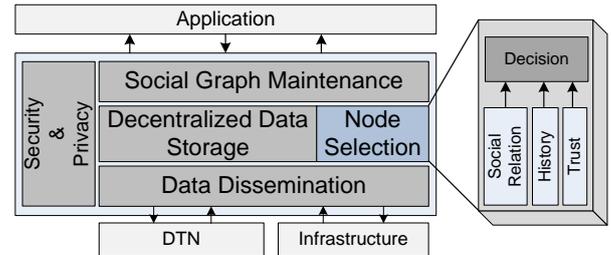


Figure 1: GEMSTONE Node Architecture

1. *Social connection*: Data is preferably stored at socially related nodes to ensure that the storing node has an incentive to store data for others.
2. *Availability and resources*: GEMSTONE keeps track of previous node encounters and availability information, allowing to select a node with sufficient resources that is met frequently.
3. *Experience*: A sophisticated trust and reputation module recommends highly trustworthy nodes based on own and other nodes experiences.

Whereas previous approaches [2, 3] treat all nodes equally, we take resource limitations, availability and even a node's intention into account. In addition to increasing the robustness of decentralized data storage, GEMSTONE inherently eases the burden on mobile devices since they are less likely to be chosen as mirroring nodes. We have implemented a basic GEMSTONE prototype and are currently evaluating its performance.

4. REFERENCES

- [1] Baden *et al.* Persona: an online social network with user-defined privacy. In *SIGCOMM*, 2009.
- [2] Buchegger *et al.* PeerSoN: P2P social networking: early experiences and insights. In *SNS*, 2009.
- [3] Cuttillo *et al.* Safebook: A privacy-preserving online social network leveraging on real-life trust. *IEEE Communications Mag.*, Dec. 2009.
- [4] Pietiläinen *et al.* MobiClique: middleware for mobile social networking. In *WOSN*, 2009.