**Group 2015.010 members: Qi Liu (20358515)**

**Asif Arman (20349964)**

**SangHoon Lee (20357600)**

**Danny Yan (20387735)**

**Distributed Messaging**

Instant messaging systems of today simply cannot adequately safeguard the privacy of their users. Users’ contacts lists, profile data, and even message histories are always logged and stored on centralized servers fully-controlled by the messaging system’s service providers. There is simply no guarantee that users’ data won’t be searched and abused by these companies. Even if we put aside the trust issue between customer and service provider, data breaches by malicious third-parties are dangerous, ever-present possibilities on any centralized server exposed to the internet. Furthermore, recent leaks provided by Edward Snowden on NSA’s overreach in its information collection practices has highlighted the fact that governments can easily and legally force service providers to hand over any and all user data available to them. We have designed an instant messaging system that protects the privacy of its users as an utmost priority. Our system implements a truly decentralized peer-to-peer architecture with no centrally controlled servers of any kind. Unlike existing centralized messaging systems, messages in our distributed system will thus travel directly from the sender to the recipient, through a completely encrypted channel, giving no opportunity for any third-party to access message contents.