InM (InMind): Affect and Availability Sharing In Social Circles

by

Joy C. Chen

Submitted to the Department of Electrical Engineering and Computer Science
in partial fulfillment of the requirements for the degrees of

Bachelor of Science

and

Master of Science in Computer Science and Engineering

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

June 2014

Author .....
Department of Electrical Engineering and Computer Science
May 23, 2014

Certified by .....
Rosalind Picard
Professor of Media Arts and Sciences
Thesis Supervisor

Accepted by .....
Albert Meyer
Chairman, Department Committee on Graduate Theses

InM (InMind): Affect and Availability Sharing In Social Circles

by

Joy C. Chen

Submitted to the Department of Electrical Engineering and Computer Science
on May 23, 2014, in partial fulfillment of the
requirements for the degrees of
Bachelor of Science
and
Master of Science in Computer Science and Engineering

Abstract

TBD

Thesis Supervisor: Rosalind Picard
Title: Professor of Media Arts and Sciences

Acknowledgments

TBD

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 TBD

Chapter 2

Background

2.1 TBD

Chapter 3

System Overview

3.1 Application

3.1.1 Hardware

3.1.2 Security

3.2 Server

3.2.1 Design

The server for InMind was written using Node.js. The choice of Node.js offered many benefits, including asynchronous responses, lightweight maintenance, and easy integration with MongoDB for data retention.

MongoDB gave us flexibility for designing how we wanted data to be stored, and we took advantage of MongoDBś simple backup mechanism for data integrity.

The data saved on the server included records of all the app interactions. For each of the actions performed by the users, we logged the timestamp of the operation as well as the recipients.

To keep user data secure, the server was hosted on an MIT Media Lab server. The machine... TBD

3.2.2 Security

During the study, while the server was running, it was password protected, as was the database in which the data was stored.

For added protection for our users, all messages were encrypted. This encryption was on several levels, primarily using the AES standard. TBD

1. To protect user identities, signup for the lead participant was performed manually. All "lead" participants had to be entered into the database manually, and later participants sign up anonymously with a user id and password. Data on all users are deidentified; the database remembers only an alphanumeric user id.

2. Each group shares an initialization vector.

3. Each topic has a salt and an autogenerated passphrase.

3.3 Design Challenges

Chapter 4

User Study

4.1 TBD

Chapter 5

Results

5.1 TBD

Chapter 6

Conclusion

6.1 TBD

Appendix A

Additional Materials

Appendix B

Data