Professor R. G. N. Meegama
Department of Computer Science
Faculty of Applied Sciences
University of Sri Jayewardenepura

12th August 2014

Registrar
Faculty of Graduate Studies
University of Sri Jayewardenepura

Declaration of the Supervisor:
PhD thesis on "Demand-based Mobile Learning Network

I certify that the candidate has incorporated all corrections, additions and amendments recommended by the examiners in the viva-voce examination which was held on 04th August 2014.

Thanking you.

Sincerely,

.....

Prof. R.G.N. MEEGAMA
Department of Statistics and
Computer Science
Faculty of Applied Sciences
University of Sri Jayawardenepura
Nugegoda - Sri Lanka.

Demand-based Mobile Learning Network

By

Hathurusingha Kankanamalage Salinda Premadasa

Ph.D. 2014

Demand-based Mobile Learning Network

By

Hathurusingha Kankanamalage Salinda Premadasa

Thesis submitted to the University of Sri Jayewardenepura for the award of the Degree of Doctor of Philosophy in Computer Science on August 2014

Declaration

The work described in this thesis was carried out by me under the supervision of

Professor R. G. N. Meegama
Department of Computer Science
Faculty of Applied Sciences
University of Sri Jayewardenepura

A report on this thesis has not been submitted in whole or in part to any university or any other institution for another Degree/Diploma.

Salinda Premadasa
.....

12/08/2014
.....

H. K. Salinda Premadasa

Date

Supervisor's Declaration

I certify that the above statement made by the candidate is true and that this thesis is suitable for submission to the University for the purpose of evaluation

.....

12/08/2014
.....

Professor R. G. N. Meegama
Department of Computer Science
Faculty of Applied Sciences
University of Sri Jayewardenepura

Date

Prof. R.G.N. MEEGAMA
Department of Statistics and
Computer Science
Faculty of Applied Sciences
University of Sri Jayawardenepura
Nugegoda - Sri Lanka.

Supervisor's Declaration

I certify that the candidate has incorporated all corrections, additions and amendments recommended by the examiners.

.....

12/08/2014

.....

Professor R. G. N. Meegama
Department of Computer Science
Faculty of Applied Sciences
University of Sri Jayewardenepura

Date

Prof. R.G.N. MEEGAMA
Department of Statistics and
Computer Science
Faculty of Applied Sciences
University of Sri Jayawardenepura
Nugegoda - Sri Lanka.

ACKNOWLEDGEMENT

First of all, I am deeply grateful to my supervisor Professor R. G. N. Meegama who had been a steady influence throughout my Ph.D. career and have oriented and supported me with promptness and care, and have always been patient and encouraging in times of new ideas and difficulties have listened to my ideas and discussions frequently led to key insights.

Very special thanks to the Faculty of Graduate Studies, University of Sri Jayewardenepura for giving me the opportunity to carry out my doctoral research and for their official support on just-in-time. I also honour that I was appointed as the first PhD student in the discipline of computer science in their university. I would also like to take this opportunity to thank Professor S. Piyasiri-Dean, Faculty of Graduate Studies and Professor Pradeep Jayaweera-Chairman, Board of Studies and other members and my viva examiners, for their very helpful comments and suggestions. I will never forget their support and encouragement.

I warmly thank Mr. Malraj Silva-Director and my colleagues in the Centre for Computer Studies, Sabaragamuwa University of Sri Lanka who have taken an encouragement during the time that I have spent on scientific work.

I owe my deepest gratitude to my foreign colleagues for providing me research articles and sharing the theoretical knowledge. I would especially like to mention R.S. Shaw-Associate Professor, D. Victoria Lopez-Senior Lecturer, Hui-Chun Chu-Assistant Professor, MAO Mao Stephanie-Professor, Luvai Motiwalla-Professor, Silvia Schiaffino-Assistant Professor, Keenan Pituch-Associate Professor, Georgios Kambourakis-Assistant Professor, Yu-Feng Lan-Professor, Francisco Montero-

Professor, Sheng-Wen Hsieh-Assistant Professor, Yong Liu-Professor, Neil Selwyn-Professor, Elena Gaudioso-Associate Professor, Ruimin Shen-Professor, Rinaldi Munir-Assistant Professor and John Traxler-Professor whose example of doing excellent support has definitely encouraged me to undertake this research.

I am also indebted to the students I had the pleasure to work with especially in survey analysis. You have been an invaluable support day in, day out, during all these years. Special thanks to Harsha Harishchandra for his great support and providing a pleasant technical assistance in working atmosphere.

Words cannot express the feelings I have for my parents and my brother for their constant unconditional support in both emotionally and financially. I would not be here if it were not for you. It is amazing to have family close by so far away from home.

Thanks to all of you! This thesis would not have been a reality but your help.

H. K. Salinda Premadasa

University of Sri Jayewardenepura

August, 2014

Demand-based Mobile Learning Network

H. K. Salinda Premadasa

ABSTRACT

With the advent of mobile technology, integrating an open-source secure mobile learning environment, coupled with a Short Messaging Service (SMS) also with message concatenation, into a learning management system (LMS) has been a challenging task in mobile learning platforms during the past few years. Although there are number of services available over the web that facilitates sending secure messages via an LMS, they are often paid services that account for restricted number of messages. Conversely, a major limitation in two-way texting is sending back a part of received data with the reply message. This limitation results in users of a mobile learning environment being unable to reply back to the correct destination as the mobile communication gateway handles sending out information of several users through a single phone number. Nevertheless, the extensive text message is increased the message payload size and it will grounds to convert a standard text message into a concatenated message automatically. Sending bulk concatenated messages in the mobile learning environment is a major drawback when considering the cost per messages. However, SMS is not secure to be used to transport sensitive data because confidentiality and integrity is not available in the SMS. Hence, the assurance cannot be given for its current security mechanism for protection from modification, eavesdropping and man-in-the-middle attacks. The main goal of this thesis is to address the open-source and secure mobile learning environment with short messaging system which facilitate two-way communication with data concealment and extensive message compression mechanism with cryptographic protection that can be easily integrated into an LMS to

provide an interactive learning experience to the user community. Initially, a database is integrated into the Moodle LMS that holds usernames, passwords and enrolment keys for the courses, message information such as recipient's phone number, message body, user data header (UDH) etc. Authenticated students can perform learning activities such as content downloading, group discussions, online quizzes and assignments in the mobile learning environment using their mobile devices. Authenticated teachers can create text messages using a mobile device connected to the Internet. The text message is inserted into the LMS integrated database and SMS Daemon periodically checks and sends it out through the SMS gateway to the recipients. If the message is extensive than 160 characters, it is compressed and given cryptographic protection by the system prior to inserting into the database. The recipients who handle mobile devices decompress such compressed message into an original form of texts to view them. The UDH associated port addressing technique with short messaging service is used to conceal and exchange data relevant to a particular course unit concealed in the message body itself. Subsequently, software installed in the user's mobile device captures this message and sends back the reply message to the appropriate course unit allowing both teachers and students to view messages sent and replies received pertaining to a particular course unit. Statistical results are presented, together with the practical experiences gathered from the interactions with the students. Results indicate that the students' preference in studying with a group while using mobile technologies for their academic activities, system relevance and interoperability of the two-way text messaging with data concealment and educational impact on improving the learning environment by the proposed system. Finally, the message compression ratios, compression time variations for the various types of standard file sizes and message

delivery time with the comparison of standard SMS, illustrate that the relevance of using compression mechanism to mitigating major drawbacks such as cost per message in the mobile learning environment.

Keywords: LMS, SMS, UDH, mobile learning, cryptography, message compression

List of publications

A major part of the research for this thesis has been published in peer-reviewed journals and conferences in the area of computer supported learning, communication technology and mobile learning. Here the list of the papers is given, ordered by publication date.

Published Articles

International Refereed Journals

[1] H. K. S. Premadasa and R. G. N. Meegama, "Mobile Learning Environment with Short Messaging Service: Application to a Campus Environment in a Developing Country," ***Campus Wide Information Systems***, **Emerald Publication**, vol. 30, no. 2, pp. 106-123, March 2013.

National and International Conferences

[2] H.K.S. Premadasa and R.G.N. Meegama, "Extensive Text Message Compression with Security on Android Mobiles," in ***IEEE International Conference on Advances in ICT for Emerging Regions (ICTer)***, Colombo, Sri Lanka, 2013, pp. 80-83.

[3] H. K. S. Premadasa and R. G. N. Meegama, "Implementation of Concatenated Short Messaging System in a Campus Environment," in ***IEEE 8th International Conference on Computer Science & Education (ICCSE)***, Colombo, Sri Lanka, 2013, pp. 207-212.

[4] H. K. S. Premadasa and R. G. N. Meegama, "Transmission of Concealed Data in Short Messaging System," in ***National Conference on Technology & Management, Sri Lanka Institute of Information Technology (SLIIT)***, Colombo, Sri Lanka, 2013, pp. 120-124.

[5] H. K. S. Premadasa and R. G. N Meegama, "Concealed Data in Two Way Text Messaging: A Framework for Interactive Mobile Learning Environment," in ***IEEE International Conference on Advances in ICT for Emerging Regions (ICTer)*** , Colombo, Sri lanka, 2012, pp. 122-127.

[6] H. K. S. Premadasa and R. G. N. Meegama, "Mobile Learning Environment with Short Messaging System," in ***National Conference on Technology & Management, Sri Lanka Institute of Information Technology (SLIIT)***, Colombo, Sri Lanka, 2012, pp. 95-99.

TABLE OF CONTENTS

INTRODUCTION **1**

1.1 MOBILE DEVICES FOR DELIVERING LEARNING MATERIALS 2
1.2 SMS IN MOBILE LEARNING ARENA 3
1.3 TWO-WAY SMS COMMUNICATION 5
1.4 COMPRESSION AND COMMUNICATION SECURITY IN SMS 7
1.5 PROBLEM STATEMENT 11
1.6 RESEARCH MOTIVATION 12
1.7 THESIS ORGANIZATION 18

LITERATURE REVIEW **22**

DEFINING MOBILE LEARNING **28**

3.1 THE MOBILE LEARNING STATE OF THE ART 30
3.2 SCOPE OF THE SHORT MESSAGING SERVICE IN MOBILE LEARNING 35

MOBILE LEARNING ENVIRONMENT WITH SHORT MESSAGING SERVICE **39**

4.1 THEORETICAL FRAMEWORK 39
4.2 SYSTEM FUNCTION AND ARCHITECTURE 41
4.3 METHODOLOGY 46
4.4 RESULTS AND DISCUSSION 48
4.4.1 Pre-survey results *48*
4.4.2 Post-survey results *51*
4.4.3 Suitability of SMS system for academic notifications *52*
4.4.4 Reliability of the mobile learning environment *53*

CONCEALED DATA IN TWO-WAY TEXT MESSAGING: SMS BASED ASSIGNMENT SYSTEM AND NEWS FORUM **57**

5.1 THEORETICAL FRAMEWORK 57
5.1.1 SMS-SUBMIT Protocol Description Unit (PDU) *58*
5.1.2 SMS-DELIVER Protocol Description Unit (PDU) *59*
5.1.3 User Data Header (UDH) *60*
5.1.4 Port number addressing *62*
5.2 SYSTEM FUNCTION AND ARCHITECTURE 63
5.2.1 SMS-based assignment system *63*
5.2.1 SMS-based news forum *67*
5.3 METHODOLOGY 71
5.4 RESULTS AND DISCUSSIONS 73
5.4.1 Educational Impact of the proposed system *73*
5.4.2 User friendliness, technical feasibility and cost effectiveness *76*

CONCATENATED SHORT MESSAGING SERVICE FOR ACADEMIC AND ADMINISTRATIVE ACTIVITIES **84**

6.1 THEORETICAL FRAMEWORK 84
6.2 SYSTEM FUNCTION AND ARCHITECTURE 86
6.3 METHODOLOGY 88
6.4 RESULTS AND DISCUSSION 90
6.4.1 Pre-survey results: Existing methods of academic and administrative activities and mobile phone usage *90*
6.4.2 Post-survey results: Suitability of the proposed system to obtaining academic and administrative information *91*

EXTENSIVE TEXT MESSAGE COMPRESSION WITH CRYPTOGRAPHIC PROTECTION **93**

7.1 THEORETICAL FRAMEWORK 93
7.1.1 Advanced Encryption Standard (AES) *94*
7.1.2 Initialization Vector (IV), Secret Key and (S_k) and Cipher Feed Back (CFB) mode *95*
7.1.3 Message Digest-5 algorithm (MD5) *96*
7.2 SYSTEM FUNCTION AND ARCHITECTURE 100
7.3 RESULTS AND DISCUSSION 103
7.3.1 Message Response Time *105*
7.3.2 Compression Performance *106*

CONCLUSION AND FUTURE WORK **110**

BIBLIOGRAPHY **115**

APPENDIX A: **132**

SERVER IMPLEMENTATION 132