TalkOut : Protecting Mental Health Application With A Lightweight Message Encryption

GAVIN TEO JUEN

FACULTY OF COMPUTING AND INFORMATICS
UNIVERSITY MALAYSIA SABAH
2022

TalkOut : Protecting Mental Health Application With A Lightweight Message Encryption

GAVIN TEO JUEN

THESIS SUBMITTED IN PARTIAL FULFILLMENT FOR THE DEGREE OF BACHELOR OF COMPUTER SCIENCE WITH HONOURS (NETWORK ENGINEERING)

FACULTY OF COMPUTING AND INFORMATICS
UNIVERSITY MALAYSIA SABAH
2022

NAME **:** GAVIN TEO JUEN

MATRIC NUMBER **:** BI18110239

TITLE : TalkOut: Protecting Mental Health Application With A Lightweight Message Encryption

DEGREE **:** BACHELOR OF COMPUTER WITH HONOURS (NETWORK ENGINEERING)

VIVA'S DATE **:** 25th January 2022

CERTIFIED BY;

1. **SUPERVISOR** Signature

Dr. Tan Soo Fun

DR TAN SOO FUN
SENIOR LECTURER
FACULTY OF COMPUTING AND INFORMATICS
UNIVERSITI MALAYSIA SABAH

DECLARATION

I hereby declare that the material in this thesis is my own except for quotations, equations, summaries and references, which have been duly acknowledged.

25th JANUARY 2022

GAVIN TEO JUEN
BI18110239

ACKNOWLEDGEMENT

I would like to express my gratitude and appreciation to my supervisor, Dr Tan Soo Fun who gave me an opportunity to do this wonderful project on the topic TalkOut: Protecting Mental Health Application with A Lightweight Message Encryption, which also helped and provide invaluable guidance to me in doing research and development and I came to know about so many new things. My completion of this project could not have accomplished without the support of my supervisor, friends and family. Lastly, I can't express enough thanks to my caring, loving and supportive parents for their support and encouragement.

GAVIN TEO JUEN
25th January 2022

ABSTRACT

The rise of technology and the Internet has changed how people communicate in society and virtual counselling development since the 1970s. It offers an effective way to seek psychotherapy and consultation services without physically presented by exploiting accessibility, ease of use, comfort and convenience of Internet features. However, the increased security breaches of recent mental health applications that leaked the patient's profile. This project proposed a virtual mental health mobile application, called TalkOut, with a lightweight message encryption algorithm to protect patient's profile, conversation messages and treatment history. The project objectives includes:(i) To investigate lightweight message encryption algorithms by benchmarking their efficiency in terms of computation speed and generated cipher text size; (ii) To design and develop the TalkOut mobile application with lightweight message encryption by using prototype software development model.; and (iii) To evaluate the usability performance of the developed proposed TalkOut mobile application using System Usability Scale (SUS) approach. Questionnaire and interview methods is used to gather user's requirement from campus students and campus counsellors. The investigation of lightweight message encryption algorithms is conducted with systematic quantitative literature and experiment implementation in Java and Android running environment. The outcome of this project provides an alternative for campus students to seek psychotherapy and consultation services and sharing platform, especially during distance online learning and covid-19 pandemic.

ABSTRAK

TalkOut : Melindungi Aplikasi Kesihatan Mental Dengan Penyulitan Mesej Ringan

Kebangkitan teknologi dan Internet telah mengubah cara orang berkomunikasi dalam masyarakat dan pembangunan kaunseling maya sejak 1970-an. Ia menawarkan cara yang berkesan untuk mendapatkan perkhidmatan psikoterapi dan perundingan tanpa dibentangkan secara fizikal dengan mengeksploitasi kebolehcapaian, kemudahan penggunaan, keselesaan dan kemudahan ciri Internet. Walau bagaimanapun, peningkatan pelanggaran keselamatan aplikasi kesihatan mental baru-baru ini yang membocorkan profil pesakit. Projek ini mencadangkan aplikasi mudah alih kesihatan mental maya, dipanggil TalkOut, dengan algoritma penyulitan mesej ringan untuk melindungi profil pesakit, mesej perbualan dan sejarah rawatan. Objektif projek termasuk:(i) Untuk menyiasat algoritma penyulitan mesej ringan dengan menanda aras kecekapannya dari segi kelajuan pengiraan dan saiz teks sifir yang dijana; (ii) Untuk mereka bentuk dan membangunkan aplikasi mudah alih TalkOut dengan penyulitan mesej ringan dengan menggunakan model pembangunan perisian prototaip.; dan (iii) Untuk menilai prestasi kebolehgunaan aplikasi mudah alih TalkOut yang dicadangkan dibangunkan menggunakan pendekatan Skala Kebolehgunaan Sistem (SUS). Kaedah soal selidik dan temu bual digunakan untuk mengumpul keperluan pengguna daripada pelajar kampus dan kaunselor kampus. Penyiasatan algoritma penyulitan mesej ringan dijalankan dengan literatur kuantitatif sistematik dan pelaksanaan eksperimen dalam persekitaran berjalan Java dan Android. Hasil projek ini memberi alternatif kepada pelajar kampus untuk mendapatkan perkhidmatan psikoterapi dan perundingan dan platform perkongsian, terutamanya semasa pembelajaran dalam talian jarak jauh dan pandemik covid-19.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

Psychotherapy sessions traditionally performed face-to-face; since the emergence of the Internet, virtual psychotherapy became an alternative approach to virtually providing mental health consultation services. People began to express their feelings and experiences with mental health issues through videos and text on social media sites as communication technologies progressed. Virtual counselling has become popular among youth as it brings convenience and comfort from the Internet environment rather than face to face (Gibson & Cartwright, 2014). Cell phone and text messaging are secure and practical for young people in youth advocacy programmes to maintain contact and coordinate meetings with mental health practitioners (Furber *et al*., 2011). Online counselling is one way to deliver counselling services over the Internet, either synchronous mode (chat) or asynchronous mode (forum). The individual conversation is often used to provide mental health services, and online counselling's effectiveness is encouraging (Dowling & Rickwood, 2013).

The COVID-19 pandemic of 2020 has compelled mental health counsellors to consider new approaches to offer counsel to their patients/clients. If the pandemic progresses, ongoing and necessary public health efforts expose a growing number of people to situations that are related to poor mental health outcomes, such as loneliness and job loss.

The application and emergence of technology in mental health therapy have become essential to meet patients' needs. The mobile application, TalkOut, allows the campus graduates to seek psychotherapy treatment and consultation services remotely and a platform to share their difficulties and challenges and encourage each other privately. Users can set the conversation's tempo and address topics that they would be hesitant to say out loud in the real world. Chat apps provided many advantages, including increased social support, positive words, and knowledge to improve health and well-being.

1.2 Problem Background/Motivation

Many individuals hesitate to seek face-to-face counselling as they are not comfortable with it. An individual associated with mental health is often discouraged from seeking professional help, especially in Asian countries (Heflinger & Hinshaw, 2010). Studies found that Asians are not comfortable revealing their feelings and are less likely to acknowledge their problems than Western people (Youssef *et al.,* 2014; Haroz *et al.,* 2017). With the ongoing COVID-19 pandemic, many of those seeking counselling help cannot meet their counsellors face-to-face. The need for access to psychotherapy sessions and counselling services increased by 124% since the outbreak does not allow people to meet their therapist and counsellors. According to Islamic University Malaysia (IIUM,2020), it has shown a rising trend in students seeking counselling during the Movement Control Order (MCO) period. The lack of expressing feelings and emotions would lead to depression and, worst-case scenario, suicide. Simultaneously, there is growing concern about the leak of privacy resulting from mental health apps and instant messaging services.

For instance, a healthcare services application called HealthEngine was recently found to be sharing patient's information with attorneyship to identify patient for personal injury (McGrath *et al.*, 2018) without getting patient's consent. Loss of privacy can have a significant result on patients.

As indicated by Parker *et al.* (2019), 41 % of mental health apps did not inform users how their personal information would be retained if shared with third parties. The study shows that the app industry did not comply with the rules and regulation and did not protect mental health application users' privacy. The common problem with mental health applications is the manipulation of user's personal information that is collected. User's personal information collected from the apps can be used and shared with other parties, which is rarely disclosed to users (Hess, 2019). Besides that, the growth of data is the result of the development of the various application. Data must be secured and stored to ensure confidentiality, privacy, and integrity from preventing attackers from hacking.

Besides that, recent campuses including Universiti Malaysia Sabah (UMS), still practice traditional face-to-face counselling sessions. Without alternative virtual counselling services, it is harder to provide dedicated counselling services for students who may need emotional and psychological support from professional counsellors, especially during distance online learning and the COVID-19 pandemic. The lack of integration of online counselling causes students unable to receive the help that is not responsive to their needs. Web-based counselling services may have advantages in providing counselling services that help counsellors and effective communication with patients. However, previous developed final year projects are insufficient and inadequate to adapt to the real world to support UMS campus counselling activities.

1.3 Problem Statements

The main problem statements are summarized as below:

i. Leakage of User's Privacy on recent Mental Health and Instant Messaging apps

Three hundred million messages were left exposed online in WeChat instant messaging application (Liao, 2019). Personal information such as citizen identity numbers, address, and GPS location on the type of device was being used. Users are worried their personal information would be leaked through messaging apps. Most of the mental health applications are often associated with sharing data, including patient's personal information such as treatment history and suicidal thoughts, according to Herzog (2020), who discovered that recent Talkspace and BetterHelp, apps that provide users with online mental health counselling, share data with third parties.

ii. Insecure of Chat Message history

WhatsApp messaging app that is widely used in facilitating the Mental Health Application communication provides end to end encryption to the users when communicating. However, data storage's message security does not guarantee the messages free from third-party attacks, allowing the third party to read all the data storage messages (Siahaan *et al.,* 2018). Thus, it does not secure the message all the time. On the other hand, WeChat also does not provide end-to-end encryption to encrypt user messages but used symmetric AES encryption. However, with the lack of end-to-end encryption, there is a high chance of accessing the server's message by a third party (Grigg, 2018).

The proposed TalkOut mobile application will implement end-to-end encryption, and encrypted messages are stored on application servers that are more secure and decryption key only available from user's devices only to avoid data breaching the application server is hacked.

iii. Lack of lightweight Message Encryption Algorithm

Most instant messaging apps such as Whatsapp and Telegram used conventional cryptography, such as the RSA algorithm and Advanced Encryption Standard (AES) algorithm (Abiodun *et al.*,2020). Several studies had mentioned that virtual communication such as Whatsapp and Telegram was considered a growing communication tool to conduct online counselling, and counsellors make use of both chat applications in providing guidance and counselling activities to students (Wulz *et al.*,2018; Srivastava *et al.*,2020). Both studies showed a positive result on the usage of Whatsapp and Telegram in the aspect of online counselling. The recent algorithms used in instant messaging apps such as Whatsapp and Telegram are AES and RSA, considered conventional cryptography. The limitation of the RSA algorithm is it has a greater computational overhead due to its large key size, which causes high complexity and slower computation speed. James & Kumar (2016) stated that the conventional AES algorithm produced more time delayed in mixed columns and substitution bytes. The drawback of conventional algorithms in proposing lightweight encryption algorithms in this project in terms of computation speed and generated cipher text as conventional algorithms is not relevant for lower computing resources and resource-constrained devices.

Optimization in terms of performance, security and resource requirements makes those conventional algorithms challenging to implement in resource constraint devices resulted in investigating the performance issues in the proposed lightweight encryption algorithm. It can hinder the performance of mobile devices. A lightweight message encryption algorithm provides confidentiality in a lightweight environment such as a mobile device.

1.4 Project Objectives

In this study, the main objectives of this project are listed as follows:

i. To investigate lightweight message encryption algorithms by benchmarking their efficiency in terms of computation speed and generated ciphertext size.
ii. To design and develop the TalkOut mobile application with lightweight message encryption by using prototype software development model.
iii. To evaluate the usability performance of the developed TalkOut mobile application using the System Usability Scale (SUS) approach.

1.5 Project Scope

TalkOut mobile application's target users are campus students and counsellor, includes JFPIU, consisted of Department, Faculty, Centre, and Institute and Unit. Considered the time and cost feasibility, this project further scoped and targeted to cope with a consultation scenario in the counsellor department, Universiti Malaysia Sabah (UMS). This project's research embedded elements are aimed to protect the patient's data and conversation with a lightweight message encryption algorithm.