CYBERGUARD - APLIKASI PENGESAN PEMBULIAN SIBER MUDAH ALIH

Kevin Choo Tze Herng
Tan Siok Yee

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Media sosial merupakan sesuatu yang digunakan oleh ramai orang di Malaysia pada setiap hari terutamanya dalam golongan remaja. Media sosial merupakan satu jenis platform interaksi di mana pengguna dari mana-mana tempat di dunia boleh berinteraksi antara satu sama lain dan ia terdapat dalam pelbagai jenis seperti berinteraksi menggunakan forum seperti Facebook dan Twitter. Namun begitu, disebabkan oleh kemudahan yang disediakan, seseorang boleh menghantar mesej kepada seseorang melalui media sosial dengan sekelip mata. Terdapat pelbagai kes pembulian atas talian dan sekarang dinamakan sebagai pembulian siber. Pembulian siber berlaku di mana seseorang membuli dan menganggu pengguna yang lain melalui pembulian seperti menghantar mesej yang mengganggukan seperti gangguan mental atau gangguan seksual. Pembulian siber merupakan sesuatu yang membahayakan dan akan menganggu emosi seseorang terutamanya kepada golongan muda kerana mereka tidak mengetahui mereka telah mengalami pembulian siber dan tidak mengetahui cara untuk mengatasi masalah ini. Oleh hal yang demikian, satu aplikasi berasaskan Android yang dinamakan sebagai Cyberguard - Aplikasi Pengesan Pembulian Siber Muda Alih telah dibangunkan untuk mengatasi masalah ini. Tujuan pembangunan aplikasi ini adalah untuk membolehkan pengguna untuk mengetahui sama ada mereka telah mengalami pembulian siber. Aplikasi ini akan menunjukkan perkataan amaran kepada pengguna apabila terdapat perkataan yang berunsurkan negatif dalam mesej media sosial (Twitter) mereka. Aplikasi ini juga akan menerangkan makna perkataan yang diberi amaran dan memberikan kategori bagi perkataan tersebut. Untuk pengguna yang telah mengalami pembulian siber, aplikasi ini juga akan memberikan nasihat dan cara untuk mereka mengatasi masalah pembulian siber tersebut. Aplikasi ini dibangunkan dengan menghubungkan profil pengguna Twitter dengan aplikasi supaya aplikasi boleh mengekstrak mesej pengguna dari mesej Twitter dan memberi amaran tentang potensi kes pembulian siber yang sedang berlaku pada mereka. Aplikasi ini adalah penting kepada semua golongan terutamanya remaja sekarang supaya mereka boleh mengetahui mereka telah mengalami pembulian siber dan cara untuk mengatasinya. Aplikasi ini telah diuji oleh 15 orang pengguna dan aplikasi telah mendapat maklum balas yang baik daripada pengguna tersebut.

1 PENGENALAN

Media sosial merupakan media atas talian yang digunakan oleh pengguna untuk mudah menyertai, mencipta isi, meliputi blog, rangkaian sosial dan sebagainya. Media sosial terdapat dalam pelbagai jenis dan bentuk yang boleh digunakan dalam pelbagai cara oleh pengguna berdasarkan keperluan atau kemahuan mereka. Akibat daripada penggunaan komputer dan

teknologi maklumat yang semakin diperluaskan dalam kehidupan seharian, manusia telah menggunakan teknologi tersebut sebagai sebahagian kehidupan mereka. Media sosial juga diperluaskan melalui peningkatan penggunaan teknologi komputer dan semakin mudah digunakan sampai tahap budak sekolah juga mengetahui cara menggunakan media sosial dalam komputer dari umur yang kecil.

Namun begitu, walaupun media sosial adalah sesuatu yang boleh diguna oleh setiap orang, ramai tidak mengetahui bahawa media sosial juga boleh menjadi satu medium dalam pembulian. Kes pembulian ini dikenali sebagai pembulian siber di mana kes buli atau gangguan ini dilakukan dengan menggunakan alat-alat elektronik seperti telefon bimbit, komputer dan tablet. Kes pembulian siber boleh dilakukan dalam pelbagai cara seperti melalui mesej teks atau melalui aplikasi media sosial seperti Facebook atau Twitter.

Pembulian siber merupakan satu kebimbangan yang besar kepada rakyat Malaysia terutamanya dalam golongan remaja kerana mereka adalah pengguna yang paling banyak menggunakan media sosial (Ismail 2014) dan yang paling mudah terdedah kepada kes pembulian siber (Vaillancourt et al. 2017). Kes pembulian siber juga amat bahaya kerana pembulian jenis ini adalah sesuatu yang mudah menjejaskan kehidupan seseorang kerana kebanyakan pembulian siber akan sentiasa berterusan jika seseorang tidak mengambil langkah untuk menyelesaikannya (Peebles 2014).

2 PENYATAAN MASALAH

Pada masa kini, penggunaan media sosial merupakan sesuatu yang digunakan oleh banyak pengguna terutamanya dalam golongan remaja (Ismail 2014). Penggunaan media sosial ini merupakan sesuatu yang mudah diguna dan terdapat dalam pelbagai jenis seperti Facebook, Twitter dan sebagainya. Namun begitu, disebabkan oleh kemudahan penggunaannya, pengguna juga mudah didedahkan dalam pembulian siber kerana pembuli dapat menghantar mesej yang boleh mengejek dan memalukan kepadapengguna. Ini merupakan satu perkara yang boleh menyerang fikiran mental seseorang akibat daripada menerima mesej-mesej yang berunsurkan buruk tersebut.

Selain itu, masalah pembulian siber juga boleh menyebabkan masalah yang lebih besar sekiranya pengguna media sosial tidak mengetahui tentang unsur-unsur pembulian siber. Ini

akan menyebabkan masalah kerana jika seseorang tidak mengetahui bahawa mereka sedang dibuli, mereka tidak berasa mereka memerlukan bantuan untuk menyelesaikan masalah tersebut dan tidak akan mencari orang lain yang untuk membantu mereka semasa kejadian pembulian siber sedang berlaku.

Akhir sekali juga adalah masalah pengguna terutamanya golongan muda yang tidak mengetahui apa yang perlu dilakukan semasa kejadian ini berlaku kerana mereka tidak pernah mengalami perkara ini dalam kehidupan mereka. Ini boleh juga membawa masalah yang besar terutamanya pada pemikran mental pengguna sekiranya pengguna tidak memastikan apakah jenis pembulian siber yang sedang menyerang mereka dan apa yang boleh dibuat untuk menyelesaikan masalah tersebut.

3 OBJEKTIF KAJIAN

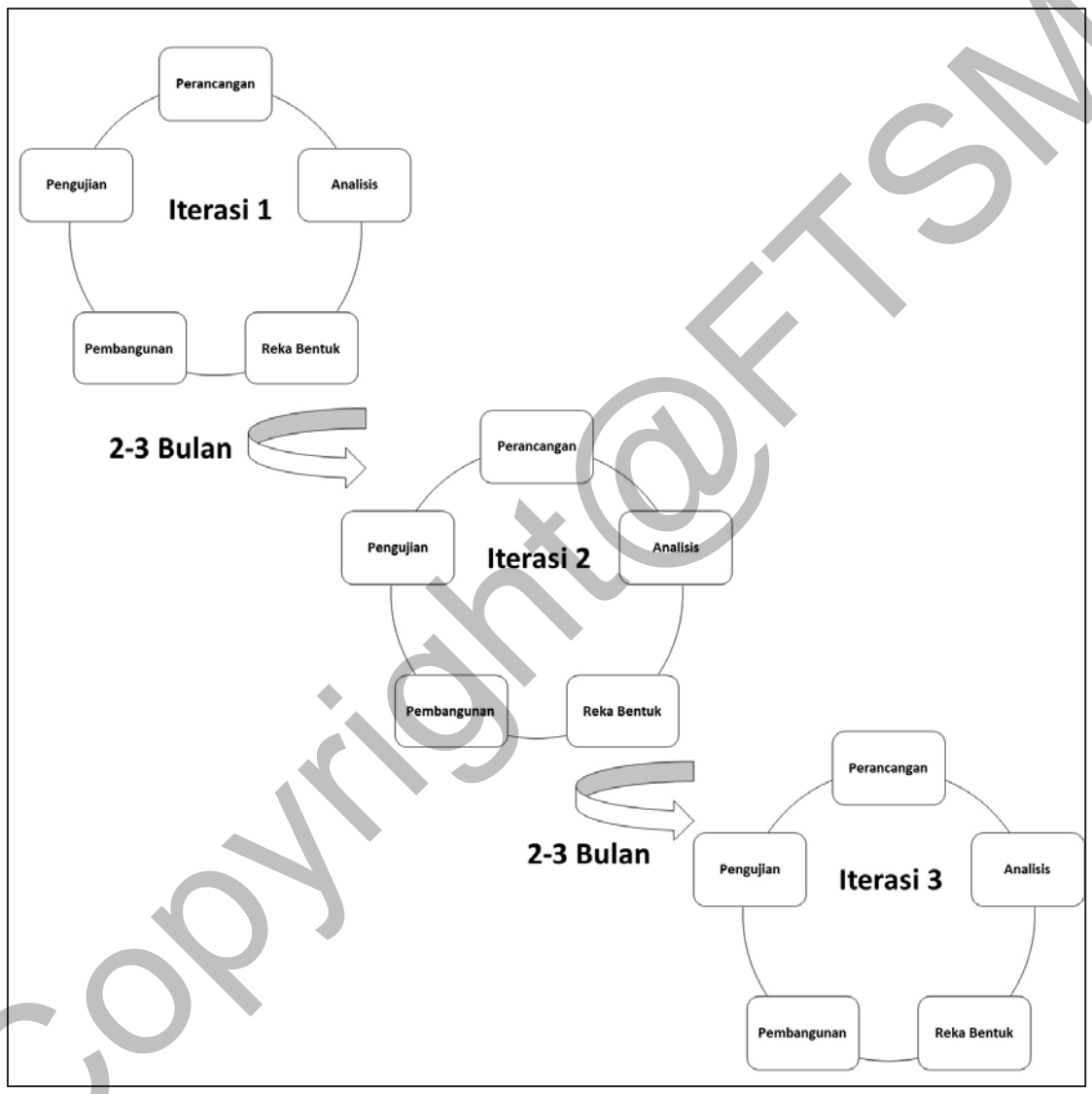
Objektif utama projek ini adalah untuk membangunkan satu aplikasi pengesanan pembulian siber mudah alih. Oleh itu, terdapat dua objektif yang digariskan untuk memastikan kelancaran dan kecekapan projek ini. Objektif pertama untuk projek ini adalah untuk membangunkan aplikasi pengesanan pembulian siber mudah alih yang mempunyai fungsi pengesanan yang berlaku dalam sosial media Twitter, fungsi kategori pembulian dan fungsi cara mengatasi pembulian siber tersebut.

Selain itu, projek ini juga dibuat untuk menjalankan penilaian atas aplikasi mudah alih dalam kalangan remaja untuk menguji kebolehgunaan aplikasi pengujian aplikasi dengan percubaan.

4 METOD KAJIAN

Dalam kajian ini, model pembangunan apliksai yang digunakan adalah model Agile. Model Agile merupakan combinasi model proses berulang dan tambahan yang memberikan fokus kepada proses penyesuaian dan kepuasan pelanggan dengan penghantaran produk perisian yang berfungsi (Kendall&Kendall 2010). Model Agile digunakan kerana model ini membolehkan adaptasi dan penukaran kepada aplikasi dibuat dengan kerap mengikut keperluan pengguna. Model Agile mempunyai 5 fasa iaitu Fasa Perancangan, Fasa Analisis, Fasa Reka Bentuk, Fasa Pembangunan dan Fasa Pengujian (Balaji&Murugaiyan 2012).

Model Agile digunakan untuk projek ini kerana maklum balas daripada pengguna juga boleh didapati secara cepat untuk memudahkan penukaran yang boleh dibuat berdasarkan maklum balas atau pembaikian apabila terdapat isu dalam aplikasi. Rajah 1 menunjukkan rajah untuk aliran model Agile.



Rajah 1 Rajah Aliran Model Agile

4.1 Fasa Perancangan

Dalam fasa ini, perancangan akan dibuat untuk mengenal pasti skop untuk masalah yang berlaku dan untuk mengenal pasti apa penyelesaian yang boleh dilakukan bagi masalah yang dibincangkan. Untuk aplikasi *Cyberguard*, perancangan yang akan dibuat adalah mengenal pasti cara untuk membangunkan aplikasi ini supaya aplikasi ini dapat digunakan bersama

profil Twitter pengguna. Anggaran masa dan kos pembangunan untuk aplikasi ini juga akan dibincangkan dalam fasa ini.

4.2 Fasa Analisis

Dalam fasa analisis, keperluan yang diperlukan untuk membangunkan aplikasi *Cyberguard* akan dibincangkan. Dalam fasa ini, kajian akan dibuat pada aplikasi mudah alih yang sedia ada bagi merekodkan kebaikan dan keburukan aplikasi sedia ada. Fungsi yang ada pada aplikasi mudah alih yang sedia ada akan dipilih dan digunakan dalam pembangunan aplikasi *Cyberguard*. Peningkatan fungsi daripada aplikasi sedia ada juga akan dibuat sekiranya terdapat peningkatan yang boleh dibuat.

4.3 Fasa Reka Bentuk

Dalam fasa ini, spesifikasi dan ciri-ciri yang diperlukan untuk pengguna akan dibincangkan dengan terperinci termasuk susun atur skrin dalam aplikasi dan macam mana ia digunakan dalam fungsi. Dengan menggunakan data dan analisis yang dikenal pasti pada fasa sebelumnya sebagai rujukan, reka bentuk awal untuk aplikasi *Cyberguard* akan dibina di mana reka bentuk adalah berasaskan kemudahan pengguna untuk menggunakan aplikasi tersebut. Reka bentuk aplikasi *Cyberguard* akan dibina dahulu dengan model High-Fidelity untuk pengujian dan maklum balas tentang kemudahan menggunakan aplikasi dan apa yang boleh dibuat untuk menambah baikkan aplikasi. Model High-Fidelity merupakan model yang membawa model yang sehampir mungkin ke perwakilan sebenar antara muka aplikasi (Preece 2002). Model High-Fideliti digunakan kerana model ini lebih berkesan untuk mendapat data dan untuk menunjukkan produk sebenar kepada pengguna.

4.4 Fasa Pembangunan

Dalam fasa ini, pembangunan aplikasi akan dilakukan di mana aplikasi yang sebenar akan dibuat. Pembinaan fungsi aplikasi akan dibuat melalui pengekodan untuk aplikasi di mana aturcara untuk fungsi-fungsi dan antara muka pengguna akan dibuat berdasarkan reka bentuk yang dibina pada fasa sebelumnya. Dalam fasa ini, aplikasi *Cyberguard* akan dibangunkan dengan menggunakan Android Studio untuk membina aplikasi di mana aplikasi *Cyberguard* akan dapat mendapat digunakan dengan media sosial Twitter dengan menghubungkan aplikasi dengan Twitter API. Selepas itu pengguna juga akan dapat menggunakan aplikasi *Cyberguard* untuk melihat mesej yang mempunyai unsur pembulian siber. Pengguna kemudian boleh

melihat deskripsi ayat pembulian siber yang telah dikesan dan juga boleh mendapatkan nasihat untuk menyelesaikan kes pembulian siber mereka berdasarkan kepada perkataan yang dikesan.

4.5 Fasa Pengujian

Fasa Pengujian dan Penilaian adalah fasa terakhir dalam *Software Development Life Cycle* sebelum aplikasi akan diberikan kepada pelanggan. Dalam fasa ini, aplikasi yang telah dibangunkan akan diuji mengikut keperluan yang diperlukan. Fasa ini bertujuan untuk mencari kecacatan yang mungkin ada pada aplikasi dan juga memastikan aplikasi berfungsi seperti yang dirangkakan. Bagi aplikasi *Cyberguard*, aplikasi akan diuji dengan membuat pengujian dengan 15 orang remaja yang berumur 15 tahun ke atas dan 30 tahun ke bawah yang dipilih secara rawak untuk menguji fungsi aplikasi tersebut dan memberikan maklum balas tentang aplikasi yang termasuk maklum balas untuk reka bentuk dan fungsi aplikasi. Selepas pengujian tersebut, maklum balas yang didapati akan digunakan untuk membuat peningkatan kepada aplikasi *Cyberguard* sekiranya boleh.

5 HASIL KAJIAN

Bahagian ini membincangkan hasil daripada proses pembangunan aplikasi *Cyberguard.* Untuk pembangunan aplikasi bagi projek ini, beberapa keperluan perisian akan digunakan untuk memudahkan pembangunan projek ini dan memastikan aplikasi tersebut dapat digunakan dengan senang oleh pelbagai pengguna. Antara perisian yang digunakan dalam pembangunan aplikasi ini adalah *Android Studio*, *Firebase*, dan *Android Virtual Device* (AVD).

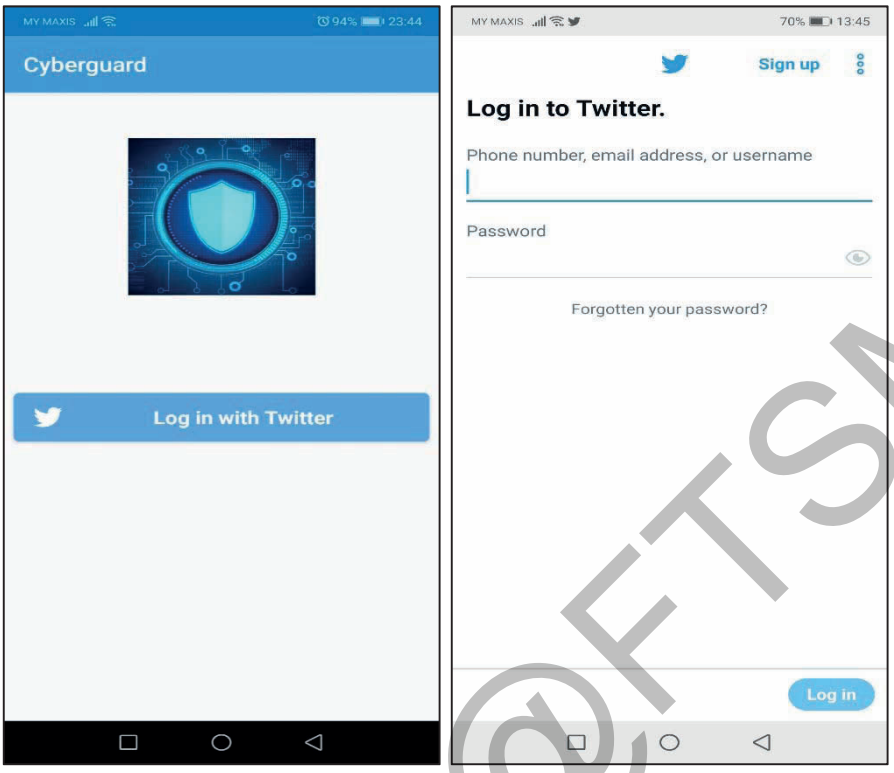
Android Studio merupakan persekitaran pembangunan bersepadu atau *Integrated Development Environment* (IDE) untuk sistem operasi *Android*. *Android Studio* boleh digunakan dalam *Windows*, *macOS* dan *Linux*. *Android Studio* dibina pada perisian *IntelliJ IDEA* dan direka bentuk khususnya untuk pembangunan *Android*. *Firebase* merupakan satu sistem pengurusan pangkalan data relasi atau *Relational Database Management System* (RDBMS). *Firebase* pula adalah pangkalan data sumber terbuka yang menyimpan data dalam fail teks dalam peranti. *Android* biasanya datang dengan implementasi pangkalan data

Firebase. *Firebase* menyokong semua ciri-ciri pangkalan data dan pengguna tidak perlu menubuhkan sebarang jenis sambungan. *Android Virtual D evice* (AVD) adalah konfigurasi peranti yang dijalankan dengan *Android Emulator* . Ia digunakan dengan emulator untuk menghasilkan persekitaran khusus peranti maya untuk memasang dan menjalankan aplikasi *Android*.

Untuk tujuan pembangunan aplikasi bagi projek ini, spesifikasi keperluan perkakasan perlu diambil kira untuk memastikan perkakasan komputer adalah cukup untuk membangunkan aplikasi ini tanpa masalah. Bagi membangunkan aplikasi ini, spesifikasi keperluan perkakasan yang diperlukan adalah computer dan telefon pintar. Bagi komputer yang digunakan, Sistem pengoperasian komputer yang digunakan adalah Windows 10 Profesional dengan pemproses Intel(R) Core TM i7-6700HQ CPU @ 2.60GHz. Komputer yang digunakan juga mempunyai ingatan capaian rawak (RAM) yang mempunyai saiz 8GB dan ruang cakera yang mempunyai saiz 4GB. Sistem untuk komputer yang digunakan adalah sistem pengoperasian 64-bit atau dikenali sebagai x64. Komputer yang digunakan juga mempunyai resolusi skrin 1200x800. Telefon pintar yang digunakan semasa pembangunan aplikasi ini adalah telefon pintar yang mempunyai sistem pengoperasian *Android Nougat, 7.0* dan mempunyai memori dalaman sebanyak 16GB.

Dalam pembangunan aplikasi ini, pembinaan reka bentuk antara muka adalah sesuatu yang penting dilakukan kerana reka bentuk antara muka merupakan salah satu faktor penarikan untuk penggunaan aplikasi ini oleh pelanggan. Sekiranya reka bentuk aplikasi adalah tidak menarik atau tidak senang untuk digunakan, aplikasi yang telah dibina tidak akan digunakan oleh orang yang ramai. Oleh itu, aplikasi harus dibina di mana pengguna boleh menavigasi aplikasi dengan mudah dan cepat untuk menyelesaikan masalah mereka dengan interaksi yang minimum. Bagi pembinaan aplikasi *Cyberguard*, aplikasi akan dibina dan dibangunkan berasaskan reka bentuk antara muka seperti yang ditunjukkan.

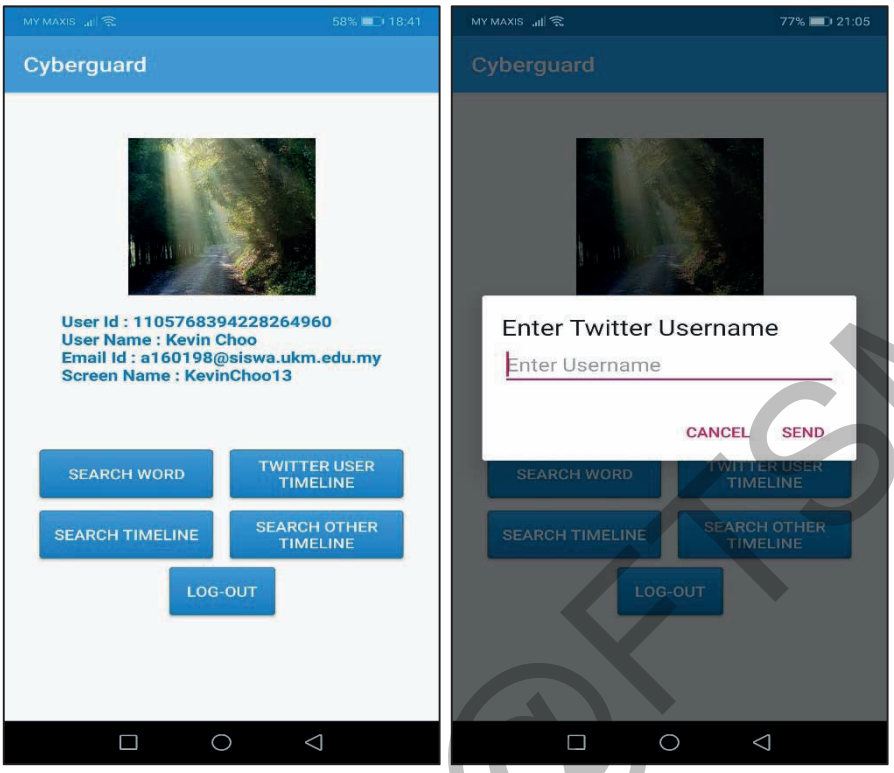
Rajah 2 menunjukkan antara muka bagi halaman skrin permulaan untuk aplikasi *Cyberguard*.



Rajah 2 Antara Muka Halaman Skrin Permulaan

Aplikasi akan bermula dengan halaman ini dan hanya mempunyai 1 fungsi yang boleh dibuat oleh pengguna. Sekiranya pengguna menekan butang '*Log in with Twitte r*', pengguna akan dapat mengakses aplikasi *Twitter* untuk log masuk dan membuat pengesahan. Selepas pengguna telah log masuk profil *Twitter*, pengguna akan diarahkan ke halaman skrin selepas log masuk.

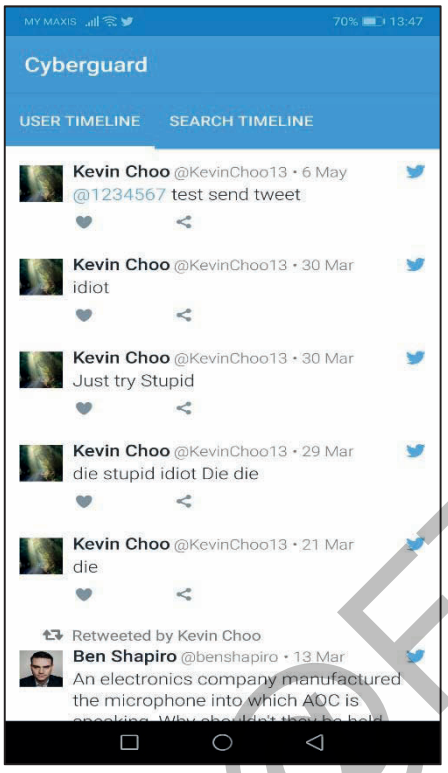
Rajah 3 menunjukkan antara muka untuk halaman skrin bagi aplikasi *Cyberguard* selepas pengguna telah log masuk ke profil *Twitter*.



Rajah 3 Antara Muka Halaman Skrin Selepas Log Masuk

Dalam halaman ini, pengguna boleh melihat id pengguna, nama pengguna, e-mel pengguna dan nama skrin pengguna. Antara muka ini juga mempunyai 4 butang untuk mengarahkan pengguna ke halaman seterusnya. Sekiranya pengguna menekan butang '*Search Word'*, pengguna akan diarahkan kepada halaman Pencarian Perkataan. Jika pengguna menekan butang '*Twitter User Timeline*', pengguna akan diarahkan kepada halaman Garis Masa Pengguna. Jika pengguna menekan butang '*Search Timeline*', pengguna akan diarahkan kepada halaman Pencarian Garis Masa dengan nama skrin pengguna. Jika pengguna menekan butang '*Search Other Timeline*' pula, satu kotak dialog akan dibuka untuk memasukkan nama skrin pengguna lain. Apabila nama skrin telah diisi dan dihantar, pengguna akan diarahkan kepada halaman Pencarian Garis Masa dengan nama skrin yang telah diiisi. Jika pengguna menekan butang '*Log-Out*', pengguna akan log keluar daripada aplikasi dan akan diarahkan semula kepada halaman skrin permulaan.

Rajah 4.5 menunjukkan antara muka untuk halaman Garis Masa Pengguna.



Rajah 4 Antara Muka Halaman Garis Masa Pengguna

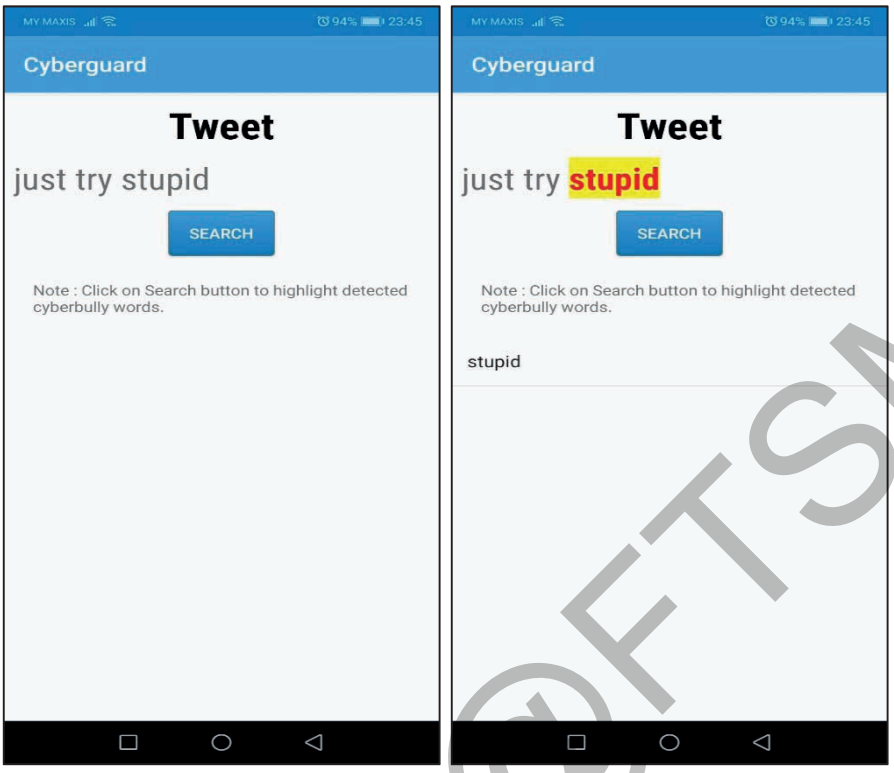
Dalam halaman ini, pengguna boleh melihat garis masa pengguna untuk profil sendiri. Halaman ini akan menunjukkan *Tweet* yang telah dipos oleh pengguna dan juga *Retweet* yang dibuat oleh pengguna. Jika pengguna menekan *Tweet* di halaman ini, pengguna akan dihantar ke dalam aplikasi *Twitter* utama.

Rajah 5 menunjukkan antara muka untuk halaman Pencarian Garis Masa.

Rajah 5 Antara Muka Halaman Pencarian Garis Masa

Dalam halaman ini, nama skrin pengguna atau nama skrin yang diiisi oleh pengguna akan ditunjukkan di atas. Halaman ini akan menyenaraikan 200 *Tweet* yang terbaru yang telah diposkan dalam profil *Twitter* pengguna. Satu penapis juga disediakan dalam halaman ini untuk memudahkan pengguna untuk mencari *Tweet* yang mungkin mengandungi unsur pembulian siber. Dalam halaman ini, jika pengguna menekan salah satu *Tweet* yang terdapat dalam senarai, pengguna akan diarahkan kepada halaman Senarai Perkataan Amaran dan ayat yang dipilih akan ditunjukkan dalam halaman seterusnya.

Rajah 6 menunjukkan antara muka untuk halaman Senarai Perkataan Amaran.



Rajah 6 Antara Muka Halaman Senarai Perkataan Amaran

Dalam antara muka ini, halaman akan menunjukkan *Tweet* yang telah dipilih daripada halaman Pencarian Garis Masa. Sekiranya pengguna menekan butang '*Search*', aplikasi akan mewarnakan perkataan amaran untuk menunjukkan perkataan tersebut dikesan sebagai perkataan amaran. Perkataan tersebut juga akan dimasukkan dalam senarai di bawah butang. Jika pengguna menekan perkataan dalam senarai tersebut, pengguna akan diarahkan kepada halaman Butiran Perkataan Amaran untuk melihat butiran perkataan berdasarkan perkataan yang dipilih. Jika *Tweet* yang dipilih oleh pengguna tidak mempunyai perkataan amaran yang boleh dikesan oleh aplikasi, satu mesej *Toast* yang berkata bahawa tiada perkataan kunci yang dikesan di dalam *Tweet* atau "*No bullying keywords detected in Tweet*" akan ditunjukkan.

Rajah 7 menunjukkan antara muka untuk halaman Pencarian Perkataan.

Rajah 7 Antara Muka Halaman Pencarian Perkataan

Dalam halaman ini, satu senarai untuk perkataan amaran yang terdapat dalam aplikasi *Cyberguard* akan ditunjukkan. Sekiranya pengguna menekan salah satu perkataan dalam senarai, pengguna akan dapat melihat butiran tentang perkataan amaran yang dipilih di halaman Butiran Perkataan Amaran. Halaman ini juga mempunyai satu penapis untuk memudahkan pengguna mencari perkataan dalam senarai tersebut.

Rajah 8 menunjukkan antara muka untuk halaman butiran perkataan amaran.

Rajah 8 Antara Muka Halaman Butiran Perkataan Amaran

Selepas menekan pada perkataan yang dipilih dalam halaman senarai perkataan amaran atau halaman pencarian perkataan, perkataan tersebut akan dipilih sebagai kata kunci yang ditunjukkan dan kemudiannya, deskripsi untuk perkataan tersebut akan ditunjukkan bersama dengan kategori dan sub-kategori berdasarkan perkataan tersebut. Aplikasi juga akan menunjukkan nasihat bagi perkataan amaran tersebut.

Deskripsi bagi setiap perkataan yang terdapat dalam pangkalan data diambil oleh kamus web untuk memberikan makna perkataan (Thinkmap 2016). Perkataan amaran tersebut pula akan dikategorikan berdasarkan penyelidikan yang dibuat untuk menkategorikan perkataan berunsur pembulian siber (Golbeck et al. 2017). Dalam penyelidikan tersebut, perkataan akan dibahagikan kepada kategori yang terdiri daripada kategori gangguan, berpontesi menyinggung perasaan dan tidak mengganggu. Selepas itu, perkataan amaran juga akan dibahagikan kepada sub-kategori gangguan ditujukan dan gangguan yang umum. Bagi sub-kategori gangguan langsung, perkataan yang berunsur pembulian siber tersebut merupakan perkataan amaran yang ditujukan kepada seseorang untuk pembulian. Sub-kategori gangguan yang umum pula

merupakan sub-kategori untuk perkataan amaran yang berunsur negatif yang tidak ditujukan kepada sesiapa dan merupakan perkataan berunsur pembulian siber yang umum.

6 KESIMPULAN

Secara keseluruhannya, dokumen yang telah dibuat adalah untuk menunjukkan masalah yang dihadapi oleh seseorang dan cadangan aplikasi yang boleh dibangunkan untuk menghadapinya. Dalam dokumen ini, aplikasi *Cyberguard* akan dibangunkan untuk membuat aplikasi yang senang digunakan oleh seseorang untuk menangani masalah pembulian siber.

Dokumen yang dibuat mempunyai kajian literasi yang dibuat untuk membuat perbandingan dengan aplikasi yang sedia ada untuk mengenali apakah kekuatan dan kelemahan bagi aplikasi yang sedia ada sebagai tanda rujuk pembangunan aplikasi *Cyberguard*. Spesifikasi sistem dan reka bentuk sistem juga dibuat untuk memastikan pembangunan aplikasi dapat dibuat dengan baik dan lancar.

Untuk projek ini, kejayaan yang dibuat setakat ini adalah sistem dan reka bentuk aplikasi telah dikenal pasti dan prototaip aplikasi telah siap dibina dengan reka bentuk atur cara.

7 RUJUKAN

Balaji, S. & Murugaiyan, M. S. 2012. Waterfall Vs. V-Model Vs. Agile: A Comparative Study on Sdlc. *International Journal of Informati on Technology and Business Management* 2(1): 26-30.

Golbeck, J., Ashktorab, Z., Banjo, R. O., Berlinger, A., Bhagwan, S., Buntain, C., Cheakalos, P., Geller, A. A., Gergory, Q., Gnanasekaran, R. K., Gunasekaran, R. R., Hoffman, K. M., Hottle, J., Jienjitlert, V., Khare, S., Lau, R., Martindale, M. J., Naik, S., Nixon, H. L., Ramachandran, P., Rogers, K. M., Rogers, L., Sarin, M. S., Shahane, G., Thanki, J., Vengataraman, P., Wan, Z. & Wu, D. M. 2017. A Large Labeled Corpus for Online Harassment Research. Proceedings of the 2017 ACM on Web Science Conference. Anjuran ACM. Troy, New York, USA, Huscher, B. 2000. Database Design and Modeling Fundamentals. [16 November 2018].

Ismail, N. 2014. Young People's Use of New Media through Communities of Practice.

Peebles, E. 2014. Cyberbullying: Hiding Behind the Screen. *Paediatrics & child health* 19(10): 527-528.

Preece, J., Rogers, Y., and Sharp, H. 2002. Interaction Design: Beyong Human-Computer Interaction.

Thinkmap. 2016. Vocabulary.Com Online Dictionairy. https://www.vocabulary.com/ [9 April 2019].

Vaillancourt, T., Faris, R. & Mishna, F. 2017. Cyberbullying in Children and Youth: Implications for Health and Clinical Practice. *Canadian journal of psychiatry. Revu e canadienne de psychiatrie* 62(6): 368-373.