(Borang JKPTA FTSM UKM 3)

UNIVERSITI KEBANGSAAN MALAYSIA
National University of Malaysia

FAKULTI TEKNOLOGI DAN SAINS MAKLUMAT

BORANG PENYERAHAN LAPORAN ILMIAH

SEM 2 SESI 20 / 21

Bahagian A: Maklumat Diri Pelajar
Part A: Student's Details

No. Matrik *(Matric Number)*	A170859	
Nama *(Name)*	Firzana Binti Mohamed Firoz	
Program pengajian (*Programme*)	Teknologi Maklumat (TM)	
No. Telefon (*Telephone Number*)	0174297237	
Emel (*Email*)	A170859@siswa.ukm.edu.my	

Tajuk Projek (*Project Title*):

Aplikasi Kesedaran Siber Berasaskan Web "CyberRescue"

Tandatangan (*Signature*): _____ Tarikh (*Date*) : 14/7/21

Bahagian B: Perakuan Penyelia
Part B: Supervisor's Approval

Saya peraku laporan ini telah disemak dan dibaiki, dan **menyokong / ~~tidak menyokong~~*** penyerahan laporan ilmiah ini.
*I certify that this report has been reviewed and amended, and **approved / rejected*** the report submission.*

Tandatangan (*Signature*): _____ Tarikh (*Date*) : 14/7/21

Cap Rasmi :

Copyright@FTSM UKM

PROF. MADYA. DR. ZULAIHA ALI OTHMAN
Penyelia
Fakulti Teknologi dan Sains Komputer
Universiti Kebangsaan Malaysia

(Official Stamp)

APLIKASI MUDAH ALIH KESEDARAN SIBER PINTAR "CyberRescue"

Firzana Binti Mohamed Firoz Assoc.
Prof Dr. Zulaiha Ali Othman

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

Copyright@FTSM UKM

ABSTRAK

Dunia kini, semua orang amatlah bergantung kepada teknologi dan sentiasa berada atas talian sepanjang masa. Remaja ialah orang yang sering menggunakan internet kerana ia adalah cara yang paling mudah bagi mereka mengetahui berita semasa yang berlaku di sekeliling mereka dan juga untuk berkomunikasi dengan orang di seluruh dunia. Mereka tidak menyedari bahawa sering kali mereka terlibat dalam tingkah laku yang berisiko tanpa menyedarinya apabila mereka secara tidak sengaja memberikan butiran peribadi mereka kepada orang yang tidak sepatutnya. Laman rangkaian sosial yang popular seperti Facebook boleh mengakibatkan pelbagai risiko keselamatan siber terganggu jika tidak berhati-hati. Untuk mengatasi masalah ini, sebuah aplikasi berasaskan web dibangunkan untuk memberi kesedaran tentang penggunaan siber terhadap remaja. Aplikasi ini menyediakan maklumat berkaitan siber dan tips untuk sentiasa selamat berada atas talian dan mencegah diri daripada terlibat dengan sebarang ancaman jenayah siber. Seterusnya, kajian yang dilakukan oleh pelajar PTA semester lalu telah menghasilkan model risiko siber menggunakan rangkaian neural yang dibangunkan daripada 4500 soal selidik secara asalnya. Kajian tersebut menunjukkan bahawa model rangkaian neural ialah model yang terbaik untuk risiko siber. Oleh itu, tujuan kajian ini adalah untuk membangunkan aplikasi berasaskan web kesedaran siber dengan sistem risiko siber yang membolehkan remaja mengenal pasti sejauhmana tahap risiko penggunaan siber berasaskan perlakuan dan aktiviti mereka di siber. Aplikasi berasaskan web ini dibangunkan menggunakan PHP. Kesimpulannya, diharapkan perkembangan aplikasi berasaskan web ini dapat memberi kesedaran mengenai keselamatan siber melibatkan remaja.

1 PENGENALAN

Dalam era teknologi ini, setiap individu menggunakan Internet untuk melakukan pelbagai aktiviti harian. Internet dilihat sebagai keperluan asas yang penting untuk semua lapisan masyarakat dan juga dalam sektor perniagaan mahupun pendidikan. (Tharek Abdul Rahman, 2020). Terdapat pelbagai kepentingan menggunakan Internet kepada masyarakat. Untuk maklumat segera, masyarakat boleh melayari laman web menggunakan laman sesawang seperti Internet Explorer, Yahoo dan Google. Seterusnya, setiap individu boleh berbual dengan orang lain, tidak kira di mana sahaja mereka berada, di dalam atau di luar negara melalui pelantar media sosial. Bagi individu yang gemar membeli-belah, mereka juga boleh membeli-belah dalam talian untuk menjimatkan

masa. Dengan teknologi ini, ramai orang sering menghabiskan terlalu banyak masa di ruang siber tanpa meragui tahap risiko siber yang mereka hadapi.

Istilah 'Cyber Crime' meliputi pelanggaran yang dilakukan dengan menggunakan sumber web dan alat elektronik apa pun. Ini termasuk menghantar atau menyebarkan program jangkitan, penggodaman dan pemisahan, e-mel spam, phishing dan mendapatkan akses tanpa izin ke komputer lain untuk mencuri maklumat kewangan (Liaqat Ali, 2019). Memang, terdapat begitu banyak kes mengenai jenayah siber hari ini. Justeru, masalah yang membimbangkan ini perlu ditangani dengan serius. Berdasarkan statistik laman web Pasukan Tindak Balas Kecemasan Komputer Malaysia (MyCert), sejumlah 10,699 kes jenayah siber dicatatkan pada tahun 2019 dan jumlahnya meningkat sebanyak 25.6 peratus berbanding tahun sebelumnya, sebanyak 7962 kes. Statistik yang dikeluarkan oleh MyCert juga menunjukkan sembilan kategori jenayah siber termasuk gangguan siber, penolakan perkhidmatan dan pencerobohan.

Sementara itu, jenayah siber dalam kategori penipuan merangkumi penipuan yang mempunyai jumlah tertinggi setiap tahun. (Sinar Harian, 9 Jun 2019).

Terdapat banyak jenis penipuan seperti penipuan membeli-belah dalam talian, penggodaman komputer, penipuan temu janji dan percintaan dan banyak lagi. "Penipuan boleh berlaku kepada siapa saja dari profesional hingga pesara kerajaan, nelayan, petani, pegawai sektor kerajaan dan swasta, termasuk warga tua dan pelajar" (Sinar Harian, 9 Jun 2019). Sehingga hari ini, jenayah siber masih banyak berlaku tetapi kebanyakannya berlaku di kalangan remaja. Ini kerana remaja adalah salah satu pengguna Internet yang paling kerap dan mereka mungkin akan berusaha sepenuhnya dalam talian. Remaja berpendapat bahawa mereka mengetahui banyak perkara mengenai dunia Internet berbanding ibu bapa mereka.

2 PENYATAAN MASALAH

Remaja mudah dipengaruhi oleh apa sahaja yang mereka lihat dalam talian. Sebilangan besar remaja pada masa kini sangat terlibat dengan media sosial. Mereka akan mempercayai apa sahaja yang disiarkan oleh seseorang di platform media sosial daripada berita sebenar. Ini adalah cara

Copyright@FTSM UKM

berita palsu tersebar di luar kawalan kita. Menyiarkan berita palsu dalam talian adalah suatu jenayah dan sebilangan besar remaja tidak mengetahui akibatnya dalam isu ini kerana mereka berpendapat bahawa tindakan yang mereka lakukan dalam talian tidak dapat dilihat oleh orang lain. Remaja dan generasi muda pada masa kini cukup mahir dalam semua butiran yang berkaitan dengan alat yang disambungkan ke Internet tetapi biasanya, sangat bebas untuk berkongsi data melalui Web, memasuki hotspot terbuka atau tidak mengamankan peranti mereka dengan betul.

Oleh itu, perbincangan telah dimulakan mengenai seberapa awal generasi muda harus didedahkan dengan semua idea penting mengenai keselamatan siber. Walau apa pun, menyebarkan maklumat berguna mengenai kesedaran siber kepada remaja sangat penting pada ketika ini. Terdapat pelbagai usaha oleh pemerintah dan juga Badan Bukan Kerajaan (NGO) untuk memulihkan keadaan jenayah siber yang semakin berleluasa. Kerajaan Malaysia dengan sokongan badan korporat dan Badan Bukan Kerajaan (NGO) telah merancang pelbagai kempen kesedaran siber di peringkat nasional sebagai strategi untuk memupuk keprihatinan pengguna terhadap siber. Advokasi program inisiatif dari Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM), "Klik dengan Bijak" telah dibentuk untuk melatih penggunaan rangkaian yang berkesan meliputi aspek keselamatan, kesediaan dan tanggungjawab dalam memerangi masalah penderaan (Zakiah Saizan, 2018). Selanjutnya, Yayasan Pencegahan Jenayah Malaysia (MCPF) telah mengambil tindakan menyebarkan kesedaran siber melalui penerbitan buku panduan berjudul "AWASpada" Ini adalah usaha untuk mendidik pelajar dan remaja agar selalu menggunakan media sosial dan dalam talian permainan. Buku Panduan “AWASpada” bertujuan memberi kesedaran kepada pengguna media sosial dan permainan dalam talian, mengenai kesan negatif jika tidak digunakan dengan bijak. (Berita Harian, 13 Dis 2019).

Sebaliknya, terdapat alat kesedaran siber lain yang digunakan dalam mengatasi masalah keselamatan siber. Penggunaan kecerdasan buatan boleh digunakan untuk mempelajari corak dan mengenal pasti penyimpangan. Kecerdasan buatan juga penting untuk menjimatkan masa kritikal dengan menganalisis sejumlah besar data dengan cepat dan komprehensif. (Liubomir Lazir, 2019). Teknik kecerdasan buatan sudah mempunyai banyak aplikasi dalam mengatasi jenayah siber. Sebagai contoh, jaringan saraf digunakan untuk pengesanan dan pencegahan pencerobohan, tetapi ada juga proposal untuk menggunakan jaringan saraf dalam pengesanan "Denial of Service (DoS),

Copyright@FTSM UKM

pengesanan cacing komputer, pengesanan spam, pengesanan zombie, klasifikasi malware dan penyelidikan forensik" Teknik AI seperti Heuristik, Perlombongan Data, Rangkaian Neural, dan AIS, juga telah diterapkan pada teknologi anti-virus generasi baru.

Seterusnya, ejen pintar adalah kekuatan autonomi yang dihasilkan komputer yang saling berkomunikasi untuk berkongsi data dan bekerjasama antara satu sama lain untuk merancang dan melaksanakan tindak balas yang sesuai sekiranya berlaku kejadian yang tidak dijangka. Mobiliti dan kemampuan menyesuaikan diri dalam lingkungan tempat mereka digunakan, serta sifat kolaboratif mereka, menjadikan teknologi agen pintar sesuai untuk memerangi serangan siber. (Selma Dilek 2015). (Gou et al. 2006) merancang MWDCM sistem multi-agen untuk pengesanan dan pengekalan cacing komputer di rangkaian kawasan metropolitan, yang secara automatik memuat penyebaran cacing yang menyempitkan rangkaian jalur lebar dan menyebabkan kerosakan router. Eksperimen menunjukkan bahawa sistem mereka berkesan menghalang penyebaran cacing walaupun pada kadar jangkitan cacing yang tinggi. (Phillips et al. 2006) mengemukakan sistem gabungan ejen yang diedarkan yang memelihara operasi normal, menerapkan strategi operasi dan keselamatan, menangani kejadian yang tidak dijangka, dan melindungi dari orang dalam yang berniat jahat, kesilapan dan serangan dalam grid kuasa elektrik yang diedarkan. Kajian juga dilakukan dalam mencadangkan model keselamatan siber, model matang keselamatan siber, kesejahteraan digital dan kesejahteraan siber tetapi bukan model risiko siber.

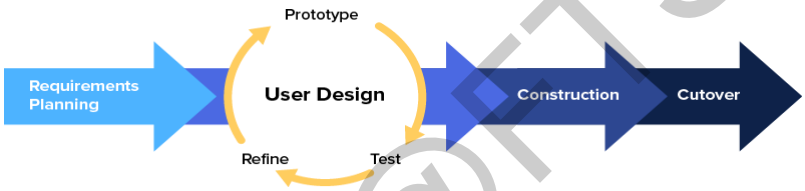
3 OBJEKTIF

Objektif projek adalah untuk membangunkan aplikasi kesedaran siber berasaskan web untuk remaja yang terdiri daripada dua fungsi utama iaitu modul kesedaran siber, yang mengandungi kandungan kesedaran siber dan sistem risiko siber untuk mengenal pasti penggunaan risiko siber untuk remaja. Selain itu, mempelajari asas pembelajaran rangkaian neural kecerdasan buatan.

Copyright@FTSM UKM

4 METOD KAJIAN

Model kitaran hidup pengembangan perisian (SDLC) adalah struktur konseptual yang mewakili semua tugas dari perancangan hingga penyelenggaraan dalam projek pembangunan perisian (Techopedia, 31 Ogos 2020). Pembangunan projek ini dilaksanakan berdasarkan pembentukan fasa yang terdapat dalam kitaran hidup pengembangan sistem (SDLC). Model yang dipilih adalah Model “Rapid Application Development” untuk aplikasi berasasaskan web "CyberRescue".



Rajah 4.1 Model RAD

Sumber : Google image

Pembangunan (RAD) adalah kitaran hidup pembangunan yang dirancang untuk memberikan lebih cepat pembangunan dan hasil berkualiti tinggi daripada yang dicapai dengan tradisional kitaran hidup. Ia dirancang untuk memanfaatkan kelebihan pembangunan yang maksimum perisian yang telah berkembang baru-baru ini. (Daud, Bakar, & Rusli. 2010).

Terdapa beberapa dalam metodologi RAD iaitu fasa perancangan dan analisis, fasa reka bentuk, fasa pembinaan, fasa ujian dan perolehan. Penerangan bagi setiap fasa adalah seperti berikut :

4.1 Fasa Perancangan dan Analisis

Pada fasa ini pelbagai perancangan telah dilakukan. Antaranya ialah tajuk aplikasi yang sesuai dipilih berdasarkan masalah yang perlu diselesaikan dan juga melihat pada data-data yang relevan untuk digunakan pada fasa pembinaan. Pada fasa ini juga, kaedah meniliti pada aplikasi-aplikasi

Copyright@FTSM UKM

yang sedia ada juga dijalankan untuk mendapatkan idea bagi pembangunan projek. Fasa ini menentukan tujuan dan harapan untuk projek.

4.2 Fasa Reka Bentuk

Setelah projek dirancang, fasa reka bentuk menfokuskan kepada membangun reka bentuk sesuai untuk melancarkan proses pembinaan. Fasa ini sangan penting bagi memastikan keperluan pengguna dipenuhi pada setiap langkah dalam proses reka bentuk. Pelbagai perkara perlu dipilih contohnya penggunaan bahasa, perisian yang akan digunakan dan lakaran awal aplikasi yang dilaksanakan. Antara muka aplikasi dan direka bentuk supaya lebih mesra pengguna dan mudah digunakan untuk pengguna. PHP digunakan untuk membangun aplikasi termasuk HTML, CSS, dan JavaScript.

4.3 Fasa Pembinaan

Pada fasa ini, aplikasi sebenar dibina dan pengekodan dilakukan dengan menggunakan semua perancangan yang direka bentuk dan untuk menukar proses dan model data menjadi prototaip sebenar. Sebahagian besar masalah dan perubahan ditangani selama fasa reka bentuk, jadi pada fasa ini pembangun dapat membuat model kerja akhir dengan lebih cepat Fasa ini terbahagi kepada beberapa langkah yang lebih kecil. Antaranya ialah persiapan untuk pembinaan yang cepat, pembangunan program dan pengekodan yang lebih terurus.

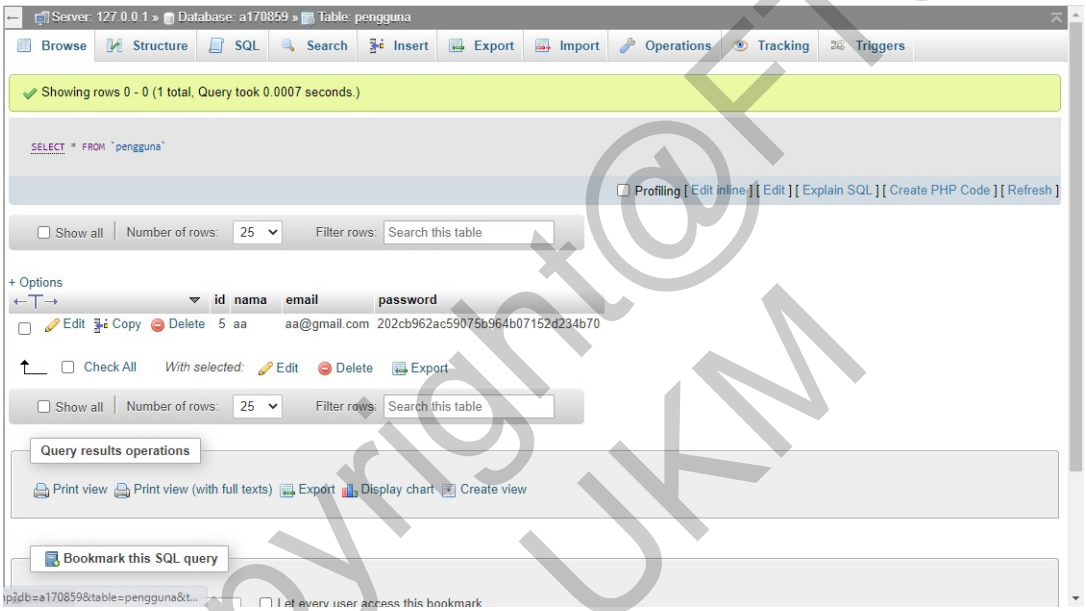
4.4 Fasa Pengujian dan Perolehan

Pada fasa ini, pengujian dilakukan supaya tiada masalah apabila pengguna menggunakan aplikasi. Masa ujian keseluruhan dikurangkan dalam model RAD kerana prototaip diuji secara bebas semasa setiap perolehan. Walau bagaimanapun, aliran data dan antara muka antara semua komponen perlu diuji secara menyeluruh dengan liputan ujian yang lengkap. Oleh kerana sebahagian besar komponen pengaturcaraan telah diuji, ia mengurangkan risiko masalah besar.

Copyright@FTSM UKM

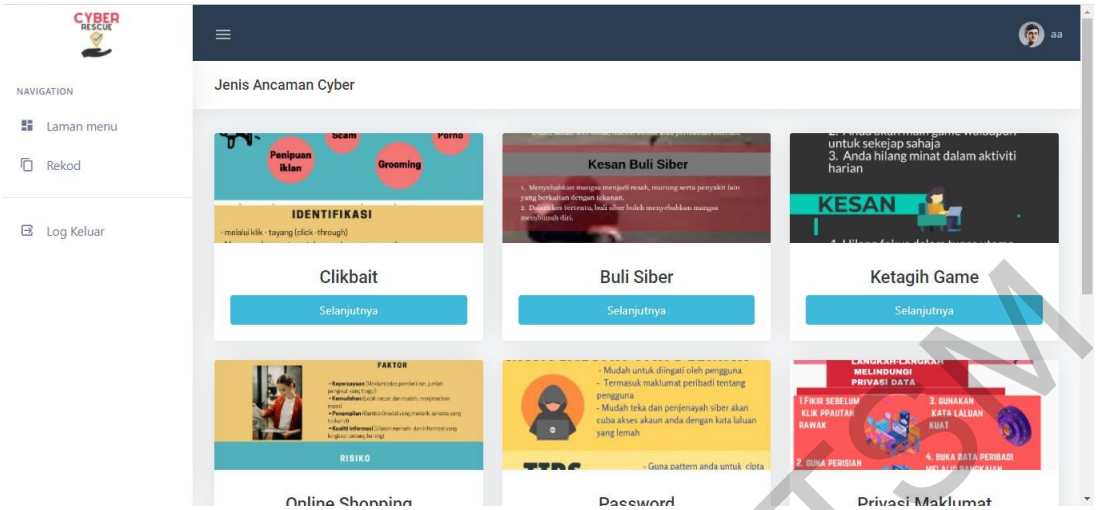
5 Hasil Kajian

Bagi aspek hasil kajian, proses pembangunan perisian yang digunakan ialah xampp, sublime, php admin untuk membangunkan aplikasi dan weka bagi proses perlombongan data model rangkaian neural untuk menguji akurasinya. Bahasa pengaturcaraan yang digunakan dalam pembangunan aplikasi ini ialah html, css, dan juga javascript. Terdapat tiga proses utama yang terlibat dalam pembangunan aplikasi iaitu proses pengujian akurasi di weka, proses antara muka jenis ancaman siber, proses antara muka soalan bagi risiko siber dan pengiraannya.

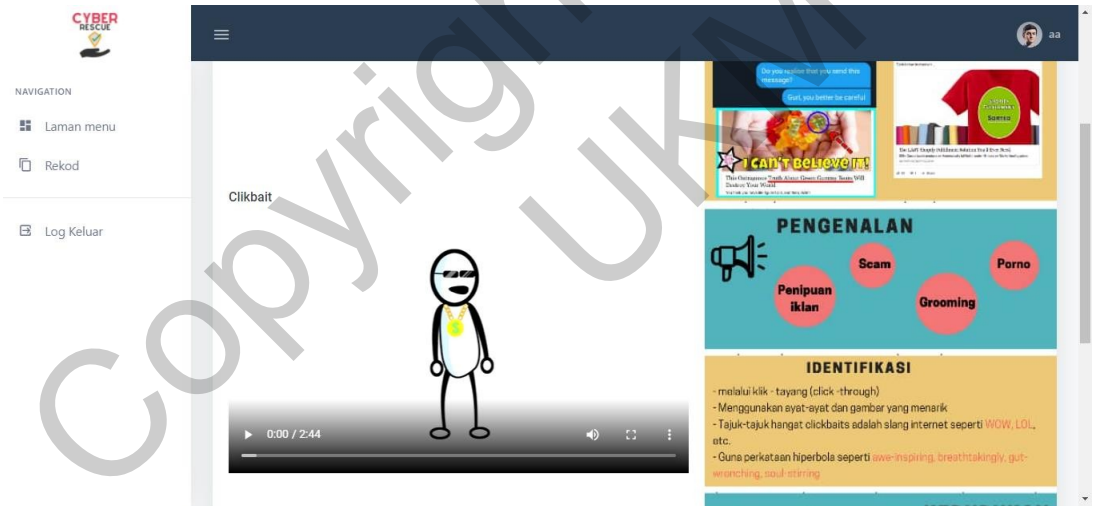


Paparan Pangkalan Data Untuk Menyimpan Data Pengguna

Copyright@FTSM UKM



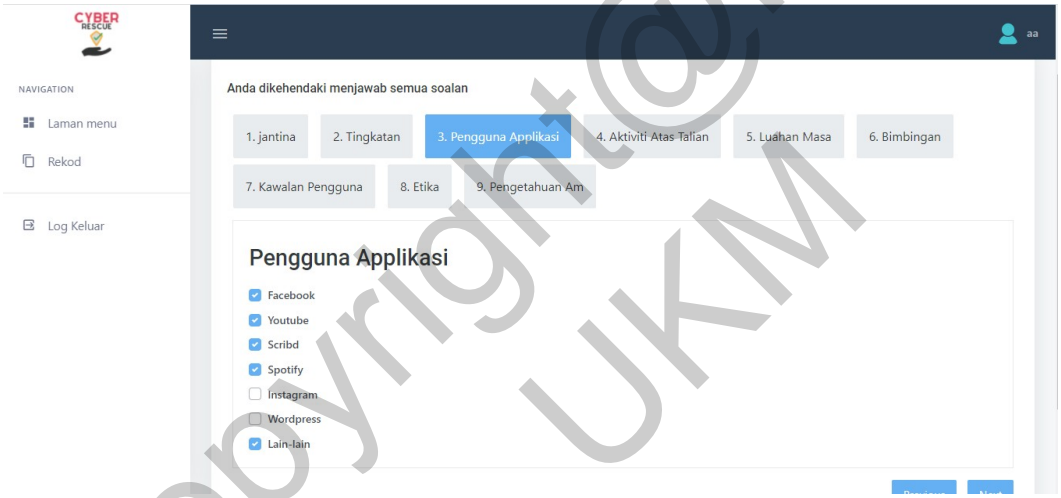
Paparan Antara Muka Jenis Ancaman Siber



Paparan Antara Muka Video Dan Inforgrafik Clickbait

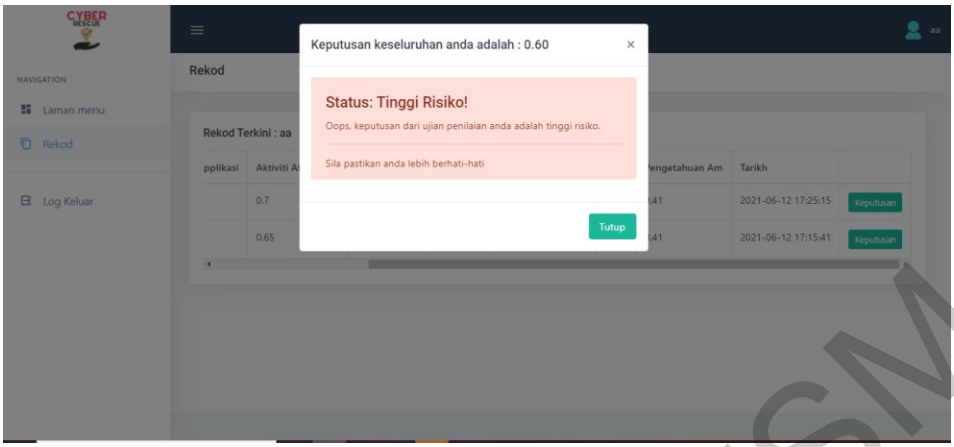
Copyright@FTSM UKM

Paparan Antara Muka Berita & Artikel

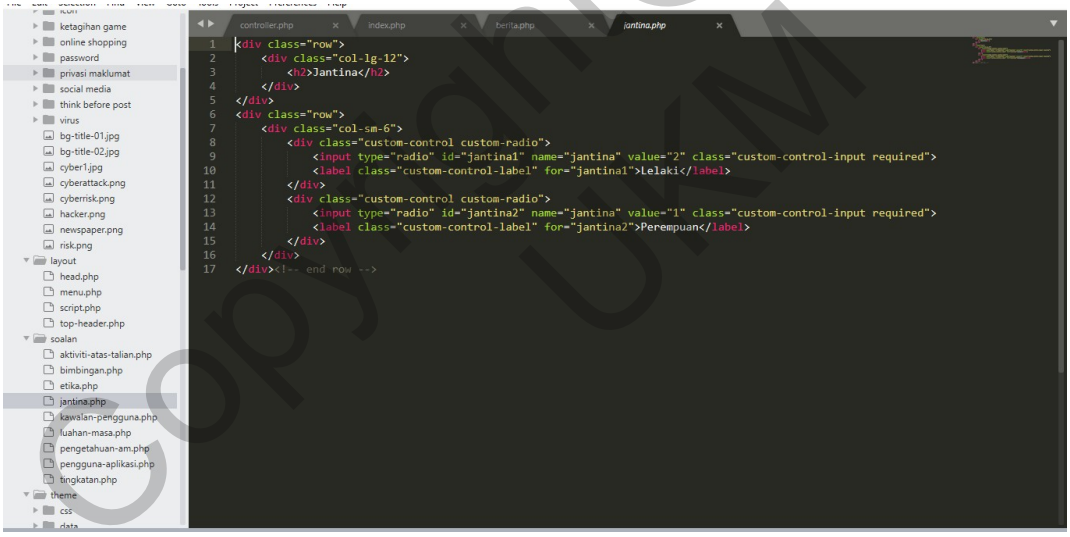


Paparan Antara Muka Penilaian Risiko Bagi Kategori Pengguna Aplikasi

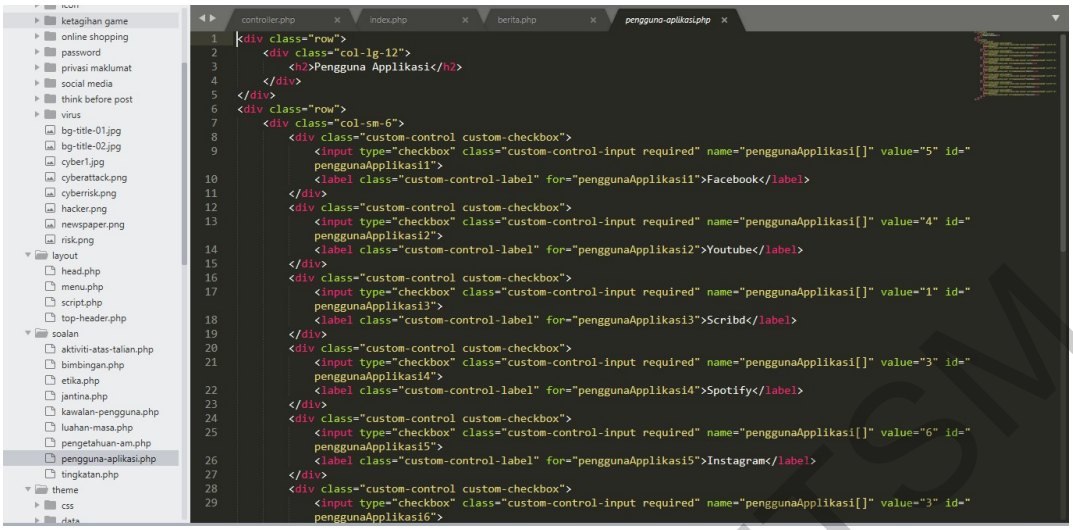
Copyright@FTSM UKM



Paparan Antara Muka Keputusan Penilaian Risiko



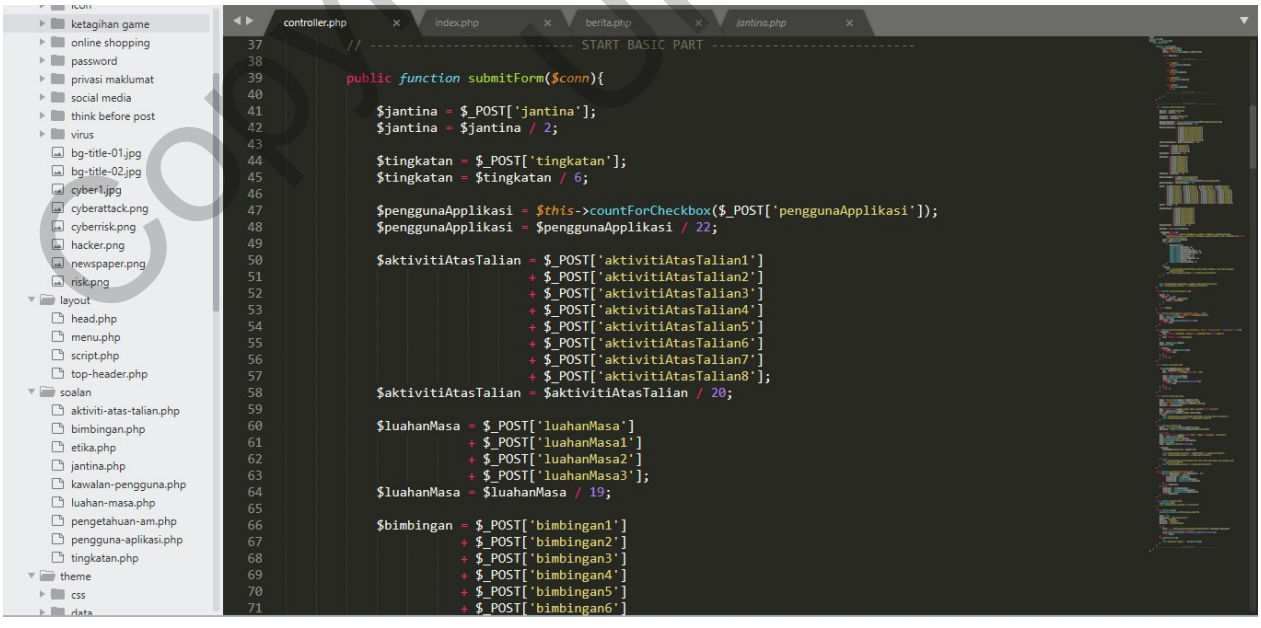
Copyright@FTSM UKM



```
<div class="row">
    <div class="col-lg-12">
        <h2>Pengguna Applikasi</h2>
    </div>
</div>
<div class="row">
    <div class="col-sm-6">
        <div class="custom-control custom-checkbox">
            <input type="checkbox" class="custom-control-input required" name="penggunaApplikasi[]" value="5" id="
            penggunaApplikasi1">
            <label class="custom-control-label" for="penggunaApplikasi1">Facebook</label>
        </div>
        <div class="custom-control custom-checkbox">
            <input type="checkbox" class="custom-control-input required" name="penggunaApplikasi[]" value="4" id="
            penggunaApplikasi2">
            <label class="custom-control-label" for="penggunaApplikasi2">Youtube</label>
        </div>
        <div class="custom-control custom-checkbox">
            <input type="checkbox" class="custom-control-input required" name="penggunaApplikasi[]" value="1" id="
            penggunaApplikasi3">
            <label class="custom-control-label" for="penggunaApplikasi3">Scribd</label>
        </div>
        <div class="custom-control custom-checkbox">
            <input type="checkbox" class="custom-control-input required" name="penggunaApplikasi[]" value="3" id="
            penggunaApplikasi4">
            <label class="custom-control-label" for="penggunaApplikasi4">Spotify</label>
        </div>
        <div class="custom-control custom-checkbox">
            <input type="checkbox" class="custom-control-input required" name="penggunaApplikasi[]" value="6" id="
            penggunaApplikasi5">
            <label class="custom-control-label" for="penggunaApplikasi5">Instagram</label>
        </div>
        <div class="custom-control custom-checkbox">
            <input type="checkbox" class="custom-control-input required" name="penggunaApplikasi[]" value="3" id="
            penggunaApplikasi6">
```

Paparan Kod Segmen Untuk Soalan Risiko Siber

Terdapat dua jenis soalan yang dijawab oleh pengguna. Jenis soalan yang digunakan ialah soalan jenis“multiple choice” dan “checkbox”. Bagi soalan jenis “multiple choice” input type “radio” digunakan manakala bagi jenis soalan “checkbox” input type “checkbox” digunakan



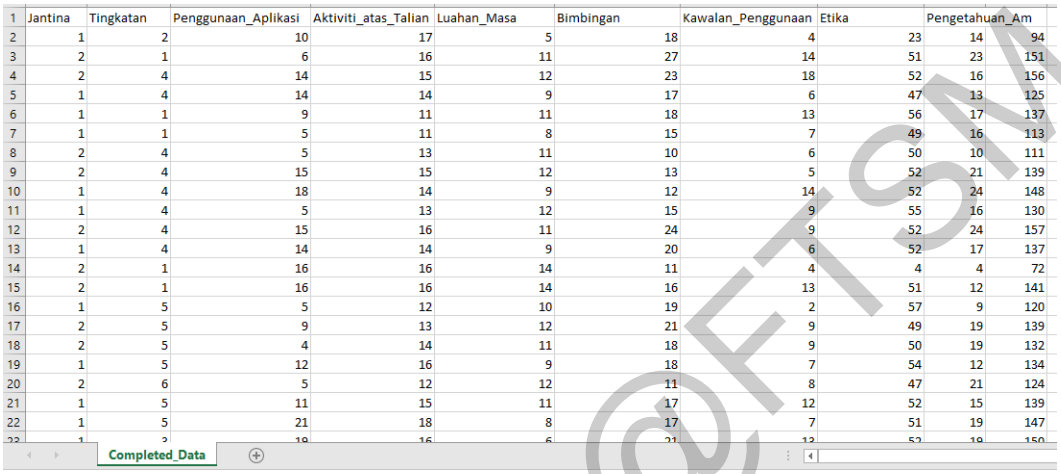
```
// ------------------------- START BASIC PART -------------------------

public function submitForm($conn){

    $jantina = $_POST['jantina'];
    $jantina = $jantina / 2;

    $tingkatan = $_POST['tingkatan'];
    $tingkatan = $tingkatan / 6;

    $penggunaApplikasi = $this->countForCheckbox($_POST['penggunaApplikasi']);
    $penggunaApplikasi = $penggunaApplikasi / 22;

    $aktivitiAtasTalian = $_POST['aktivitiAtasTalian1']
                        + $_POST['aktivitiAtasTalian2']
                        + $_POST['aktivitiAtasTalian3']
                        + $_POST['aktivitiAtasTalian4']
                        + $_POST['aktivitiAtasTalian5']
                        + $_POST['aktivitiAtasTalian6']
                        + $_POST['aktivitiAtasTalian7']
                        + $_POST['aktivitiAtasTalian8'];
    $aktivitiAtasTalian = $aktivitiAtasTalian / 20;

    $luahanMasa = $_POST['luahanMasa']
                + $_POST['luahanMasa1']
                + $_POST['luahanMasa2']
                + $_POST['luahanMasa3'];
    $luahanMasa = $luahanMasa / 19;

    $bimbingan = $_POST['bimbingan1']
               + $_POST['bimbingan2']
               + $_POST['bimbingan3']
               + $_POST['bimbingan4']
               + $_POST['bimbingan5']
               + $_POST['bimbingan6']
```

Paparan Kod Segmen Bagi Pengiraan Markah Soalan

Copyright@FTSM UKM

Kod segmen yang dipaparkan adalah bagi pengiraan markah setiap soalan yang terdiri daripada 9 attribut risiko siber.

MODEL RANGKAIAN NEURAL MENGGUNAKAN WEKA

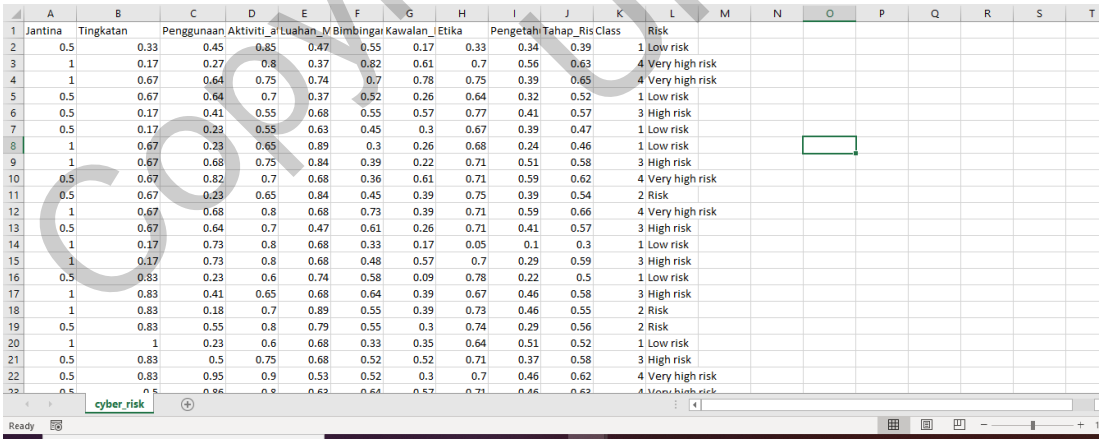


	Jantina	Tingkatan	Penggunaan_Aplikasi	Aktiviti_atas_Talian	Luahan_Masa	Bimbingan	Kawalan_Penggunaan	Etika	Pengetahuan_Am	
2	1	2	10	17	5	18	4	23	14	94
3	2	1	6	16	11	27	14	51	23	151
4	2	4	14	15	12	23	18	52	16	156
5	1	4	14	14	9	17	6	47	13	125
6	1	1	9	11	11	18	13	56	17	137
7	1	1	5	11	8	15	7	49	16	113
8	2	4	5	13	11	10	6	50	10	111
9	2	4	15	15	12	13	5	52	21	139
10	1	4	18	14	9	12	14	52	24	148
11	1	4	5	13	12	15	9	55	16	130
12	2	4	15	16	11	24	9	52	24	157
13	1	4	14	14	9	20	6	52	17	137
14	2	1	16	16	14	11	4	4	4	72
15	2	1	16	16	14	16	13	51	12	141
16	1	5	5	12	10	19	2	57	9	120
17	2	5	9	13	12	21	9	49	19	139
18	2	5	4	14	11	18	9	50	19	132
19	1	5	12	16	9	18	7	54	12	134
20	2	6	5	12	12	11	8	47	21	124
21	1	5	11	15	11	17	12	52	15	139
22	1	5	21	18	8	17	7	51	19	147

Completed_Data

Data Asal

Data asal ini digunakan dan kemudian dialihkan pada dokumen excel baharu dan semua attribute diubah dalam bentuk perpuluhan.



	A	B	C	D	E	F	G	H	I	J	K	L
1	Jantina	Tingkatan	Penggunaan	Aktiviti_a	Luahan_M	Bimbingar	Kawalan_I	Etika	Pengetahı	Tahap_Ris	Class	Risk
2	0.5	0.33	0.45	0.85	0.47	0.55	0.17	0.33	0.34	0.39	1	Low risk
3	1	0.17	0.27	0.8	0.37	0.82	0.61	0.7	0.56	0.63	4	Very high risk
4	1	0.67	0.64	0.75	0.74	0.7	0.78	0.75	0.39	0.65	4	Very high risk
5	0.5	0.67	0.64	0.7	0.37	0.52	0.26	0.64	0.32	0.52	1	Low risk
6	0.5	0.17	0.41	0.55	0.68	0.55	0.57	0.77	0.41	0.57	3	High risk
7	0.5	0.17	0.23	0.55	0.63	0.45	0.3	0.67	0.39	0.47	1	Low risk
8	1	0.67	0.23	0.65	0.89	0.3	0.26	0.68	0.24	0.46	1	Low risk
9	1	0.67	0.68	0.75	0.84	0.39	0.22	0.71	0.51	0.58	3	High risk
10	0.5	0.67	0.82	0.7	0.68	0.36	0.61	0.71	0.59	0.62	4	Very high risk
11	0.5	0.67	0.23	0.65	0.84	0.45	0.39	0.75	0.39	0.54	2	Risk
12	1	0.67	0.68	0.8	0.68	0.73	0.39	0.71	0.59	0.66	4	Very high risk
13	0.5	0.67	0.64	0.7	0.47	0.61	0.26	0.71	0.41	0.57	3	High risk
14	1	0.17	0.73	0.8	0.68	0.33	0.17	0.05	0.1	0.3	1	Low risk
15	1	0.17	0.73	0.8	0.68	0.48	0.57	0.7	0.29	0.59	3	High risk
16	0.5	0.83	0.23	0.6	0.74	0.58	0.09	0.78	0.22	0.5	1	Low risk
17	1	0.83	0.41	0.65	0.68	0.64	0.39	0.67	0.46	0.58	3	High risk
18	1	0.83	0.18	0.7	0.89	0.55	0.39	0.73	0.46	0.55	2	Risk
19	0.5	0.83	0.55	0.8	0.79	0.55	0.3	0.74	0.29	0.56	2	Risk
20	1	1	0.23	0.6	0.68	0.33	0.35	0.64	0.51	0.52	1	Low risk
21	0.5	0.83	0.5	0.75	0.68	0.52	0.52	0.71	0.37	0.58	3	High risk
22	0.5	0.83	0.95	0.9	0.53	0.52	0.3	0.7	0.46	0.62	4	Very high risk

cyber_risk

Ready

Data Yang Dibuat Perubahan

Copyright@FTSM UKM

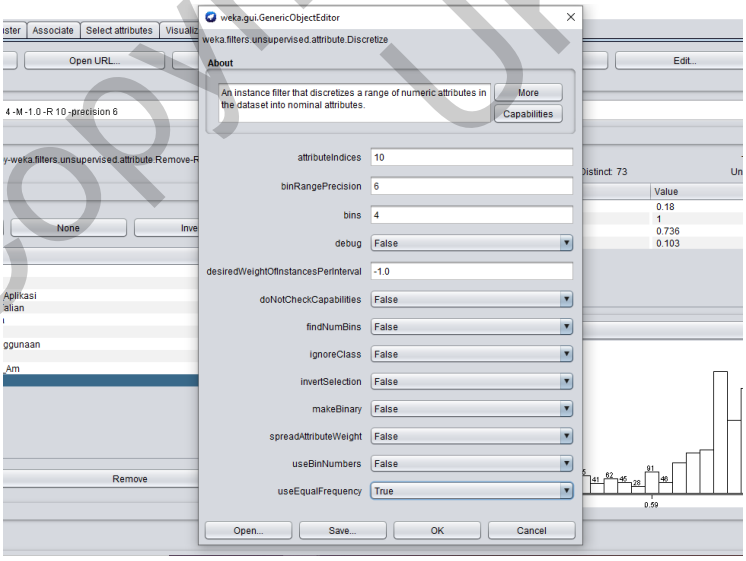
Dua eksperimen dijalankan dengan menggunakan data risiko siber yang telah dikategorikan menjadi 9 attribut. Eksperimen pertama dijalankan dengan tidak menggunakan kaedah “discretize” pada attribute tahap risiko. Eksperimen yang kedua dijalankan dengan menggunakan kaedah “discretize” pada attribute tahap risiko dan juga kaedah “equal frequency” digunakan. Eksperimen ini dijalankan menggunakan Weka. Akurasi yang didapati dalam dua eksperimen ini dipaparkan dalam jadual.

Paparan Keputusan Eksperimen Pertama

Name Algorithm	Accuracy	RMSE	ROC Area	Precision	Recall	F-Measure
Neural Network	96.12	0.07	1.00	0.938	1.00	0.963

Paparan Keputusan Eksperimen Kedua

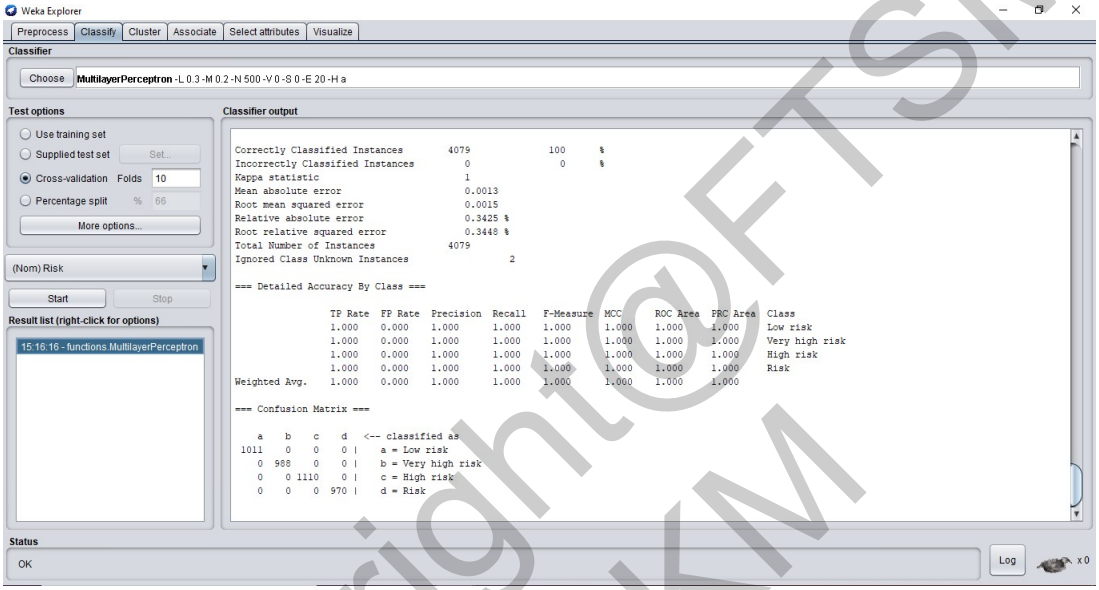
Name Algorithm	Accuracy	RMSE	ROC Area	Precision	Recall	F-Measure
Neural Network	100	0.0015	1.00	1.00	1.00	1.00



Paparan Tetapan Yang Digunakan Pada Weka

Copyright@FTSM UKM

Rajah di atas menunjukkan tetapan penuh yang digunakan pada Weka. Tetapan yang digunakan ialah “attributesindices” yang diletakkan 10, “binRangePrecision” yang diletakkan 6, dan “bins” yang diletakkan 4, “useEqualFrequency” diletakkan sebagai “true”. Kaedah “cross validation folds 10” digunakan bagi mendapat keputusan. Penggunaan tetapan ini telah dilakukan untuk mendapat akurasi 100% bagi model rangkaian neural seperti yang ditunjukkan di dalam rajah 4.12.



Model Rangkaian Neural Setelah Selesai “cross validation folds 10

6 Kesimpulan

Secara kesimpulannya, aplikasi kesedaran siber "CyberRescue" ini telah dibangunkan dan telah memenuhi objektif yang telah ditetapkan pada awal fasa pembangunan yang telah dibincang Pembangunan aplikasi kesedaran siber ini merupakan aplikasi yang membenarkan pengguna mengetahui tentang ancaman siber yang berlaku pada sekeliling mereka dan juga mengetahui tahap risiko siber mereka. Walaupun aplikasi ini mempunyai beberapa kelebihan, namun aplikasi ini juga terdapat beberapa kelemahan yang perlu diperbaiki. Oleh itu, kajian yang mendalam terhadap aplikasi ini harus diteruskan untuk meningkatkan kualiti dan kecanggihan aplikasi ini.

Copyright@FTSM UKM

Bagi, aspek kelebihan dan kekurangan aplikasi yang dapat dikesan pula. Antaranya ialah aplikasi ini mempunyai maklumat tentang siber secara ringkas dan menarik dalam bentuk infografik dan video. Selain itu, pengguna boleh mengetahui tahap risiko siber mereka pada bila bila masa sahaja dengan mengambil penilaian yang ada pada aplikasi "CyberRescue". Aplikasi bukan sahaja boleh digunakan oleh para pelajar sekolah, malah ibu bapa juga boleh menggunakannya dan menyuruh anak mereka untuk menjawab penilaian yang disediakan.

Seterusnya bagi kekurangan aplikasi pula, maklumat yang terdapat dalam web ini adalah terhad. Tidak ada banyak contoh- contoh tentang jenis ancaman siber. Selain itu, aplikasi ini secara keseluruhan tidak terlalu menarik.

Cadangan penambahbaikan diperlukan untuk memastikan pembangunan aplikasi yang akan dijalankan kelak adalah lebih baik dan sempurna. Antara cadangan penambahbaikan adalah seperti berikut :

i. **Menambah maklumat yang lebih luas tentang ancaman siber atau apa-apa yang dapat membantu memperluaskan kesedaran siber dalam masyarakat.**

ii. **Bagi reka bentuk aplikasi, keputusan risiko siber terus dipaparkan setelah menjawab semua soalan tanpa perlu klik pada butang keputusan.**

iii. **Menambah fungsian aplikasi seperti memasukkan permainan tentang keselamatan siber dan ruangan mesej untuk berhubung dengan agensi-agensi yang berkaitan untuk mengetahui lebih mendalam tentang risiko siber.**

7 Rujukan

Berita Harian Online. 2019. Disember 19. Kesejahteraan siber tanggungjawab Bersama. Retrieved from :https://www.bharian.com.my/rencana/surat-pembaca/2019/12/638215/kesejahteraan-siber-tanggungjawab-bersama-sekolah

Bernama 2019. 6 November. Penggunaan Internet dalam kalangan remaja. Retrieved from : https://www.astroawani.com/gaya-hidup/penggunaan-internet-dalam-kalangan-remaja-membimbangkan-mcpf-221947

Copyright@FTSM UKM

Giannakas, Filippos & Kambourakis, Georgios & Gritzalis, Stefanos. 2015. CyberAware: A mobile game-based app for cybersecurity education and awareness.

Liaqat Ali, 2019. "Cyber Crimes-A Constant Threat For The Business Sectors And Its Growth (A Study Of The Online Banking Sectors In GCC)," Journal of Developing Areas, Tennessee State University, College of Business, vol. 53(1), pages 253-265.

Luqman Hakim Mohomad Salehin. 2020. A Mobile Game On Awareness Of Calorie and Sugar Intake For Teenagers: Universiti Kuala Lumpur Malaysian Institute of Information Technology.

Nazilah Ahmad@Ahmad Arifin, Umi Asma' Mokhtar, Zaihosnita Hood, Tiun S, Dian Indrayani Jambari. Parental Awareness on Cyber Threats Using Social Media. Jurnal Komunikasi: Malaysian Journal of Communication. 2019;35(2).

Pitchan, Muhammad Adnan & Omar, Siti & Akmar, Ghazali. 2019. Amalan Keselamatan Siber Pengguna Internet terhadap Buli Siber, Pornografi, E-Mel Phishing dan Pembelian dalam Talian (Cyber Security Practice Among Internet Users Towards Cyberbullying, Pornography, Phishing Email and Online Shopping). Jurnal Komunikasi: Malaysian Journal of Communication. 35. 212-227.

RAD Model.Retrieved from: https://hackr.io/blog/rapid-application-development-model

Salina Ibrahim. 2015. November 19. Mewujudkan Sistem Aplikasi: Kepentingan Keperluan Pengguna (User Requirements). Retrieved from : http://www.ukm.my/wadahict/mewujudkan-sistem-aplikasi-kepentingan-keperluan-pengguna-user-requirements/

SDLC Model. Retrieved : from:https://www.techopedia.com/definition/22193/software-development-life-cycle-sdlc

Sinar Harian Online. 2019. 9 Jun. Ancaman jenayah siber. Retrieved from: https://www.sinarharian.com.my/article/31637/BERITA/Nasional/Ancaman-jenayah-scam

Copyright@FTSM UKM