PEMBANGUNAN SISTEM KESELAMATAN MENGGUNAKAN PENGESAHAN KATA LALUAN TIGA PERINGKAT

SASHNEETA A/P SUBAHAR
WAN FARIZA FAUZI

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Pada zaman sekarang, keselamatan komputer kebanyakannya bergantung pada kata laluan untuk mengesahkan sesuatu akaun pengguna. Terdapat banyak kaedah pengesahan akaun yang dicadangkan kini. Sesetengah kaedah pengesahan berdasarkan pada sifat fizikal dan tingkah laku pengguna. Sebagai contoh, pengecaman suara. Manakala, beberapa kaedah lain berdasarkan pengetahuan pengguna seperti kata laluan teks dan grafik. Walau bagaimanapun, kaedah-kaedah ini masih tidak selamat dan mengundang penggodam mencuri data dengan mudah. Tambahan pula, pengguna sering menggunakan kata laluan mudah yang boleh diramal oleh penggodam dengan mudah. Oleh itu, sesuatu kaedah pengesahan yang selamat dan mesra pengguna diperlukan untuk mengatasi masalah ini. Dalam projek ini, suatu kaedah pengesahan kata laluan tiga peringkat dibangunkan untuk mengatasi masalah ini. Dalam kaedah pengesahan yang dibangunkan kata laluan teks, kata laluan grafik dan pengesanan kod warna merupakan tiga peringkat berbeza yang digunakan. Kaedah pengesahan ini dikelaskan sebagai pengesahan berasaskan pengetahuan. Strategi pengesahan berbilang faktor yang dicadangkan dalam projek ini ialah gabungan teknik / kaedah pengesahan semasa yang sedia ada. Sistem ini mempunyai dua fungsi iaitu pendaftaran sistem dan log masuk sistem dimana metodologi air terjun yang memberi penekanan kepada pembangunan langkah demi langkah digunakan dengan menamatkan satu langkah sebelum mara ke langkah yang lain sehingga mencapai prototaip peringkat akhir. Teknik/kaedah pengesahan sedia ada masing-masing mempunyai kelemahan dan kesukaran tersendiri apabila digunakan secara berasingan. Oleh itu, objektif utama sistem keselamatan tiga peringkat ini adalah untuk menyiasat pengesahan berbilang yang sedia ada, mengukuhkan mekanisme pengesahan kata laluan yang menyediakan tahap keselamatan terbaik semasa mengesahkan pengguna dan menganalisis serta menguji keupayaan kaedah pengesahan untuk menghalang akses haram. Mudah-mudahan, sistem ini dapat memberikan persekitaran yang lebih baik dan selamat kepada pengguna daripada akses tanpa izin.

1 PENGENALAN

Tanpa mengira persekitaran berkomputer dan kemajuan teknologi zaman ini, bergantung semata-mata pada pengesahan faktor tunggal adalah berisiko dan tidak selamat. Keselamatan sistem dan akses rangkaian tidak pernah menjadi lebih sukar. Risiko keselamatan dan perlindungan perisian hasad sentiasa boleh dipertikaikan, sama ada dari segi kuantiti atau kualiti. Penggodaman dan penipuan atas talian telah menjadi lebih mudah dengan lebih banyak ketersediaan data. Pengesahan log masuk/kata laluan biasa dianggap tidak selamat dalam keadaan ini. Kesukaran menghadkan akreditasi palsu juga meningkat saban hari. (D. Florencio, C. Herley, & B. Coskun 2007).

Kebimbangan keselamatan semakin meningkat pada masa kini. Jadi, lebih daripada satu elemen pengesahan mula digunakan. Dua pengesahan elemen yang menggunakan *OTP* dan pin/kad *ATM* telah dilaksanakan untuk menangani isu kata laluan dalam sektor perbankan serta untuk pemindahan internet (*online transfers*). Dengan menambah komponen pengesahan tunggal, pengesahan dua elemen menjamin tahap keyakinan yang lebih baik (Dmitrienko et al. 2014). Majoriti rangka kerja pada masa ini bergantung pada kata laluan statik untuk mengesahkan keunikan pelanggan. Pelanggan lebih suka menggunakan kata laluan yang jelas, ringkas, mudah diteka, dan kata laluan yang sama untuk banyak rekod atau laman web, malah mereka menulis kata laluan mereka, menyimpannya pada sistem mereka untuk mengingati kata laluan mereka.

Mengikut definisi, pengesahan ialah penggunaan satu atau lebih komponen untuk membuktikan bahawa anda adalah diri anda yang anda katakan. Akses diberikan selepas personaliti diterima. *Multi Factor Authentication* (*MFA*) menyediakam lapisan keselamatan tambahan yang memastikan dan meningkatkan mekanisme pengesahan sekarang tanpa menggantikan mekanisme pengesahan yang asal (Shacklett, M. E. & Contributor, T. T 2021).

Pengesahan berasaskan token, pengesahan berasaskan biometrik dan pengesahan berasaskan pengetahuan ialah tiga kategori utama kaedah pengesahan. "Apa yang anda ada" ialah maksud berasaskan token. Penyelesaian berasaskan token memanfaatkan token yang digunakan secara meluas seperti kad kunci, kad bank dan kad pintar. Pengguna yang kehilangan tokennya tidak akan dapat log masuk. Akibatnya, kategori pengesahan berasaskan token sangat sensitif terhadap penipuan, kecurian atau kehilangan token itu sendiri (Mughele Ese Sophia, 2015). Pendekatan biometrik merujuk kepada "siapa anda." Biometrik fisiologi, seperti cap jari, geometri muka, dan ukuran iris, digunakan dalam prosedur ini (Babich A, 2012). Kelemahan utama strategi ini ialah sistem mungkin lebih mahal dan pengiktirafan sistem ini mungkin ditangguhkan. Akhir sekali, istilah "kaedah berasaskan pengetahuan" merujuk kepada "apa yang anda tahu." Ia adalah cara pengesahan yang kerap. Ia menyokong kata laluan teks dan grafik (Mughele Ese Sophia, 2015).

Jika pengguna mendakwa dirinya adalah pengguna yang sah, sistem yang dicadangkan menyemak pernyataan itu. Sebelum log masuk berjaya, pengguna harus melepasi

pengesahan kata laluan tiga peringkat. Memandangkan sudah terdapat begitu banyak sistem kata laluan yang berbeza, dan beberapa daripadanya nampaknya gagal disebabkan oleh serangan bot menurut (Unknown, *Journal of Computer and System Sciences* 2014), sistem ini telah mengambil kira serangan bot juga. Salah satu daripada tiga peringkat dikhususkan sepenuhnya untuk serangan bot untuk mengelakkan penggodaman sistem melalui bot. Jadi, sistem yang dicadangkan dibina untuk menyediakan tahap keselamatan pengesahan pengguna yang setinggi mungkin.

2 PENYATAAN MASALAH

Strategi pengesahan berbilang faktor yang dicadangkan dalam projek ini ialah gabungan teknik/kaedah pengesahan semasa. Teknik/kaedah pengesahan sedia ada masing-masing mempunyai kelemahan dan kesukaran tersendiri apabila digunakan secara berasingan.

Pengesahan berasaskan kata laluan meluas dan konvensional untuk menyediakan keselamatan asas yang telah digunakan selama beberapa dekad. Isu utama dengan kata laluan teks ialah apabila pengguna menjana kata laluan asas yang mudah diingati. Akibatnya, kata laluan mudah untuk dikesan dan dipecahkan, yang membawa kepada aktiviti berniat jahat. Walau bagaimanapun, terdapat beberapa percubaan sepanjang tahun untuk mencipta kata laluan teks yang kukuh. Contohnya, gabungan nombor, aksara khas, aksara abjad sensitif huruf besar dan jujukan nombor serta abjad yang unik tanpa aksara tunggal diulang dalam susunan berturut-turut. Ini menyukarkan orang ramai untuk mengingati kata laluan ini. Walaupun begitu, masalah masih berterusan dimana kod program komputer yang mudah boleh memecah masuk ke dalam kata laluan berasaskan teks yang paling rumit sekalipun menurut *Kevin Beaver* (2021). Akibatnya, pengesahan sistem berasaskan kata laluan sahaja tidak selamat.

Hasilnya, pengesahan dua faktor telah diperkenalkan dan cepat diterima pakai. *2FA* melindungi log masuk pengguna daripada pancingan data, kejuruteraan sosial dan percubaan kata laluan *brute-force*, serta penyerang yang menggunakan bukti kelayakan yang lemah atau dicuri. Walau bagaimanapun, terdapat masalah dengan teknik yang dicadangkan juga. Salah satunya ialah kebanyakan individu tidak mempraktikkan (*Turn on* / *Enable*) ciri pengesahan dua faktor kerana ia sukar, menyusahkan dan sebagainya.

Tambahan pula, pelaksanaan pengesahan dua faktor mungkin tidak betul sehingga boleh dilangkau sepenuhnya. Ini dikenali sebagai *2FA* logik rosak (*2FA Broken Logic*). Contohnya, jika pengguna diminta menyerahkan kata laluan sebelum diminta memasukkan kod pengesahan pada halaman lain, pengguna pada asasnya "log masuk" sebelum memasukkan kod pengesahan. Dalam senario ini, adalah wajar melihat sama ada pengguna boleh pergi terus ke tapak "log masuk sahaja" selepas proses pengesahan awal selesai. Kadangkala, tapak web tidak akan mengesahkan sama ada pengguna telah menyelesaikan langkah kedua sebelum memuatkan halaman atau tidak (Rezaduty, 2020).

Tambahan pula, token pengesahan dua faktor mungkin membawa kepada kelemahan keselamatan juga. Sesetengah tapak web menghantar mesej teks dengan nombor pengesahan ke telefon pengguna. Walaupun ini masih mengesahkan aspek "sesuatu yang anda ada", ia terdedah kepada eksploitasi. Sebagai permulaan, kod dihantar melalui *SMS* dan bukannya dihasilkan oleh peranti. Ini meningkatkan peluang kod dipintas. Terdapat juga kemungkinan penukaran *SIM*, di mana penyerang memperoleh kad *SIM* dengan nombor telefon mangsa secara curang. Semua mesej SMS yang dihantar kepada mangsa, termasuk yang mempunyai kod pengesahan mereka, akan diterima oleh penyerang (Rezaduty, 2020).

Kebanyakan penyelesaian dua faktor telah terbukti tidak berkesan terhadap pengguna yang canggih. Menurut dokumen yang didedahkan oleh *The Intercept*, kumpulan Rusia yang menyasarkan pegawai pilihan raya *AS* mempunyai strategi sedia untuk akaun dengan pengesahan dua faktor, mengumpulkan kod pengesahan menggunakan taktik yang sama yang mereka gunakan untuk mendapatkan kata laluan. Menurut pencipta Perisian Simbolik Nadim Kobeissi (Brandom R, 2017), walaupun selepas sistem telah ditetapkan semula, peranti yang didaftarkan secara hasad membenarkan penyerang memintas keselamatan dua faktor sasaran.

3 OBJEKTIF KAJIAN

Matlamat projek ini adalah untuk melihat sejauh mana kejayaan meningkatkan keselamatan dengan menggunakan mekanisme pengesahan tiga peringkat. Berikut adalah objektif projek ini:

i. Untuk menyiasat pengesahan berbilang semasa yang sedia ada.
ii. Untuk merekabentuk mekanisme pengesahan kata laluan yang meningkatkan tahap keselamatan semasa mengesahkan pengguna.
iii. Untuk menganalisis dan menguji keupayaan skim pengesahan untuk menghalang akses haram.

4 METOD KAJIAN

Model Air Terjun ialah metodologi pembangunan yang digunakan dalam sistem ini. Paradigma Air Terjun diterangkan dalam rajah 1.1. Analisis keperluan, reka bentuk sistem, pelaksanaan, ujian, pembangunan dan fasa penyelenggaraan adalah enam fasa utama pendekatan ini.

4.1 Fasa 1: Keperluan Pengumpulan (Analisis)

Matlamat utama fasa ini adalah untuk mengetahui matlamat sistem dan cara keseluruhan sistem untuk pengesahan tiga peringkat akan berfungsi. Semasa fasa ini, keperluan pengguna dianalisis. Di samping itu, fasa ini digunakan untuk menentukan skop untuk pengguna dan sistem, serta membuat pemerhatian ke atas sistem sekarang. Fasa ini merekodkan semua keperluan sistem yang boleh difikirkan dan mendokumenkannya dalam spesifikasi keperluan.

4.1.1 Spesifikasi keperluan sistem

Fungsi pertama sistem ialah pendaftaran. Sistem ini bermula dengan pendaftaran akaun pengguna. Pada fungsi ini, pengguna harus memasukkan maklumat peribadinya seperti nama, umur, tarikh lahir, e-mel dan nombor telefon mereka serta memilih nama pengguna, kata laluan teks, kata laluan grafik dan kod warna yang bakal dimasukkan semula sewaktu log masuk bagi tujuan pengesahan tiga peringkat. Bagi memilih nama pengguna dan kata laluan teks, angka, abjad dan sebarang aksara lain dengan syarat minimum lapan aksara yang kuat tetapi mudah diingati oleh pengguna boleh digunakan. Sewaktu memilih kata laluan grafik, sistem yang dicadangkan ini menggunakan pendekatan berasaskan ingatan semula, terutamanya teknik berdasarkan *Cued Recall*. Untuk proses pendaftaran, hanya imej dari pangkalan data boleh dipilih. Pengguna tidak dibenarkan memuat naik imej mereka sendiri. Pengguna akan diberikan sepuluh gambar rawak daripada pangkalan data,

yang mana dia mesti memilih tiga dan klik pada mana-mana grid pada setiap imej yang koordinat akan direkodkan semasa pendaftaran. Oleh itu, tiga imej dengan satu koordinat titik klik pada setiap imej akan direkodkan mengikut susunan urutan. Akibatnya, peluang pengguna memilih urutan foto yang sama dan mengklik tempat yang sama adalah sangat tidak mungkin kerana terdapat 720 kombinasi susunan urutan gambar, menjadikan pengalaman setiap pengguna unik. Akibatnya, "*Cued Click Point*"(*CCP*) meningkatkan kefungsian dan keselamatan sambil menjadikan serangan lebih sukar. Seterusnya, bagi pemilihan kod warna, terdapat lima warna kesemuanya yang akan dipaparkan, dan pengguna mesti memilih mana-mana tiga warna dalam susunan tertentu. Pengguna kemudiannya perlu memasukkan kod warna yang sama dan dalam susunan yang sama semasa log masuk. Oleh kerana jujukan warna akan sentiasa tidak dapat diramalkan, pengguna mesti mengingati kod tersebut; tekan dan cuba tidak akan berfungsi kerana terdapat 120 kombinasi warna berbeza dalam semakan keselamatan ini. Setelah selesai pemilihan kesemua yang dinyatakan di atas, data berkaitan pengguna untuk penggunaan sistem akan disimpan dalam pangkalan data apabila pengguna tekan butang daftar. Dengan ini, pendaftaran sistem berjaya.

Fungsi kedua sistem ialah log masuk. Pengguna harus memasukkan nama pengguna, kata laluan teks, kata laluan grafik dan kod warna yang ditetapkan sewaktu pendaftaran akaun dengan maksimum tiga kali percubaan bagi setiap peringkat untuk berjaya log masuk ke dalam sistem.

4.1.2 Keperluan Bukan Fungsian

- Keselamatan:

Beberapa kemungkinan strategi serangan dianalisis untuk menilai keperluan keselamatan siber dan menentukan sejauh mana keselamatan sistem pengesahan yang dibangunkan. Mekanisme pengesahan yang dicadangkan telah disiasat sama ada tahan terhadap serangan sedemikian atau tidak. Dalam bahagian ini, beberapa kemungkinan serangan cuba ditangani serta dilihat sama ada ia sah atau tidak.

- Kecekapan (*Efficiency*)

Segala fungsi yang ada pada sistem perlu berjalan dengan cekap dan efisien.

- Kebolehgunaan (*Usability*)

Fungsi-fungsi yang terdapat pada sistem mesti boleh berfungsi tanpa sebarang ralat.

- Penyelenggaraan (*Maintainability*)

Penyelenggaraan adalah bahagian di mana penambahbaikan dan pengubahsuaian dilakukan bagi membetulkan segala ralat yang wujud pada sesebuah sistem. Hal yang demikian adalah bertujuan untuk memastikan sistem sentiasa berada dalam keadaan yang baik dan berfungsi sebagaimana yang dikehendaki oleh pengguna.

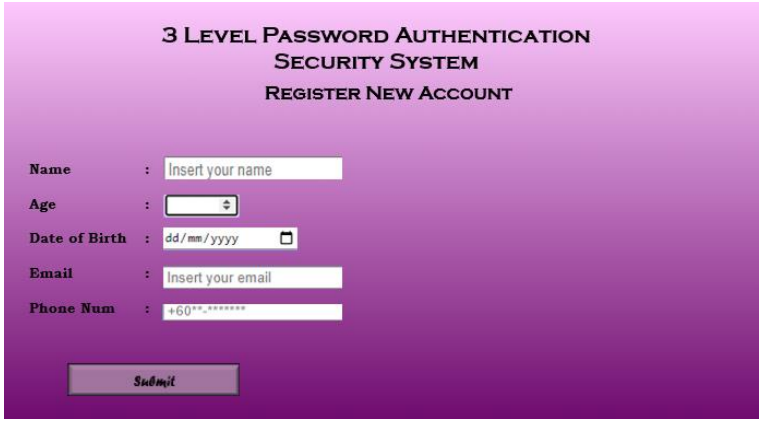
4.2 Fasa 2: Reka Bentuk Sistem

Salah satu fasa yang paling penting dalam pembangunan ialah reka bentuk sistem. Fasa ini akan menerangkan rupa dan operasi sistem. Semasa fasa ini, struktur umum sistem ditentukan, dan sistem dibina. Ia membantu dalam spesifikasi keperluan perkakasan dan perisian, serta definisi seni bina sistem keseluruhan.

Antara Muka Halaman Menu Utama

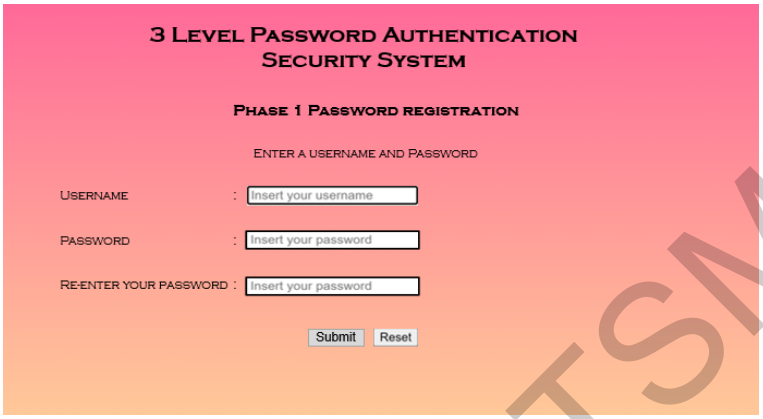
Rajah 4.1 – Antara muka halaman menu utama

Antara Muka Halaman Pendaftaran Maklumat Peribadi



Rajah 4.2 – Antara muka pendaftaran maklumat peribadi

Antara Muka Halaman Pendaftaran Kata Laluan Teks (Peringkat Satu)

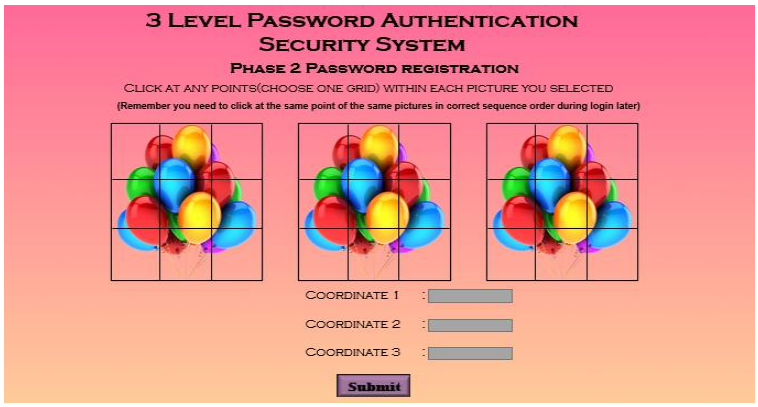


Rajah 4.3 – Antara muka pendaftaran kata laluan teks (Peringkat satu)

Antara Muka Halaman Pendaftaran Kata Laluan Grafik (Peringkat Dua)

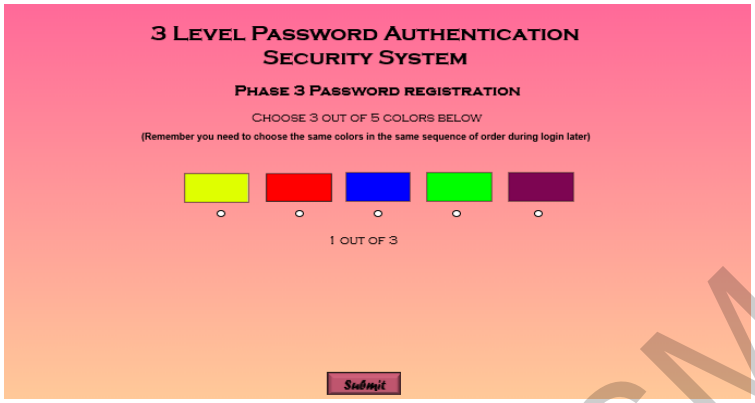
Rajah 4.4 – Antara muka pendaftaran kata laluan grafik (Peringkat dua)

Antara Muka Halaman Pendaftaran Kata Laluan Grafik (Peringkat Dua – Pemilihan Koordinat)



Rajah 4.5 – Antara muka pendaftaran kata laluan grafik (Peringkat dua) pemilihan titik koordinat

Antara Muka Halaman Pendaftaran Kata Laluan Kod Warna (Peringkat Tiga)



Rajah 4.6 – Antara muka pendaftaran kata laluan kod warna (Peringkat tiga)

Antara Muka Halaman Pendaftaran Berjaya

Rajah 4.7 – Antara muka pendaftaran berjaya

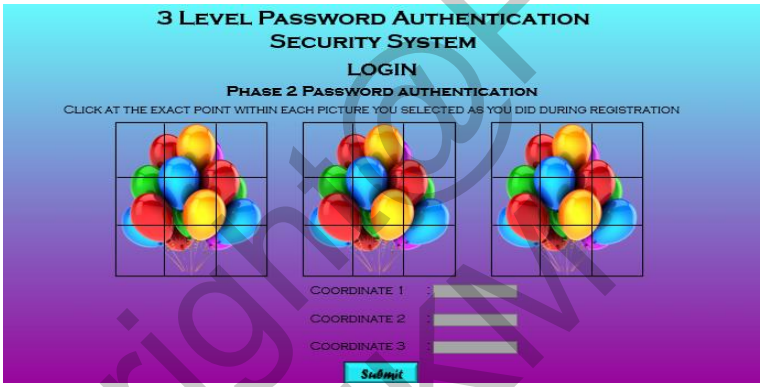
Antara Muka Halaman Log Masuk (Pengesahan Peringkat Satu)

Rajah 4.8 – Antara muka log masuk (pengesahan peringkat satu)

Antara Muka Halaman Log Masuk (Pengesahan Peringkat Dua)

Rajah 4.9 – Antara muka log masuk (pengesahan peringkat dua)

Antara Muka Halaman Log Masuk (Pengesahan Peringkat Dua – Pemilihan Koordinat)



Rajah 4.10 – Antara muka log masuk (pengesahan peringkat dua) pemilihan titik koordinat

Antara Muka Halaman Log Masuk (Pengesahan Peringkat Tiga)

Rajah 4.11 – Antara muka log masuk (pengesahan peringkat tiga)

Antara Muka Halaman Log Masuk Berjaya

Rajah 4.12 – Antara muka log masuk Berjaya

Antara Muka Halaman Log Masuk Tidak Berjaya

Rajah 4.13 – Antara muka log masuk tidak berjaya

Dengan tiga peringkat pengesahan yang berbeza, peluang untuk memasuki sistem tanpa izin adalah tipis. Serangan bot atau pengguna palsu tidak akan mendapat akses kepada sistem. Bagi mengukuhan kesselamatan sistem lagi, bilangan percubaan log masuk dihadkan kepada tiga kali bagi setiap peringkat pengesahan. Jika pengguna membuat kesilapan dalam mana-mana peringkat, pengguna akan segera dilog keluar dan akaun akan dikunci selama lima minit selepas tiga percubaan. Pengguna akan dituju ke antara muka log masuk tidak berjaya seperti rajah 4.16 selepas tiga kali percubaan dalam mana-mana peringkat.

4.3 Fasa 3: Implementasi Sistem

Perisian yang digunakan untuk membangunkan sistem ini adalah *Sublime Text*. *Xampp* juga digunakan sepanjang pembangunan sistem sebagai localhost. Pangkalan data yang digunakan adalah *MYSQL* dimana perisian *phpMyAdmin* telah digunakan untuk mengendalikan pentadbiran *MYSQL* melalui web dan bahasa pengaturcaraan yang

digunakan untuk membangunkan sistem keselamatan menggunakan pengesahan kata laluan tiga peringkat adalah *HTML*, *PHP*, *CSS* dan *JavaScript*. Selain itu, Jquery juga telah digunakan supaya laman sistem ini lebih interaktif dan lebih mesra pengguna dari segi kefungsiannya. Selain itu, *PHP* Data Objects (*PDO*) telah digunakan untuk mengakses pangkalan data dan bukannya *MYSQLi* kerana *PDO* mempunyai lebih banyak kelebihan jika dibandingkan dengan *MYSQLi* semasa proses pembangunan laman sistem keselamatan menggunakan pengesahan kata laluan tiga peringkat. *PHP* telah dipilih sebagai bahasa pengaturcaraan utama bagi pembangunan backend. Manakala bagi pembangunan frontend pula, gabungan antara *HTML* dan *CSS* telah digunakan untuk membangunkan antaramuka yang kemas dan menarik.

Proses pengekodan yang teliti dilakukan bagi memastikan tiada kesilapan bagi setiap halaman dan fungsi sistem. Sebelum mana-mana fungsi sistem dibangunkan, sambungan antara *PHP* dan pelayan pangkalan data diwujudkan. Implementasi sistem bermula dengan mencipta kelas '*database.php*' bagi mewujudkan sambungan antara *PHP* dan pelayan pangkalan data. Hal ini demikian kerana, fungsi-fungsi sistem sentiasa menghantar atau menerima data daripada pangkalan data dan saling bergantung pada satu sama lain. Setelah itu, fungsi pendaftaran sistem mula dibangunkan mengikut peringkat iaitu pendaftaran maklumat peribadi, pendaftaran nama pengguna dan kata laluan teks, pendaftaran kata laluan grafik, pendaftaran kata laluan grafik (pemilihan koordinat) dan akhir sekali pendaftaran kata laluan kod warna. Sepanjang pembangunan, kod ditulis menggunakan *Sublime Text 3* dan diuji secara dalaman menggunakan *Xampp* sebagai localhost untuk memastikan setiap halaman berfungsi baik dan mencapai objektif sebelum diterbit dan diintegrasikan kepada pelayan *lrgs.ftsm.ukm.my*. Setelah membangun dan implementasi fungsi pendaftaran sistem, fungsi log masuk mula dibangunkan mengikut peringkat. Fungsi ini lebih kepada menerima data daripada pangkalan data bagi tujuan pengesahan manakala fungsi pendaftaran lebih kepada menghantar data kepada pangkalan data. Selesai membina kedua-dua fungsi sistem, sistem keselamatan menggunakan pengesahan kata laluan tiga peringkat ini diterbit dan diintegrasikan kepada pelayan *lrgs.ftsm.ukm.my.* Pelayan serta beberapa baris kod berfungsi sebagai pengantara yang mengintegrasikan segala fungsi sistem sebagai suatu sistem lengkap.

4.4 Fasa 4: Pengujian Sistem

Kaedah pengujian yang digunakan pada sistem keselamatan menggunakan pengesahan kata laluan tiga peringkat melibatkan pengujian fungsian dan pengujian bukan fungsian, iaitu pengujian kotak hitam dan pengujian keselamatan serta kebolehgunaan.

4.4.1 Pengujian Fungsian (Functional Testing)

a. Pengujian Kotak Hitam (*Black Box Testing*)

Kaedah pengujian kotak hitam ialah kaedah yang membolehkan ujian secara rawak, tidak dirancang dan dijalankan oleh orang yang tidak memahami secara terperinci tentang spesifikasi sesuatu produk. Kaedah ini digunakan untuk menguji fungsi yang terdapat dalam sistem keselamatan menggunakan pengesahan kata laluan tiga peringkat yang telah dibangunkan.

Dalam projek ini, pengujian kotak hitam dilakukan oleh pengguna akhir untuk menguji kebolehgunaan dan kebolehfungsian sistem tersebut.

4.4.2 Pengujian Bukan Fungsian (Non-Functional Testing)

a. Pengujian Kebolehgunaan (*Usability Testing*) dan Keselamatan (*Security Testing*)

Pengujian kebolehgunaan ialah pengujian yang fokus kepada kemudahan pengguna untuk menggunakan sesuatu sistem untuk mencapai objektif tertentu. Matlamat pengujian ini adalah untuk memberi kepuasan kepada pengguna dari segi kecekapan, ketepatan dan mesra pengguna (Guru99, 2019). Menurut Guru99, aspek kecekapan dalam pengujian kebolehgunaan mewakili keseragaman format antara muka manakala aspek ketepatan menunjukkan tiada pautan atau butang yang tidak berfungsi. Aspek mesra pengguna pula bermaksud sistem yang mudah digunakan tanpa keperluan latihan serta disediakan dengan bantuan bagi pengguna memahami penggunaan sistem tersebut.

Pengujian keselamatan pula merupakan sejenis ujian perisian yang mendedahkan kelemahan sistem dan menentukan bahawa data dan sumber sistem dilindungi

daripada kemungkinan penceroboh. Ia memastikan sistem bebas daripada sebarang ancaman atau risiko yang boleh menyebabkan kerugian.

Platform yang digunakan bagi menguji keselamatan dan kebolehgunaan sistem keselamatan menggunakan pengesahan kata laluan tiga peringkat ialah laman web melalui pelayan lrgs ftsm. Pengkaji mengintegrasikan sistem keselamatan menggunakan pengesahan kata laluan tiga peringkat ke laman web melalui pelayan lrgs ftsm dan kemudian menguji keselamatan dan kebolehgunaannya untuk mencari kelemahan yang terdapat dalam sistem tersebut.

4.5 Fasa 5: Penggunaan Sistem

Selepas ujian berfungsi dan tidak berfungsi, sistem dikeluarkan ke dalam persekitaran pemasaran. Pelanggan akan diperkenalkan kepada mekanisme pengesahan kata laluan tiga peringkat, yang kemudiannya akan ditawarkan kepada pengguna.

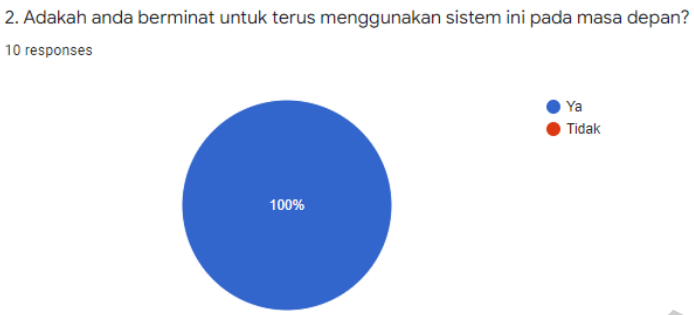
4.6 Fasa 6: Penyelenggaraan

Perubahan yang berlaku selepas sistem diserahkan kepada pengguna mestilah tidak mempunyai kesan ke atas fungsi asas sistem. Akibatnya, sistem mesti dibina dengan cara yang boleh menyesuaikan diri dengan perubahan dari semasa ke semasa. Tidak semua kesukaran dapat dilihat pada mulanya, tetapi ia berkembang dengan masa dan, seperti masalah lain, ia mesti diselesaikan.

5 HASIL KAJIAN

Kaji selidik penggunaan sistem keselamatan menggunakan pengesahan kata laluan tiga peringkat yang telah dijalankan bertujuan untuk mendapatkan maklum balas pengguna selepas menggunakan sistem tersebut. Kaji selidik ini dijalankan oleh 10 orang responden. Kaji selidik ini menunjukkan keputusan dari segi kepuasan pengguna, kebolehfungsian sistem, kebolehgunaan sistem dan masalah yang dihadapi oleh pengguna.

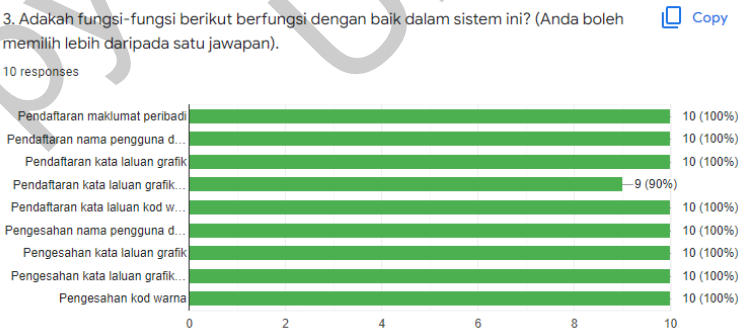
a. Kepuasan pengguna



Rajah 5.1 : Minat pengguna untuk terus menggunakan sistem

Rajah 5.1 menunjukkan bilangan responden yang berminat untuk terus menggunakan sistem keselamatan menggunakan pengesahan kata laluan tiga peringkat pada masa depan. 100% atau semua orang responden adalah berminat untuk terus menggunakan sistem yang telah dibangunkan pada masa depan. Kebanyakan pengguna adalah pengguna yang biasa menggunakan laman web dan pernah menggunakan kata laluan tiga peringkat yang ada pada sistem ini secara tunggal atau berdua. Justeru, kemudahan penggunaan sistem tersebut dapat menarik minat penggunanya dan berjaya mencapai kepuasan yang tinggi dari para pengguna.

b. Kebolehfungsian sistem

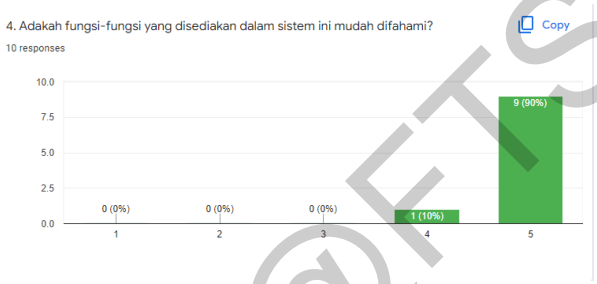


Rajah 5.2 : Kebolehfungsian sistem

Merujuk kepada Rajah 5.2, 100% atau semua responden bersetuju bahawa fungsi pendaftaran maklumat peribadi, pendaftaran nama pengguna dan kata laluan teks, pendaftaran kata laluan grafik, pendaftaran kata laluan kod warna, pengesahan nama pengguna dan kata laluan teks, pengesahan kata laluan grafik, pengesahan kata laluan grafik-pemilihan koordinat serta pengesahan kod warna beroperasi baik dalam sistem

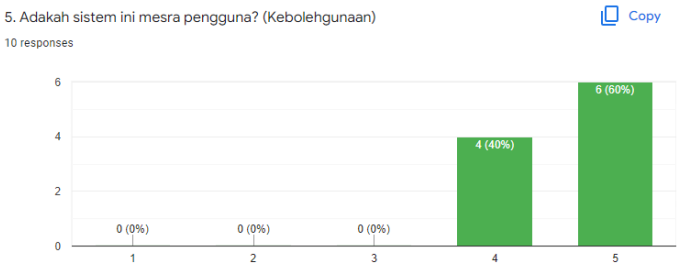
yang telah dibangunkan manakala fungsi pendaftaran kata laluan grafik-pemilihan koordinat pula mendapat persetujuan daripada 90% atau sembilan orang responden. Seorang responden memberitahu bahawa halaman pendaftaran kata laluan grafik-pemilihan koordinat menerima input kosong/dapat dihantar tanpa memilih koordinat. Namun, penyelesaian bagi isu ini dapat diselesaikan oleh pengkaji dengan membaiki kod supaya tidak menerima input kosong.

c. Kebolehgunaan sistem



Rajah 5.3 : Tahap kemudahan pemahaman sistem

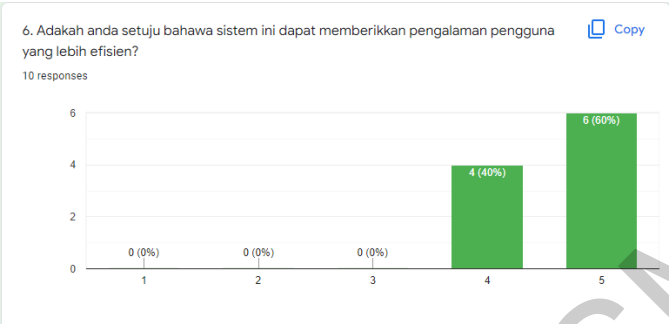
Rajah 5.3 menunjukkan tahap kemudahan pemahaman sistem di mana 90% atau sembilan orang responden sangat bersetuju bahawa fungsi-fungsi yang disediakan dalam sistem keselamatan menggunakan pengesahan kata laluan tiga peringkat adalah mudah difahami. Terdapat juga 10% atau seorang responden yang bersetuju kepada perkara yang dinyatakan tersebut. Fungsi-fungsi yang disediakan dalam sistem disertai dengan panduan yang jelas. Justeru, fungsi-fungsi tersebut dapat digunakan tanpa arahan daripada orang lain.



Rajah 5.4 : Tahap kebolehgunaan sistem dari aspek mesra pengguna

60% atau enam orang responden setuju bahawa sistem yang dibangunkan adalah sangat mesra pengguna dan mempunyai tahap kebolehgunaan yang amat tinggi. 40% atau empat orang responden pula setuju bahawa sistem tersebut adalah mesra pengguna dan

mempunyai tahap kebolehgunaan yang tinggi. Sistem yang dibangunkan ini mempunyai informasi berupa teks, gambar dan butang yang memudahkan pengguna dalam mencapai



objektif penggunaan yang dikehendaki.

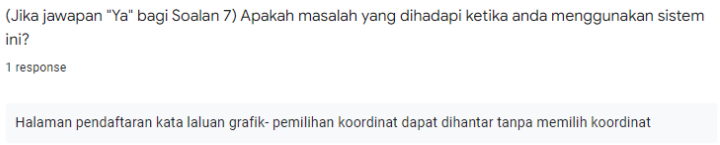
Rajah 5.5 : Tahap keefisienan dalam pengalaman pengguna

Seramai 60% atau enam orang responden sangat setuju bahawa sistem ini memberikan pengalaman pengguna yang lebih efisien. Terdapat juga 40% atau empat orang responden yang setuju bahawa sistem ini dapat memberikan pengalaman pengguna yang lebih efisien. Saiz gambar-gambar yang digunakan dalam sistem telah ditetapkan agar sistem dapat memberi paparan halaman yang lebih efisien dan mesra pengguna.

d. Masalah yang dihadapi oleh pengguna

Rajah 5.6 : Bilangan pengguna yang menghadapi masalah semasa pengunaan sistem

Rajah 5.6 menunjukkan bilangan pengguna yang menghadapi masalah semasa menggunakan sistem keselamatan menggunakan pengesahan kata laluan tiga peringkat. Hanya 10% atau seorang responden mengatakan bahawa beliau menghadapi masalah ketika menggunakan sistem tersebut.



Rajah 5.7 : Masalah yang dihadapi oleh pengguna semasa pengunaan sistem

Masalah tersebut merujuk kepada masalah penerimaan input kosong dalam penetapan koordinat kata laluan grafik yang telah dilaporkan di bahagian b. Kebolehfungsian sistem.

6 KESIMPULAN

Secara keseluruhannya, sistem yang dibangunkan diharap menepati semua keperluan pengguna yang dinyatakan dalam dokumen dan memberikan prestasi yang memuaskan hati pengguna. Hasil perancangan kajian ini diharap dapat memberi gambaran dan tunjuk ajar bagi pembangunan sistem yang lengkap.

7 RUJUKAN

A.T. Akinwale and F.T. Ibharalu, 2009, Password Authentication Scheme with Secure Login Interface

Ahmad Almulhem Computer Engineering Department King Fahd University of Petroleum and Minerals Dhahran, Saudi Arabia, A Graphical Password Authentication System

Babich, A, 2012, Biometric Authentication, Type of Biometric Identifier

Brandom, R. (2017, July 10). Two-factor authentication is a mess. The Verge. Retrieved November 13, 2021, from https://www.theverge.com/2017/7/10/15946642/two-factor-authentication-online-security-mess

Chiasson, S., van Oorschot, P.C., Biddle, R. Graphical Password Authentication Using Cued Click-points. ESORICS 2007

Cynthia Kuo, Sasha Romanosky, Lorrie Faith Cranor; 2006; Human Selection of Mnemonic Phrase-based Passwords

D. Florencio, C. Herley, and B. Coskun, “Do strong web passwords accomplish anything?” in Proceedings of the 2nd USENIX Workshop on Hot Topics in Security, ACM Digital Library, August 2007.View at: Google Scholar

Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi, “On the (In)Security of mobile two-factor authentication,” in Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3–7, 2014, Revised Selected Papers, vol. 8437 of Lecture Notes in Computer Science, pp. 365– 383, Springer, Berlin, Germany, 2014.View at: Publisher Site | Google Scholar

J. Hong and D. Reed, “Passwords getting painful, computing still blissful,” Communications of the ACM, vol. 56, no. 3, pp. 10–11, 2013.View at: Publisher Site | Google Scholar

J. Owens and J. Matthews, “A study of passwords and methods used in brute force SSH attack,” in Proceedings of the USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET '08), 2008.View at: Google Scholar

M. Raza, M. Iqbal, M. Sharif, and W. Haider, “A survey of password attacks and comparative analysis on methods for secure authentication,” World Applied Sciences Journal, vol. 19, no. 4, pp. 439–444, 2012.View at: Publisher Site | Google Scholar

Rezaduty. (2020, July 19). Security issues with two factor authentication (2FA). Medium. Retrieved November 12, 2021, from https://medium.com/@rezaduty/2fa-security-issue-675a6dec825a.

Y.-L. Chen, W.-C. Ku, Y.-C. Yeh, and D.-M. Liao, “A simple tex-tbased shoulder surfing resistant graphical password scheme,” in Next- Generation Electronics (ISNE), 2013 IEEE International Symposium on. IEEE, 2013, pp. 161–164.

Sashneeta a/p Subahar (A174559)
Wan Fariza Fauzi
Fakulti Teknologi & Sains Maklumat,
Universiti Kebangsaan Malaysia