APLIKASI PENGURUS KATA LALUAN MENGGUNAKAN ALGORITMA PENYULITAN BERGANDA

NUR AZRINA AMIRA BINTI SALEHHUDDIN

DAHLILA PUTRI BINTI DAHNIL SIKUMBANG

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor Darul Ehsan, Malaysia

ABSTRAK

Dalam dunia yang pesat membangun, teknologi telah terbukti dapat membuatkan hidup kita lebih mudah. Teknologi dapat membantu kita untuk melakukan pelbagai aktiviti seharian seperti membeli-belah, belajar, kekal berhubung dan menyelesaikan kerja dengan hujung jari. Dalam proses pendaftaran *(registration)*, pengguna biasanya perlu untuk memasukkan maklumat log masuk mereka seperti alamat emel dan kata laluan. Proses pendaftaran ini adalah penting untuk pengesahan pengguna *(user authentication)* dan pemberian kuasa kepada pengguna *(user authorization)* untuk mengakses sesebuah sistem. Masalah timbul apabila pengguna meletakkan maklumat yang berkaitan dengan diri pengguna seperti nama dan tarikh lahir, atau menggunakan kata laluan yang biasa seperti '123456' boleh membawa kepada pelanggaran data *(data breach)*. Selain itu, penyimpanan kata laluan yang tidak betul di tempat yang mudah untuk dilihat, seperti pada nota post-it pada skrin komputer untuk memudahkan mereka mengingat kata laluan tersebut berisiko untuk pelanggaran data. Masalah-masalah tersebut akan mendedahkan pengguna kepada serangan siber seperti serangan kekerasan *(brute-force attack)*. Melalui serangan ini, penggodam dapat meneka kata laluan pengguna dan menggunakannya untuk mencapai maklumat peribadi pengguna. Berdasarkan permasalahan yang dinyatakan, satu aplikasi pengurus kata laluan menggunakan algoritma penyulitan akan dibangunkan. Aplikasi pengurus kata laluan membantu pengguna untuk mencipta kata laluan yang kuat. Pengurus kata laluan berfungsi untuk menjana kata laluan yang panjang dan kompleks untuk pengguna, di mana pengguna hanya perlu memasukkan frasa rawak dan klik butang jana untuk mencipta kata laluan. Aplikasi ini menggunakan algoritma penyulitan *(encryption)* dalam kriptografi untuk membolehkan kata laluan untuk disimpan dengan selamat. Algoritma penyulitan mencampuradukkan teks biasa kepada teks sifir, dan proses penyahsulitan *(decryption)*, iaitu menukar balik teks sifir kepada teks biasa. Dengan cara ini, walaupun pelayan pengurus kata laluan digodam, penyerang hanya akan mendapat senarai teks yang telah disulitkan yang tidak berfaedah untuk mereka tanpa mengetahui kunci penyulitan. Aplikasi ini membantu pengguna menguruskan kata laluan mereka dan menyimpan data sensitif dan penting pada peranti mereka.

PENGENALAN

Dalam dunia yang pesat membangun, teknologi telah terbukti dapat membuatkan hidup kita lebih mudah. Teknologi dapat membantu kita untuk melakukan pelbagai aktiviti seharian seperti membeli-belah, belajar, kekal berhubung dan menyelesaikan kerja dengan hujung jari. Untuk menggunakan semua kemudahan ini, kebanyakan laman web dan aplikasi memerlukan pengguna mereka untuk mendaftar. Dalam proses pendaftaran sistem, pengguna biasanya perlu untuk memasukkan maklumat log masuk mereka seperti alamat emel dan kata laluan. Proses pendaftaran ini adalah penting untuk pengesahan pengguna (user authentication) dan pemberian kuasa kepada pengguna (user authorization) untuk capaian sistem. Sebagai contoh, pelajar Universiti Kebangsaan Malaysia (UKM) perlu memasukkan nombor pendaftaran mereka beserta kata laluan untuk mengakses sistem UKMFolio.

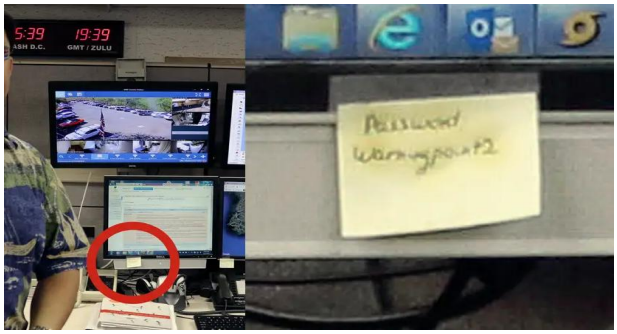
Proses pengesahan mengenalpasti identiti pengguna dengan merujuk kepada nama yang mereka gunakan yang adalah berbeza bagi setiap pengguna dalam sesebuah sistem. Sekiranya maklumat yang dimasukkan adalah salah, pengguna tidak akan diberikan akses untuk memasuki sistem kerana pengguna tidak dapat membuktikan identiti mereka. Pelbagai sistem menggunakan pengesahan berdasarkan kata laluan untuk mengesahkan identiti pengguna mereka, seperti sistem UKMFolio, Google dan Windows. Oleh sebab itu, setiap individu perlu menggunakan kata laluan yang unik kepada mereka, untuk memastikan kata laluan itu hanya boleh diketahui oleh pengguna sendiri.

Menurut National Institute of Standards and Technology (NIST), definisi kata laluan adalah rentetan aksara (huruf, nombor dan simbol lain) yang digunakan untuk mengesahkan identiti atau untuk mengesahkan kebenaran akses. Kebiasaannya, pengguna mencipta kata laluan berdasarkan diri mereka sendiri bagi memudahkan mereka untuk mengingati kata laluan tersebut. Sebagai contoh, mereka mencipta kata laluan yang mempunyai nama mereka atau tarikh lahir mereka. Terdapat juga situasi di mana mereka menggunakan kata laluan yang generik dan mudah diteka, seperti ‘password’ atau ‘123456’, untuk memudahkan mereka. Sejurus itu, perkara ini membawa kita kepada kebimbangan mengenai keselamatan komputer. Sekiranya kata laluan terdedah, ia akan membenarkan penggodam untuk mempunyai akses kepada pelbagai maklumat yang sepatutnya hanya boleh diakses oleh pengguna.

Kebanyakan organisasi mengatasi masalah ini dengan menyediakan garis panduan kepada pekerja mereka untuk mencipta kata laluan. Standard untuk dasar kata laluan adalah dengan menambah nombor, simbol, huruf besar dan kecil, dan panjang. Sebagai contoh, dasar ini turut digunakan oleh pentadbiran UKM kepada staf mereka seperti dalam sistem e-perolehan UKM (eP@UKM). Menurut Garis Panduan Keselamatan Kata Laluan Pengguna ICT UKM pindaan 2022, staf juga perlu menukar kata laluan mereka sekurang-kurangnya sekali dalam tempoh satu tahun. Perkara ini adalah bertujuan untuk melindungi akaun pengguna dan memastikan keselamatan maklumat universiti terpelihara daripada capaian yang tidak sah. Hal ini kerana kelemahan pengurusan keselamatan kata laluan boleh mendedahkan sistem dan rangkaian universiti kepada serangan penggodam.

Dalam konteks teknologi, menggunakan kata laluan yang kuat adalah penting untuk mengelak daripada pelanggaran data daripada penggodam melalui pemecahan kata laluan *(password cracking)*. Pelanggaran data ialah insiden keselamatan di mana orang dalam atau penyerang luar yang berniat jahat mendapat akses tanpa kebenaran kepada data sulit atau maklumat sensitif. Statistik melaporkan, pada suku pertama 2023, lebih daripada enam juta rekod data telah didedahkan di seluruh dunia melalui pelanggaran data (Statista, 2024). Perkara ini boleh membawa kepada kehilangan privasi dan kecurian identiti kepada individu. Menurut laporan penyiasatan pelanggaran data oleh Verizon pada tahun 2019, 43% daripada serangan siber ditujukan kepada perniagaan kecil, penjagaan kesihatan, agensi kerajaan, institusi kewangan, pendidikan, dan syarikat utiliti. Ini adalah bahaya kerana kebanyakan sektor ini mempunyai maklumat peribadi hampir semua individu seperti rakyat sesebuah negara, dan pelajar-pelajar di institusi pendidikan. Salah satu cara yang digunakan oleh penjenayah siber untuk melanggar sistem dan aplikasi yang dilindungi oleh kata laluan ialah kaedah serangan kekerasan (brute-force attack). Serangan kekerasan ialah serangan di mana penggodam cuba meneka kata laluan pengguna ke akaun dalam talian mereka dengan cepat melalui senarai perkataan, frasa dan kombinasi nombor yang biasa digunakan.

Walaupun amalan untuk penggunaan kata laluan telah dilaksanakan, kata laluan yang lemah tidak dapat menjamin keselamatan data. Cara kata laluan disimpan juga adalah penting untuk melindungi sistem atau maklumat daripada pelanggaran data. Rajah 1.1.3 menunjukkan sebuah gambar yang diambil oleh Associated Press. Dalam gambar tersebut pegawai operasi Hawaii Emergency Management Agency (HEMA) dapat dilihat menunjukkan skrin komputer yang sedang memantau bahaya (Business Insider, 2017). Masalah timbul apabila gambar tersebut tersebar di media sosial kerana nota post-it pada skrin komputer yang mengandungi frasa “Password Warningpoint2”. Manakala, terdapat sebuah kes di mana seorang lelaki telah mencuri mata wang kripto bernilai lebih daripada 575 juta dolar Amerika Syarikat semasa beliau melaraskan sistem keselamatan di rumah mangsa (Tampa Bay Times, 2022). Polis melaporkan beliau mencuri dompet perkakasan Trezor, yang yang membolehkan pengguna menyimpan mata wang kripto di luar talian, dengan menggunakan kata laluan yang disimpan berdekatan dompet tersebut. Kedua-dua kes tersebut menunjukkan bahawa penyimpanan kata laluan yang tidak betul boleh membawa kepada serangan siber. Kata laluan tersebut tidak dilindungi oleh sebarang alat keselamatan, sekaligus membolehkan orang luar untuk menggunakan kata laluan itu untuk mengakses data peribadi mangsa mereka. Oleh sebab itu, orang ramai juga mungkin menggunakan hanya satu kata laluan untuk semua akaun mereka dengan tujuan mudah untuk diingat dan untuk mengelakkan daripada menyimpan kata laluan di tempat yang tidak selamat.



Rajah 1.1.3 Kata laluan pada nota post-it pada skrin komputer di ibu pejabat HEMA
Sumber: Business Insider 2018

METODOLOGI KAJIAN

Model metodologi yang akan digunakan untuk projek ini ialah model agile. Hal ini kerana, ianya bersesuaian dengan pembangunan projek. Model ini baik untuk digunakan bagi projek yang tidak ada pengubahan ketara pada keperluan yang ditetapkan pada awal pembangunan projek. Projek berdasarkan metodologi agile juga baik untuk digunakan dalam projek di mana garis masa tempoh pembangunan telah ditetapkan. Projek ini akan dibangunkan secara berurutan mengikut fasa-fasa dalam model agile.

Fasa keperluan dan analisis

Fasa ini adalah untuk mengenal pasti perkara yang perlu dilakukan untuk membangunkan projek. Keperluan projek akan dikenal pasti berdasarkan apa yang diperlukan oleh pengguna. Fasa ini turut melibatkan pengenal pastian dan penerangan risiko, andaian, kebergantungan, metrik kejayaan, kos, dan garis masa untuk menyiapkan projek. Pada fasa ini, penyelidikan keperluan akan bermula untuk mengenal pasti keperluan untuk membangunkan aplikasi pengurus kata laluan.

Fasa reka bentuk

Pada fasa ini, penyelesaian teknikal akan direka bentuk berdasarkan keperluan yang telah dikenal pasti dalam fasa perancangan dan analisis. Reka bentuk logikal akan dicipta untuk menerangkan tujuan dan skop projek, aliran trafik umum setiap komponen, dan titik integrasi. Kemudian, reka bentuk ini akan diubah kepada reka bentuk fizikal menggunakan perkakasan dan teknologi perisian yang telah dinyatakan dalam fasa sebelumnya. Dalam fasa ini, reka bentuk aplikasi pengurus kata laluan akan dibina dengan merujuk kepada keperluan yang telah ditetapkan dalam fasa 1.

Fasa pelaksanaan

Pada fasa ini, proses pengekodan akan dimulakan berdasarkan keperluan dan spesifikasi projek, dengan beberapa ujian dan pelaksanaan turut berlaku. Jika perubahan ketara diperlukan semasa fasa ini, ini mungkin bermakna kembali ke fasa reka bentuk. Pengekodan aplikasi pengurus kata laluan akan dimulakan untuk memastikan semua keperluan yang ditetapkan dalam fasa 1 dapat ditepati.

Fasa ujian

Fasa ini diperlukan untuk memastikan produk tidak mempunyai ralat dan semua keperluan telah dilengkapkan. Hal ini adalah untuk memastikan pengguna mendapat pengalaman yang baik semasa menggunakan produk tersebut. Fasa ini akan menggunakan pelbagai kes ujian dengan merujuk kepada reka bentuk dan senario kes pengguna untuk menguji produk. Pada fasa ini, aplikasi pengurus kata laluan akan diuji dengan menggunakan pelbagai kes ujian untuk mensimulasikan senario kehidupan sebenar.

Fasa penempatan dan penyelenggaraan

Apabila produk telah dikeluarkan kepada pengguna, fasa penyelenggaraan akan bermula. Produk akan dikemas kini sekiranya terdapat sebarang kecacatan atau mendapat permintaan perubahan daripada pengguna. Fasa ini akan mengeluarkan versi produk yang baharu. Pada fasa ini, aplikasi pengurus kata laluan akan diselenggara sekiranya terdapat sebarang ralat atau permintaan daripada pengguna.

Keperluan pengguna dapat dikenalpasti berdasarkan masalah yang telah dinyatakan. Penyelesaian yang dicadangkan dalam aplikasi yang dibangunkan iaitu Cryptify ialah penjanaan kata laluan yang unik berdasarkan input frasa, penggunaan algoritma penyulitan berganda AES dan RSA, penyimpanan data dalam pangkalan data awan, pengesahan pengguna melalui log masuk dan pengesahan cap jari, dan semakan kekuatan kata laluan sebagai panduan keselamatan.

Reka bentuk kes ujian dibangunkan berdasarkan teknik reka bentuk pengujian yang dipilih iaitu kaedah pengujian kotak hitam. Pengujian dilakukan berdasarkan keperluan fungsian sistem serta spesifikasi kes guna bagi setiap keperluan pengguna. Item yang diuji mestilah memenuhi keperluan yang dinyatakan dalam spesifikasi keperluan sistem. Pengujian perlu dilakukan untuk memastikan aplikasi yang dibina memenuhi semua spesifikasi keperluan sistem yang telah dinyatakan. Pengujian yang dilakukan terhadap aplikasi pengurus kata laluan Cryptify mestilah memenuhi dua kriteria untuk dianggap lulus. Kriteria tersebut ialah:

1. Semua kes uji mestilah lulus.
2. Tiada ralat semasa ujian dijalankan.

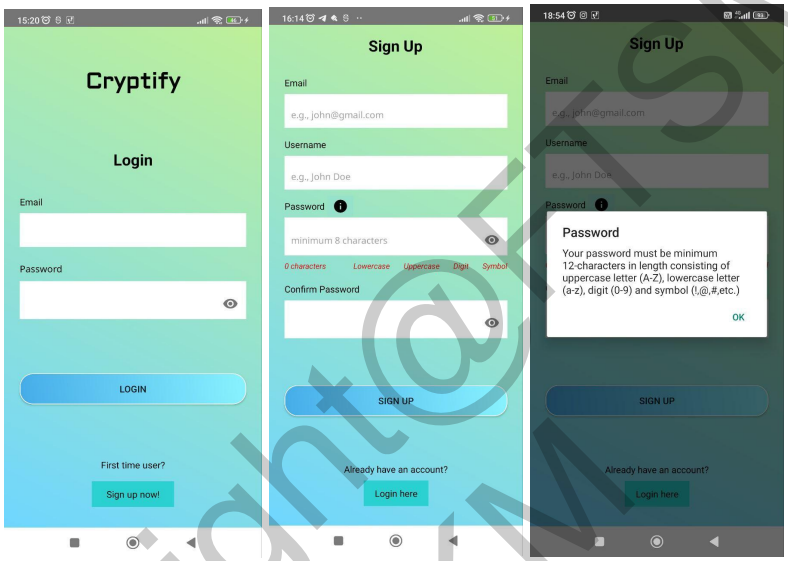
Manakala, pengujian bukan fungsian adalah melibatkan beberapa sukarelawan yang akan menggunakan aplikasi ini dan memberi maklum balas mereka dengan mengisi borang soal selidik. Pengujian yang dijalankan ialah pengujian kebolehgunaan. Pengujian kebolehgunaan digunakan untuk menilai fungsian aplikasi dan memastikan pengguna dapat menavigasinya dengan cekap. Pengujian ini menggunakan borang soal selidik yang merangkumi aspek kebolehgunaan sistem, antara muka dan kualiti sistem yang telah dibangunkan.

KEPUTUSAN DAN PERBINCANGAN

Aplikasi pengurus kata laluan Cryptify berjaya dibangunkan serta memenuhi semua

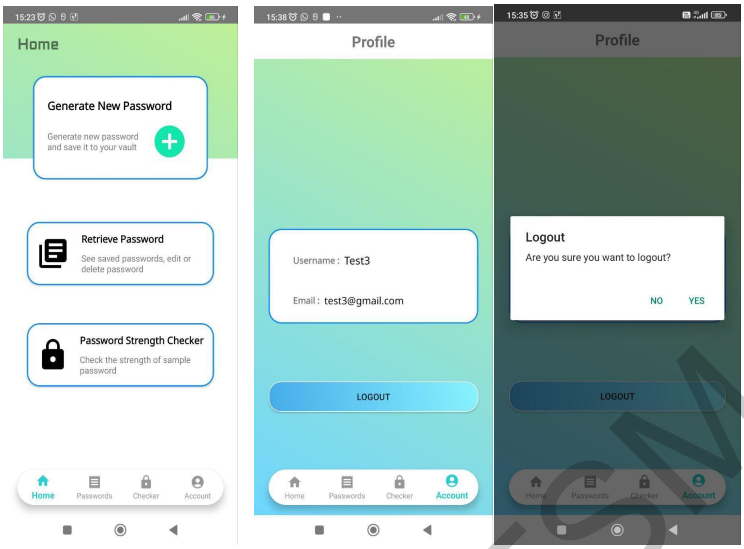
keperluan pengguna yang telah dinyatakan. Aplikasi dibangunkan menggunakan platform Android Studio dan menggunakan Java untuk pembangunan bahagian belakang *(back-end)* serta XML untuk pembangunan bahagian hadapan *(front-end)*. Pangkalan data yang digunakan ialah pangkalan data awan Firebase Firestore untuk menyimpan data pengguna.

Apabila membuka aplikasi Cryptify dalam peranti, sistem akan memaparkan antara muka log masuk. Pengguna yang mempunyai akaun berdaftar boleh log masuk ke dalam sistem menggunakan emel dan kata laluan yang telah didaftarkan. Manakala, pengguna baru boleh mendaftar akaun mereka dengan menekan butang 'Signup'. Pengguna perlu memasukkan semua maklumat yang diperlukan untuk mendaftar akaun. Rajah 1 menunjukkan antara muka log masuk dan daftar akaun.



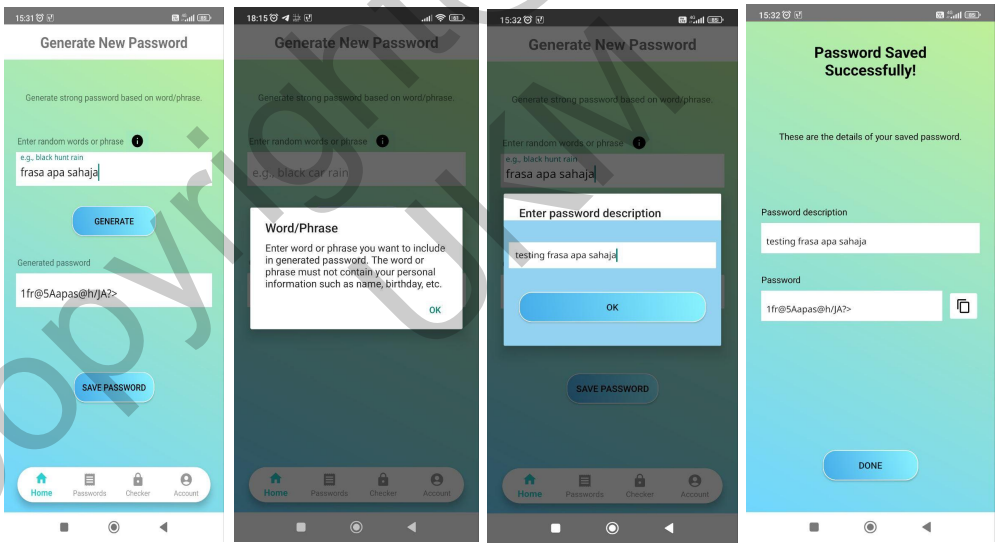
Rajah 1 Antara muka log masuk dan daftar

Apabila pengguna telah log masuk, sistem memaparkan antara muka menu utama. Pengguna boleh menekan butang yang disediakan untuk menjana kata laluan, mendapatkan semula kata laluan yang telah disimpan, atau menyemak kekuatan kata laluan. Untuk log keluar, pengguna boleh navigasi ke profil pengguna dengan menekan ikon profil pada menu navigasi dan tekan butang 'Logout'. Rajah 2 menunjukkan antara muka menu utama, profil dan log keluar.



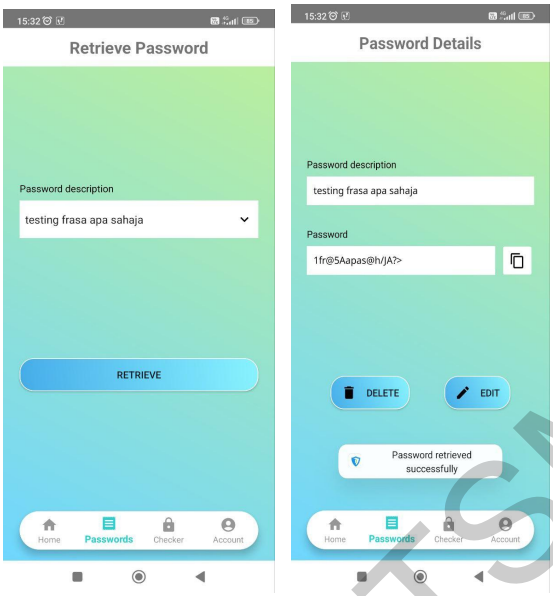
Rajah 2 Antara muka menu utama, profil dan log keluar

Untuk menjana kata laluan, pengguna perlu memasukkan frasa rawak dan tekan butang 'Generate'. Pengguna boleh simpan kata laluan yang telah dijana dengan menekan butang 'Save password' dan masukkan deskripsi kata laluan. Rajah 3 menunjukkan antara muka menjana dan menyimpan kata laluan.



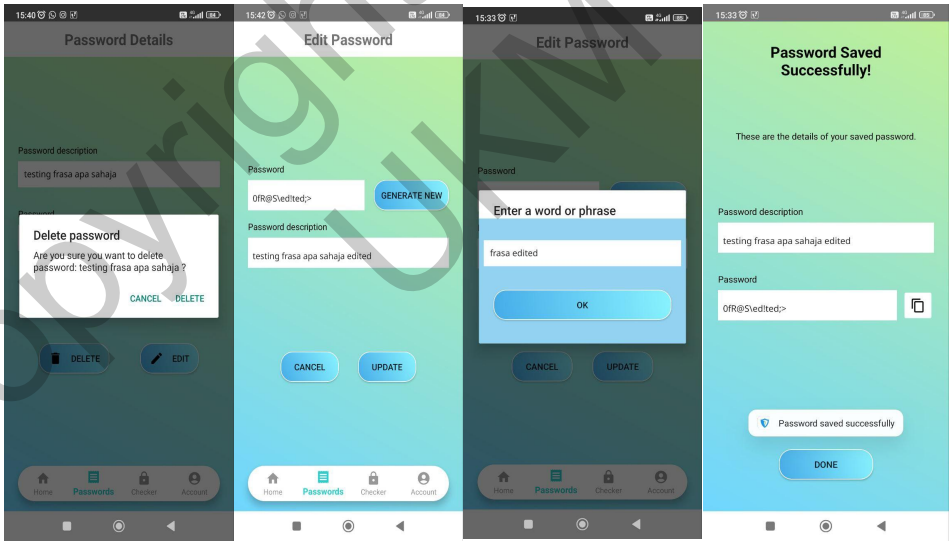
Rajah 3 Antara muka menjana dan menyimpan kata laluan

Untuk mendapatkan semula kata laluan yang telah disimpan, pengguna boleh pilih deskripsi kata laluan yang berkenaan dan tekan butang 'Retrieve'. Pengguna perlu membuat pengesahan cap jari sebelum sistem paparkan butiran kata laluan. Rajah 4 menunjukkan antara muka mendapatkan semula kata laluan.



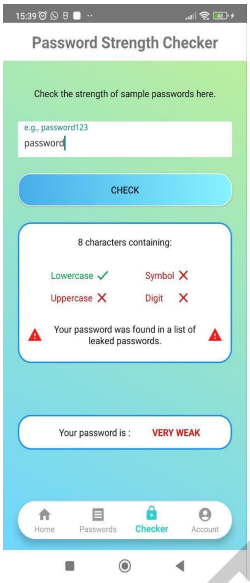
Rajah 4 Antara muka mendapatkan semula kata laluan

Setelah mendapatkan semula kata laluan, pengguna boleh memadam atau kemaskini kata laluan. Kemaskini kata laluan menggunakan proses yang seperti menjana dan menyimpan kata laluan. Manakala, pengguna perlu mengesahkan pemadaman kata laluan dengan tekan 'OK'. Rajah 5 menunjukkan antara muka memadam dan mengemaskini kata laluan.



Rajah 5 Antara muka memadam dan mengemaskini kata laluan

Pengguna boleh menyemak kata laluan dengan memasukkan sampel kata laluan dan tekan butang 'Check'. Sistem akan paparkan maklumat berkenaan kata laluan seperti Rajah 6.



Rajah 6 Antara muka menyemak kekuatan kata laluan

Pengujian Fungsian

Pengujian fungsian dilaksanakan oleh seorang untuk memerhatikan dan membuat penilaian terhadap fungsi aplikasi. Pengujian yang dilakukan merangkumi setiap kes guna yang telah ditetapkan. Pengujian yang dilakukan menunjukkan kriteria item lulus atau gagal. Lulus nermaksud pengujian yang dilakukan tiada ralat dan berfungsi dengan sepatutnya, dan sebaliknya untuk item gagal. Jadual 1 menunjukkan keputusan pengujian yang diperoleh.

Jadual 4.7.1 Keputusan pengujian

ID Fungsi	Fungsian	Senario Pengujian	Keputusan senario	Lulus/ Gagal
F01	Mendaftar akaun	Pengguna mendaftar tanpa mengisi semua maklumat yang diperlukan	Sistem paparkan mesej “Please enter all details required”	Lulus
		Pengguna mendaftar menggunakan e-mel yang telah didaftarkan	Sistem paparkan mesej “Signup failed”	Lulus
		Pengguna mendaftar menggunakan format e-mel yang tidak betul	Sistem paparkan mesej “Signup failed”	Lulus
		Pengguna mendaftar menggunakan nama pengguna yang telah didaftarkan	Sistem paparkan mesej “Signup failed”	Lulus
		Pengguna mendaftar	Sistem paparkan mesej	Lulus

		menggunakan kata laluan yang tidak mengikut syarat	"Invalid password"	
		Pengguna mengisi sahkan kata laluan yang tidak sepadan	Sistem paparkan mesej "Password doesn't match. Please try again."	Lulus
		Pengguna mendaftar dengan mengisi setiap maklumat dengan betul	Sistem paparkan mesej "Account created" dan paparkan menu utama	Lulus
		Pengguna mendaftar tanpa sambungan Internet	Sistem paparkan mesej "Signup failed"	Lulus
F02	Log masuk	Pengguna log masuk tanpa mengisi semua maklumat yang diperlukan	Sistem paparkan mesej "Please enter email and password"	Lulus
		Pengguna log masuk menggunakan e-mel yang tidak berdaftar	Sistem paparkan mesej "Login failed"	Lulus
		Pengguna log masuk menggunakan kata laluan yang salah	Sistem paparkan mesej "Login failed"	Lulus
		Pengguna log masuk menggunakan e-mel dan kata laluan yang telah didaftarkan	Sistem paparkan mesej "Login successful" dan paparkan antara muka menu utama	Lulus
		Pengguna log masuk tanpa sambungan Internet	Sistem paparkan mesej "Login failed"	Lulus
F03	Menjana kata laluan	Pengguna menjana kata laluan tanpa mengisi frasa	Sistem paparkan mesej "Please enter a phrase"	Lulus
		Pengguna menjana kata laluan menggunakan frasa yang tidak betul	Sistem paparkan mesej "Invalid phrase"	Lulus
		Pengguna menjana kata laluan menggunakan frasa yang betul	Sistem paparkan kata laluan yang dijana dan paparkan butang 'Save Password'	Lulus
F04	Menyimpan kata laluan	Pengguna menyimpan kata laluan tanpa mengisi deskripsi kata laluan	Sistem paparkan mesej "Please enter password description"	Lulus

		Pengguna menyimpan kata laluan menggunakan deskripsi kata laluan yang telah digunakan	Sistem paparkan mesej "Password for: [deskripsi kata laluan] already exists"	Lulus
		Pengguna menyimpan kata laluan menggunakan deskripsi kata laluan yang unik	Sistem paparkan mesej "Password saved successfully" dan paparkan antara muka 'Kata laluan berjaya disimpan'.	Lulus
		Pengguna menyimpan kata laluan tanpa sambungan Internet	Sistem paparkan mesej "Cannot connect to database. Please check your Internet connection"	Lulus
F05	Mendapatkan semula kata laluan	Pengguna mendapatkan kata laluan menggunakan cap jari yang tidak didaftarkan dalam peranti	Sistem paparkan mesej "Not recognised"	Lulus
		Pengguna mendapatkan kata laluan menggunakan cap jari yang telah didaftarkan dalam peranti	Sistem paparkan mesej "Password retrieved successfully" dan paparkan antara muka butiran kata laluan	Lulus
F06	Mengemaskini kata laluan	Pengguna menjana kata laluan yang baru tanpa mengisi frasa	Sistem paparkan mesej "Please enter a phrase"	Lulus
		Pengguna menjana kata laluan yang baru menggunakan frasa yang tidak betul	Sistem paparkan mesej "Invalid phrase"	Lulus
		Pengguna mengemaskini kata laluan menggunakan deskripsi kata laluan yang telah digunakan dan bukan deskripsi kata laluan yang asal	Sistem paparkan mesej "Password for: [deskripsi kata laluan] already exists"	Lulus
		Pengguna mengemaskini kata laluan tanpa mengubah kata laluan atau deskripsi kata laluan yang asal	Sistem paparkan mesej "Password saved successfully" dan paparkan antara muka 'Kata laluan berjaya disimpan'.	Lulus
		Pengguna mengemaskini kata laluan menggunakan kata laluan atau deskripsi kata laluan yang unik	Sistem paparkan mesej "Password saved successfully" dan paparkan antara muka 'Kata laluan berjaya disimpan'.	Lulus
		Pengguna mengemaskini kata laluan tanpa sambungan Internet	Sistem paparkan mesej "Cannot connect to database.	Lulus

			Please check your Internet connection"	
F07	Memadam kata laluan	Pengguna tekan 'Cancel' pada tetingkap timbul	Tiada ralat	Lulus
		Pengguna memadam kata laluan dengan menekan 'Delete' pada tetingkap timbul	Sistem paparkan mesej "Password deleted successfully" dan paparkan antara muka mendapatkan semula kata laluan	Lulus
F08	Menyemak kekuatan kata laluan	Pengguna menyemak kata laluan tanpa mengisi sampel kata laluan yang hendak disemak	Sistem paparkan mesej "Please enter a sample password"	Lulus
		Pengguna menyemak kata laluan dengan mengisi sampel kata laluan	Sistem mengemaskini panjang kata laluan, dan warna teks panjang kata laluan, 'Lowercase', 'Uppercase', 'Digit' dan 'Symbol'.	Lulus
			Sistem paparkan amaran bagi kata laluan yang terlalu pendek atau kata laluan yang terdapat dalam senarai kata laluan yang telah dibocorkan.	
F09	Log keluar	Pengguna tekan 'No' pada tetingkap timbul	Tiada ralat	Lulus
		Pengguna tekan 'Yes' pada tetingkap timbul	Sistem paparkan mesej "Password deleted successfully" dan paparkan antara muka mendapatkan semula kata laluan	Lulus

Cadangan Penambahbaikan

Berdasarkan aplikasi yang telah dibangunkan, terdapat cadangan penambahbaikan untuk meningkatkan kualiti aplikasi pengurus kata laluan Cryptify. Pembangunan fungsi-fungsi tambahan seperti menyimpan fail sulit dan mendapatkan tips keselamatan berkenaan keselamatan kata laluan juga boleh dilakukan. Aplikasi ini juga boleh ditambahbaik dengan menyediakan alternatif untuk menggunakan fungsi-fungsi yang ada walaupun tanpa sambungan Internet seperti menyimpan pangkalan data sandaran pada peranti pengguna. Aplikasi juga boleh ditambahbaik dengan pembangunan aplikasi yang boleh berintegrasi dengan pelbagai jenis sistem operasi dan platform. Sistem aplikasi juga boleh menambah fungsi untuk menukar tetapan bahasa pengguna kepada Bahasa Melayu.

KESIMPULAN

Aplikasi pengurus kata laluan Cryptify dibangunkan bagi memudahkan pengguna untuk mengurus kata laluan mereka dengan selamat. Aplikasi ini turut dibangunkan dengan tujuan untuk menyelesaikan masalah-masalah yang telah dinyatakan dalam Bab I. Aplikasi ini membantu pengguna untuk menjana kata laluan yang kuat dan tahan kepada ancaman siber dengan adanya algoritma penyulitan. Pembaharuan yang diimplementasikan dalam aplikasi Cryptify ialah algoritma penyulitan berganda, di mana kata laluan disulitkan menggunakan algoritma penyulitan AES diikuti algoritma penyulitan RSA. Melalui aplikasi ini, pengguna juga boleh menyemak kekuatan kata laluan. Walaupun terdapat kekurangan dalam aplikasi ini berbanding dengan aplikasi pengurus kata laluan yang sedia ada, aplikasi Cryptify membantu untuk memudahkan pengguna dalam menjamin keselamatan kata laluan daripada serangan kekerasan dan pelanggaran data.

Kekuatan Sistem

Aplikasi pengurus kata laluan Cryptify yang dibangunkan memenuhi keperluan-keperluan pengguna yang telah ditetapkan dalam Bab III. Oleh itu, projek ini berjaya mencapai objektif pembangunan sistem serta berjaya menyelesaikan masalah yang telah dinyatakan dengan pembangunan fungsi dan sistem yang tepat. Antara kelebihan aplikasi ini ialah aplikasi yang dibangunkan ialah mesra pengguna dan mudah untuk difahami. Selain itu, keselamatan yang diberikan melalui algoritma penyulitan berganda meningkatkan kualiti kata laluan. Akhir sekali, aplikasi menyediakan fitur yang menarik dan mudah untuk digunakan dalam kehidupan seharian.

Kelemahan Sistem

Terdapat beberapa kekurangan yang berjaya dikenalpasti dalam aplikasi. Aplikasi pengurus kata laluan Cryptify mempunyai fungsi yang terhad. Antara perkara yang perlu diambil kira adalah keperluan sambungan Internet bagi aplikasi ini untuk berfungsi sepenuhnya seperti aplikasi yang ada di pasaran. Aplikasi ini dibangunkan hanya mengambil kira sistem pengoperasian Android yang lebih mudah kepada pembangun dan direka dalam Bahasa Inggeris sahaja. Hal ini boleh menyebabkan kerumitan bagi pengguna yang tidak fasih Bahasa Inggeris untuk menggunakan aplikasi.

PENGHARGAAN

Setinggi-tinggi penghargaan ditujukan kepada Dr. Dahlila Putri Dahnil Sikumbang atas bimbingan, nasihat, dan dorongan yang berharga sepanjang penyusunan laporan ini. Kehadiran beliau telah memberikan arahan yang sangat bermakna dalam mengasah pemikiran dan penulisan saya. Terima kasih diucapkan kepada ibu saya, Murni Binti Hasan atas segala sokongan yang tidak pernah putus sepanjang tempoh penulisan laporan ini.

Tidak lupa juga jasa rakan-rakan saya yang sentiasa berkongsi maklumat dan memberi bimbingan untuk menyiapkan laporan ini. Terima kasih sekali lagi diucapkan kepada semua

pihak yang telah menyumbang dalam proses ini. Semoga hasil projek ini memberikan manfaat kepada bidang ilmu dan masyarakat

RUJUKAN

Chapple, M & Cole, B. The difference between AES and DES encryption. https://www.techtarget.com/searchsecurity/answer/The-difference-between-AES-encryption-and-DES-encryption [20 November 2023]

Cobb, M. 2021. Definition: RSA algorithm (Rivest-Shamir-Adleman). https://www.techtarget.com/searchsecurity/definition/RSA#:~:text=The%20RSA%20algorithm%20(Rivest%2DShamir%2DAdleman)%20is%20the,an%20insecure%20network%20such%20as [20 November 2023]

Florackis, C., Louca, C., Michaely, R. & Weber, M. 2023. Cybersecurity risk. The Review of Financial Studies 36:351-407

Leswing, K. 2018. A password for the Hawaii emergency agency was hiding in a public photo, written on a Post-it note. https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1[18 November 2023]

National Cyber Security Center (NCSC). 2019. Passwords, passwords everywhere. https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere [19 November 2023]

Taylor, L. 2022. Pinellas Park man stole nearly $600,000 in cryptocurrency, police say. Tampa Bay Times. https://www.tampabay.com/news/breaking-news/2022/04/09/pinellas-park-man-stole-nearly-600000-in-cryptocurrency-police-say/ [20 November 2023]

Vicente, V. 2023. NIST Password Guidelines 2023. https://www.auditboard.com/blog/nist-password-guidelines/ [19 November 2023]

Western Governors University (WGU). 2021. 6 Industries Most Vulnerable to Cyber Attacks. https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks2108.html#close [20 November 2023]

Nur Azrina Amira Binti Salehhuddin (A187944)
Dr. Dahlila Putri Dahnil Sikumbang
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia