PENYEBARAN KEKUNCI KESELAMATAN DALAM SISTEM PENGESAHAN LOG MASUK KOD QR

Loo Wooi Chun

Ts. Dr. Khairul Azmi Abu Bakar

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Pada masa sekarang, banyak aplikasi web memerlukan pengguna untuk mendaftar akaun dan log masuk untuk menggunakan perkhidmatan. Oleh itu, pengguna perlukan modul untuk menjamin proses log masuk yang senang dan selamat. Masalah yang dihadapi oleh sistem log masuk adalah masalah untuk mendapat pengesahan melalui kunci keselamatan. Tujuan projek ini adalah membangunkan satu modul penyebaran kekunci keselamatan dan integrasi ke sistem log masuk menggunakan kod QR, kunci keselamatan akan digunakan untuk meningkatkan efisien dan keselamatan proses log masuk. Pengguna hanya memerlukan aplikasi mudah alih untuk mengimbaskan kod QR dari pelayar web, selepas pengguna mendapat kod QR yang mengandungi kunci keselamatan, pengguna dapat log masuk dengan mengimbaskan kod QR dari aplikasi mudah alih ke pelayar web, dengan cara ini pengguna tidak perlu sering ingat nama dan kata laluan akaun. Sistem laman web akan dibangunkan menggunakan HTML5 dan aplikasi akan dibangunkan melalui android studio. Produk perisian akhir adalah modul penyebaran kekunci keselamatan yang integrasi ke dalam sistem log masuk. Kunci keselamatan akan dijanakan semasa pengguna mendaftar, kunci keselamatan akan dipapar dalam bentuk kod QR dan disemak semasa pengguna ingin log masuk.

1 PENGENALAN

Teknologi pintar semakin maju dan mantap sejak abad ke-21, teknologi penyebaran

kekunci menjadi semakin penting dalam bidang komputer, terutamanya dalam sistem yang mengandungi informasi sensitif seperti sistem log masuk, pembayaran. Fungsi modul penyebaran kekunci dapat mengehad akses daripada peranti yang tidak disahkan. Manakala salah satu cara yang digunakan untuk pindahkan kunci keselamatan .

Antara teknologi label yang boleh menyimpan data digunakan secara luas dalam industri ialah barkod, kod QR dan RFID(*Radio-frequency identifacation*), teknologi tersebut digunakan di situasi yang berlainan disebabkan oleh ciri-cirinya. Teknologi berikut mempunyai kebolehan menyimpan data sensitif dan pindah dari komputer kepada telefon pintar.

kod QR ialah *Quick Response Code* yang bermakna kod yang bertindak balas dengan cepat, ia mempunyai keupayaan menyimpan 7000 perkataan(K. Saranya. *Modern applications of QR-Code for security*), kod QR kini telah dinaikan taraf dan dibaiki supaya boleh menjana kekunci keselamatan yang mempunyai sama informasi pada masa yang berbeza, selain itu kod QR mempunyai kebolehan untuk dapat informasi dalam kod QR yang tidak lengkap. Dalam kriptografi, informasi yang boleh disimpan dalam kod QR ialah kunci keselamatan.

Untuk mendapatkan pengesahan dengan implikasi modul penyebaran kekunci, pihak web dan pihak aplikasi Android mestilah mempunyai kunci keselamatan yang sama, dan kunci keselamatan harus dijaga dengan baik supaya tidak dicuri oleh pihak ketiga. Kunci keselamatan juga harus dijanakan algoritma yang baik supaya kunci keselamatan panjang dan kompleks.

Modul penyebaran kekunci boleh berintegrasi dalam sistem log masuk. Pusat penyebaran kekunci akan dibangunkan di dalam web untuk memudahkan penyebaran kunci keselamatan. Setiap peranti akan mendapat identiti unik yang terdiri dari kunci keselamatan untuk pengesahan log masuk ke akaun. Kunci keselamatan amat diperlukan untuk mewujudkan sambungan selamat ke pangkalan supaya akaun tidak diguna oleh peranti yang tidak mempunyai kunci keselamatan. Aplikasi telefon pintar

yang belum dapat kunci keselamatan boleh menerima kunci keselamatan dari web yang menggunakan modul penyebaran kekunci supaya aplikasi telefon tersebut boleh mendapat kunci keselamatan.

Walaupun kapasiti kod QR terhad, tapi kunci keselamatan yang singkat boleh diimbas ke dalam telefon pintar. Kod QR yang dijanakan oleh peranti yang dapat kunci keselamatan susah untuk digodamkan oleh pihak ketiga, kod QR dinamik juga menjamin sistem lebih selamat, disebabkan oleh ciri-ciri kod QR, ia sesuai untuk digunakan dalam proses pengesahan kunci keselamatan. Pada masa sekarang, aplikasi kod QR kian menjadi satu cara praktikal untuk log masuk dalam akaun, kerana penggunaan kunci keselamatan dalam proses log masuk mudah dan selamat. Universiti Sains Islam Malaysia juga guna transaksi kewangan dengan kod QR dan kunci keselamatan mulai tahun 2018. (Utusan Online 2018).

2 PENYATAAN MASALAH

Pada masa sekarang, kata laluan masih merupakan cara pengesahan yang paling banyak digunakan, tetapi pengguna gemar guna kata laluan yang senang ingat iaitu nombor telefon, nombor kad pengenalan, nama, alamat atau e-mel, kata laluan yang mengandungi perkataan sensitif senang diteka.

Walaupun kata laluan yang dijanakan secara rawak mempunyai tahap keselamatan yang lebih tinggi, pada masa yang sama, pengguna juga menghadapi masalah untuk ingat kata laluan. Untuk meningkatkan tahap keselamatan, pengguna dinasihatkan supaya tukar kata laluan setiap tiga bulan. Walaubagaimanapun, pengguna boleh catat kata laluan yang kompleks secara manual, tapi pengguna hilangkan catatan bermaksud pengguna tidak dapat log masuk ke sistem lagi.

Tidak banyak sistem yang selamat dan senang digunakan di pasaran, jika kata laluan diketahui oleh pihak ketiga, kerugian kepada pengguna tidak hanya dalam segi

kewangan, pengguna biasa tidak akan tahu bila, mana, dan kenapa akaun akan digodam oleh sesiapa. Oleh itu, satu sistem pengesahan yang mantap, selamat, senang diguna patut dibangunkan untuk membantu pengguna untuk menyelesai masalah.

Terdapat juga sistem yang tidak menggunakan sistem kunci keselamatan, masalah akan timbul jika kata laluan ditahui oleh pihak ketiga, pengesahan tidak dilakukan sekiranya kata laluan betul, hal ini menyebab penggodam hanya perlu mencuri kata laluan sahaja untuk akses ke akaun pengguna lain. Isu yang sering dilupakan oleh pengguna ialah masalah jurutera sosial, kata laluan mudah dicuri oleh pihak ketiga jika pengguna tidak meningkatkan kewaspadaan dan kesedaran keselamatan sistem.

Untuk meningkatkan keselamatan sistem log masuk menggunakan kod QR, modul penyebaran kekunci keselamatan perlu berintegrasi ke dalam sistem kod QR, buat masa sekarang, penyebaran kekunci keselamatan yang dilakukan secara manual sangat tidak efektif. Masalah yang dihadapi ialah menambah efisien penyebaran kekunci keselamatan.

Modul penyebaran kekunci keselamatan sangat diperlukan melindungi akaun pengguna. Tapi, penggunaan modul penyebaran kekunci pula mempunyai masalah teknikal terutamanya integrasi ke dalam sistem sedia ada. Pembinaan sistem penyebaran kekunci merupakan satu cabaran jika seseorang tidak mempunyai ilmu berkaitan, setiap langkah untuk menjana kunci keselamatan dan pindahan kunci keselamatan perlu difahami oleh pembangun sistem supaya boleh tambah baik sistem dari semasa ke semasa.

3 OBJEKTIF KAJIAN

Projek ini bertujuan untuk membangunkan modul penyebaran kekunci dalam sistem pengesahan akaun untuk memudahkan proses log masuk. Pada masa yang sama, aplikasi

mudah alih juga perlu dibangunkan untuk memudahkan simpanan kunci keselamatan akaun dalam sistem. Modul ini juga dibangunkan dalam bentuk boleh berfungsi dalam keadaan tiada sambungan internet.

4 METODOLOGI PROJEK

Metodologi merupakan kepada tatacara untuk sesuatu kajian atau projek untuk mencapai objektif yang ditetapkan. Bagi projek ini, kaedah yang digunakan ialah Metodologi Agile. Kaedah Agile adalah sekumpulan metodologi pembangunan perisian berdasarkan model yang berulang kali, metodologi Agile dapat menjamin kualiti yang ditetapkan dan ada luang perkembangan yang luas, proses yang sering berulang membolehkan penambahbaikan secara berterusan dan dapat mengesan masalah yang sering membawa masalah.

4.1 Fasa Perancangan

Fasa ini mengandungi proses seperti mengenal pasti masalah dan objektif. Sorotan susastera yang teliti juga harus dijalankan, pengajian, pengumpulan, pencarian dan pembacaan kajian yang lalu dapat memberi idea dan inspirasi kepada projek seterusnya. Maklumat yang dikumpulkan dapat dipersembahkan dalam fasa analisis.

4.2 Fasa Analisis

Fasa ini bertujuan untuk analisis maklumat yang dikumpulkan dalam fasa sebelum ini. Analisis berkaitan dengan kesesuaian dan potensi projek. Pengajian berkaitan dengan penggunaan perisian dan perkakasan akan dijalankan untuk memastikan proses pembangunan lancar.

4.3 Fasa Reka Bentuk

Fasa ini adalah fasa paling penting dan ambil masa dalam seluruh projek. Fasa ini mengandungi proses reka bentuk dan pembangunan projek. Pelbagai perisian perlu digunakan untuk proses pembangunan.

Dalam proses membangunkan projek, sambungan internet diperlukan untuk sentiasa membetulkan kesalahan dalam projek. Format data juga perlu ditentukan supaya pelayar web dapat mendapatkan maklumat dengan cara yang betul dalam aplikasi *Android*.

4.4 Fasa Pengujian

Fasa ini adalah bertujuan untuk beruji segala fungsi yang direka. Segala fungsi utama seperti log masuk menggunakan kata laluan dan kod QR akan diuji dan memastikan fungsi tersebut tiada masalah. Sekiranya fungsi tertentu tidak dapat mencapai kriteria yang ditetapkan, penyelarasan perlu dijalankan atau mengimbas kembali fasa analisis untuk membuat tambah baik kajian.

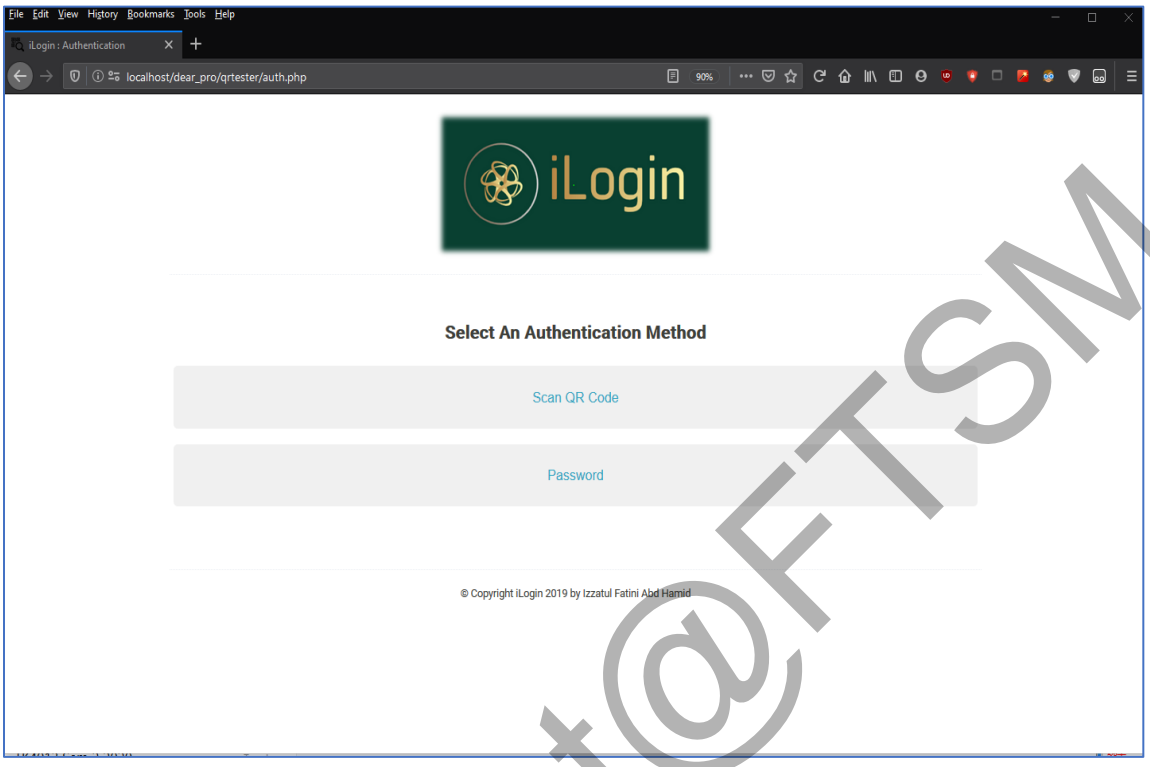
Segala persediaan dari segi perisian dan perkakasan perlu dipilih dengan betul untuk menyesuaikan pembangunan projek. Spesifikasi komputer perlu mempunyai kuasa yang cukup untuk pembangunan projek pelayar web dan aplikasi Android. Dari segi perisian pula, modul yang digunakan perlu berfungsi di telefon pintar terkini, oleh itu, versi dan sdk Android harus dipilih dengan teliti.

5 HASIL KAJIAN

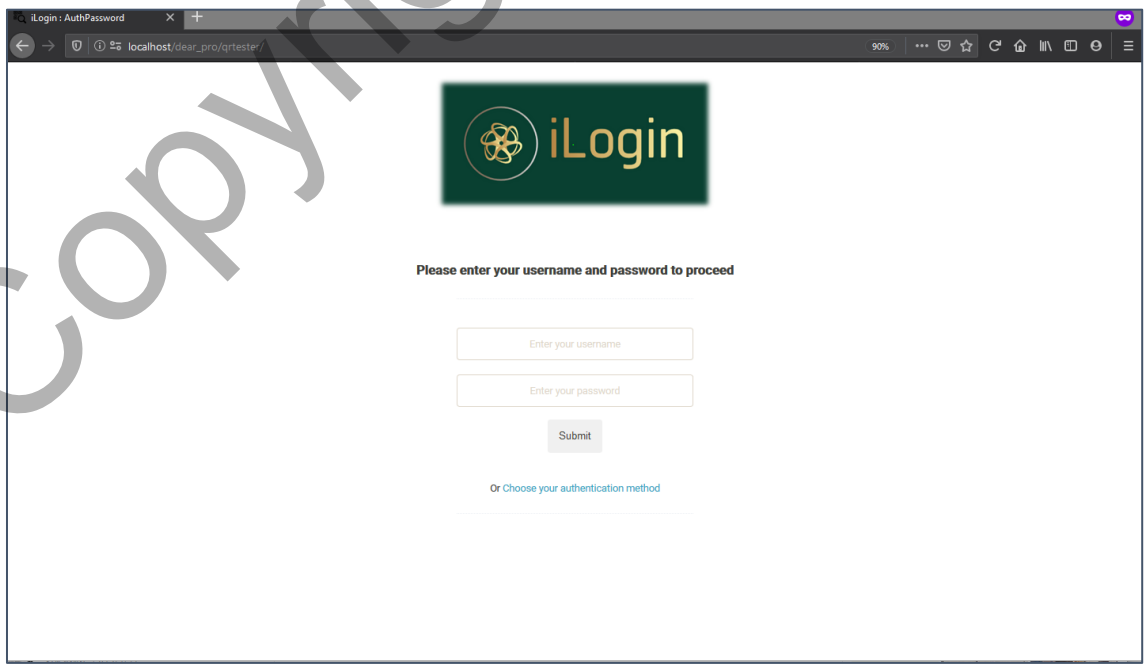
Dalam projek ini, projek pelayar web dibangunkan melalui *php* dan *javascript* dengan *Sublime*, manakala aplikasi Android dibangunkan dengan Android Studio. Proses log masuk dapat dijalankan dengan menggunakan phpMyadmin.

Antara muka sistem iLogin dan modul penyebaran kekunci keselamatan akan ditunjuk, antara muka yang ringkas dan teratur dapat membantu pengguna untuk mahir dalam mengguna sesuatu aplikasi.

Berikut akan menerangkan antara muka sistem iLogin dan menunjuk cara guna sistem ini.

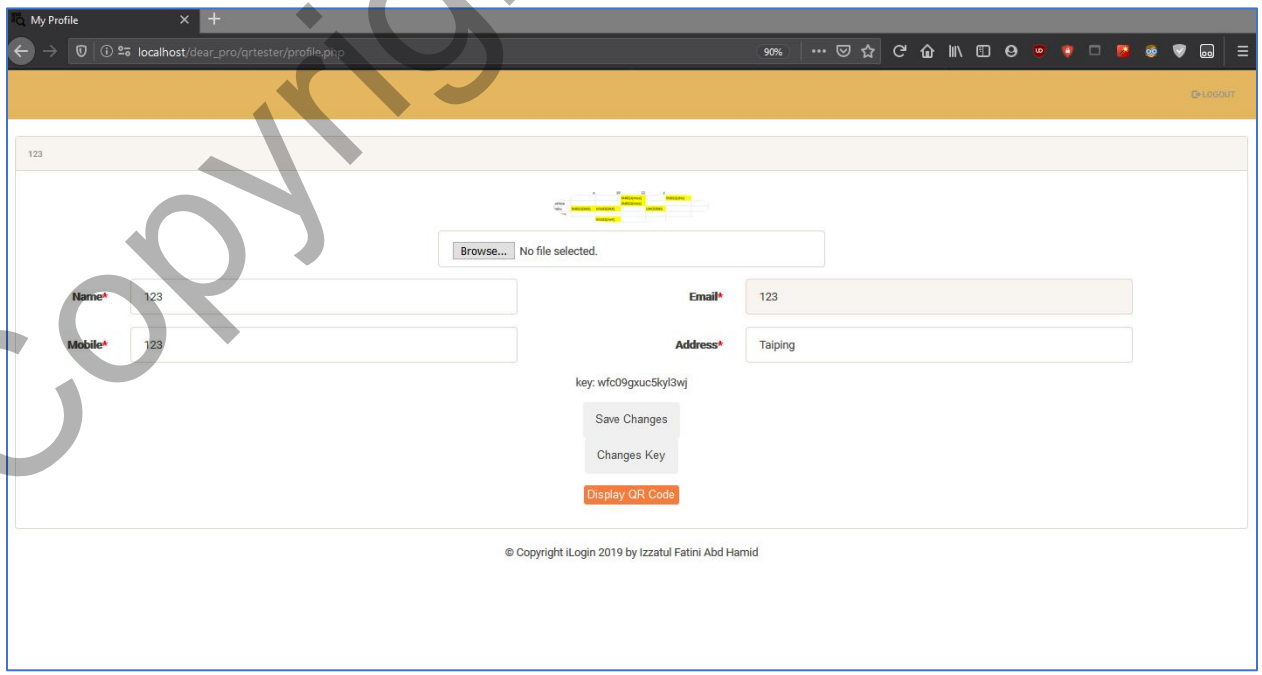


Rajah 1 Antara muka log masuk



Rajah 2 Antara muka log masuk mengguna kata laluan

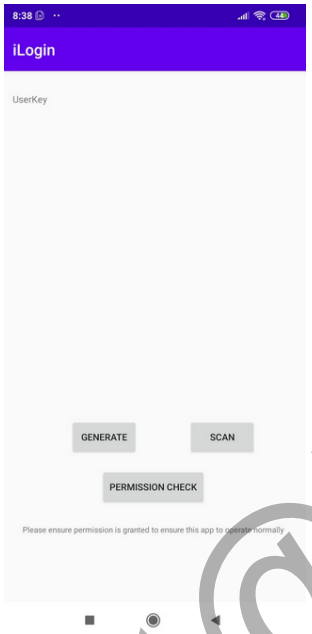
Rajah 3 Antara muka log masuk mengguna kod QR



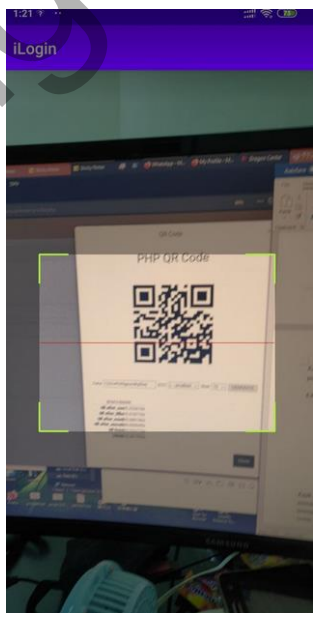
Rajah 4 Antara muka halaman utama web

Rajah 5 paparan kod QR dalam halaman utama web

Rajah 4 hingga Rajah 5 menunjukkan halaman utama web, pengguna bole kemas kini maklumat pengguna dan tukar kunci keselamatan, kunci keselamatan juga boleh dipapar sebagai kod QR.



Rajah 6 Antara muka aplikasi android iLogin



Rajah 7 Antara muka log masuk

Rajah 8 Antara muka log masuk

Rajah 6 menunjukkan antara muka utama aplikasi mudah alih iLogin, seterusnya Rajah 7 menunjukkan aplikasi iLogin menerima kunci keselamatan dan simpan di aplikasi. Rajah 8 pula menunjukkan aplikasi iLogin dapat menjana kod QR daripada kunci keselamatan untuk log masuk ke sistem.

6 KESIMPULAN

Kesimpulannya, modul penyebaran kekunci keselamatan boleh meningkatkan tahap keselamatan dan kebolehan dalam sistem log masuk yang menggunakan kod QR. kunci keselamatan amat berguna dalam pengesahan akaun dalam sistem log masuk, terutamanya sistem log masuk melalui kod QR yang tidak bergantung kepada nama dan kata laluan akaun, jadilah modul penyebaran kekunci keselamatan patut integrasi ke sistem log masuk untuk meningkatkan tahap keselamatan, pada masa yang sama juga mengurangkan masa untuk mengesahkan pengguna adalah pengguna yang sah. Masalah yang utama dihadapi ialah masalah teknikal semasa mengintegrasi modul tersebut ke sistem log masuk yang sedia ada.

7 RUJUKAN

Haeryong Park ; Wan S. Yi ; Gang Shin Lee 2010 Simple ID-Based Key Distribution Scheme 15 May https://ieeexplore.ieee.org/document/5476515

Ajeet P. Singh ; Swapnil M. Potey ; Ferdous A. Barbhuiya ; Sukumar Nandi 2012 A Scalable and Secure Key Distribution Mechanism for Multicast Networks 11 Aug 2012 https://ieeexplore.ieee.org/document/6305591

Zongmin Cui ; Hong Zhu ; Jing Yu 2014 Secure management of key distribution in cloud scenarios 14-Dec https://ieeexplore.ieee.org/document/7062498

TARUN AGARWAL 2015. What is Android? Introduction of Android OS; it's Application 11 December https://elprocus.com/what-is-android-introduction-features-applications/

Utusan Online 2018 Transaksi guna QR Code, USIM kini jadi kampus tanpa tunai 23 Mei https://www.utusan.com.my/malaysia-kita/berita/transaksi-guna-qr-code-usim-kini-jadi-kampus- tanpa-tunai-1.678243

Cambridge University Press 2006 Security analysis of quantum key distribution 10 ogos https://www.cambridge.org/core/books/quantum-cryptography-and-secretkey-distillation/security-analysisofquantumkeydistribution/DE86B0BA63503434F5B05AD0B11852D4

Sumit Tiwari 2016 An Introduction to QR Code Technology 22 Dec https://ieeexplore.ieee.org/document/7966807

P. Vijayakumar, S. Bose, A. Kannan, S. Siva Subramanian 2010 A Secure Key Distribution Protocol for Multicast Communication 12 Jun https://link.springer.com/chapter/10.1007/978-3-642-19263-0_30

Adhatrao, K.Gaykar, A.Jha, R.& Honrao, V.(n.d.) A SECURE METHOD FOR SIGNING IN USING QUICK RESPONSE CODES WITH MPBILE AUTHENTICATION. Internasional Journal of Student Research In Technology & Management,1(1), 1 November. Retrieved form www.giapjournals.com

K. Saranya ; R.S. Reminaa ; S. Subhitsha 2016 Modern applications of QR-Code for security https://ieeexplore.ieee.org/document/7569235