SISTEM 2FA UNTUK KESELAMATAN PEMAPAR WEB DICOM

NURSUHAILI BINTI JUNAIDI
DR KHAIRUL AKRAM BIN ZAINOL ARIFFIN

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Keselamatan rangkaian telah menjadi isu utama sejak dahulu lagi. Kerahsiaan, integriti dan ketersediaan data adalah kebimbangan utama mana-mana pentadbir rangkaian. Pada beberapa bulan lepas, telah berlakunya serangan yang mengakibatkan kehilangan besar sumber dan ketersediaan data. Sebagai contoh, pada Mei 2017, integriti perubatan di United Kingdom telah lumpuh akibat serangan siber perisian tebusan WannaCry di seluruh dunia. Oleh itu, objektif utama kertas kerja ini adalah untuk mencadangkan seni bina rangkaian yang lebih selamat yang akan direka bentuk untuk kes PACS dan DICOM yang digunakan untuk menyimpan dan menghantar imej dan laporan radiografi melalui rangkaian dalaman hospital. Kertas kerja ini mencadangkan untuk menggunakan pengesahan berbilang faktor seperti 2FA sebagai langkah untuk membendung akses yang tidak sah kepada pemapar web DICOM. Novelti pendekatan ini ialah dalam reka bentuk 2FA pada pemapar web DICOM yang mengawal dan memantau kesahihan identiti pengguna sebelum mengakses pemapar. 2FA dipilih sebagai alternatif keselamatan kerana 2FA meneutralkan risiko berkaitan dengan kata laluan yang terjejas.

1 PENGENALAN

Keselamatan data ialah isu kritikal dalam sesebuah organisasi yang mana pengurusan keselamatan maklumat (ISM) yang tepat ialah proses berterusan yang bertujuan untuk membina dan mengekalkan program, dasar dan kawalan untuk melindungi maklumat. Hospital ialah salah satu organisasi yang paling kompleks, di mana maklumat pesakit bukan sahaja mempunyai implikasi undang-undang dan ekonomi tetapi, yang lebih penting, kesan kepada kesihatan pesakit. Kajian pengimejan termasuklah imej perubatan, data pengenalan pesakit, dan maklumat proprietari kajian, adalah data yang terkandung dalam peranti storan PACS. Sistem ini mesti memelihara kerahsiaan, integriti, dan ketersediaan maklumat pesakit. Terdapat teknik seperti firewall, penyulitan, dan enkapsulasi data yang menyumbang kepada perlindungan maklumat dalam PACS.

Teknik pengimejan perubatan menjadi lebih digital dan lebih berhubung, menjadikan mereka terdedah kepada ancaman siber berkaitan rangkaian (Guan-Tack Oh et al. 2008). Jabatan pengimejan perubatan biasanya mempunyai kepadatan rangkaian peralatan perubatan yang paling tinggi di hospital. Ujian perubatan ini digunakan untuk pelbagai tujuan seperti menyokong rawatan menyelamatkan nyawa yang menjadikannya aset kritikal bagi hospital. Oleh itu, kegagalan satu peranti akan mengganggu keseluruhan operasi hospital, mempengaruhi kesejahteraan dan kerahsiaan pesakit. Maka, langkah yang lebih cekap dan berguna untuk menyimpan hasil ini ialah menggunakan sistem PACS untuk kebolehcapaian, kemudahan penggunaan, kapasiti dan keselamatannya.

2 PENYATAAN MASALAH

Sepanjang dekad yang lalu, imej penjagaan kesihatan telah beralih daripada salinan cetak kepada digital. Imej digital ini lebih mudah dikongsi, lantas mempercepatkan masa diagnosis. Maka, hakikat bahawa imej penjagaan kesihatan kini boleh dimuat naik, dikongsi pada peranti mudah alih peribadi, seperti telefon pintar dan tablet, dan disimpan secara digital, juga menjadikan mereka sasaran penjenayah siber (Deo, R. 2019). Piawaian DICOM dan keperluan undang-undang HIPAA adalah digunakan bagi melindungi data klinikal pesakit. Namun begitu, kaedah ini tidak digunakan secara sistematik pada metadata PACS dalam kebanyakan kes dan tidak mencukupi untuk memastikan integriti imej dan data berkaitan semasa penghantaran (Gutiérrez-Martínez, J. 2015).

Semasa proses penjagaan kesihatan, rekod perubatan pesakit diakses oleh kakitangan perubatan yang berbeza pada pelbagai peranti operasi. Sebagai contoh, imej perubatan mungkin dipaparkan pada PC doktor klinikal dan pada stesen kerja pakar radiologi (Chien-Ding Lee et .al 2011). PACS juga berinteraksi dengan berbilang sistem lain seperti pemapar web DICOM, rekod kesihatan elektronik, sistem pendaftaran maklumat hospital, dan juga arkib kerajaan, akademik dan komersial. Hal ini mewujudkan banyak jurang keselamatan yang berpotensi untuk penjenayah siber mengintai dan mencuri data.

Dalam era transformasi digital ini, maklumat penjagaan kesihatan semakin diserang oleh penggodam dan ancaman keselamatan siber yang lain. Sektor kesihatan telah menjadi industri

yang paling terdedah kepada penggodaman data dalam beberapa tahun kebelakangan ini, dengan insiden keselamatan siber mencecah kos lebih daripada $1.2 bilion pada 2017 sahaja. Dianggarkan lebih daripada 80% daripada semua penggodaman data disebabkan oleh data log masuk yang terjejas (Imaging Technology News, 2019). Dalam erti kata lain, kata laluan yang hilang atau dicuri mungkin menjadi ancaman terbesar kepada keselamatan maklumat kesihatan digital.

3 OBJEKTIF KAJIAN

Dalam kajian ini, objektif kajian ini adalah untuk membangunkan Sistem 2FA yang dapat

i. Mengenalpasti semua keperluan bagi sistem 2FA untuk keselamatan pemapar web DICOM

ii. Membangunkan sistem 2FA untuk mengesahkan pengguna pemapar web DICOM menggunakan pengesahan dua faktor.

iii. Menguji kebolehgunaan sistem 2FA untuk keselamatan pemapar web DICOM

4 METODOLOGI KAJIAN

Metodologi yang akan digunakan untuk membangunkan sistem 2FA untuk keselamatan pemapar web DICOM ialah model Agile. Metodologi ini dipilih kerana pembangunan sistem ini adalah mengikut fleksibiliti yang mana perkembangan sistem dilakukan dalam jangka masa yang pendek. Model ini telah dipilih kerana perubahan dalam sistem dapat ditangani dengan lebih pantas. Proses pembangunan projek memerlukan waktu yang relatif dan tidak memerlukan sumber daya yang besar.

i. Fasa Analisis Keperluan

Fasa Analisis Keperluan merupakan fasa terpenting dalam pembangunan sistem 2FA untuk keselamatan DICOM ini. Perancangan yang cermat dapat membantu untuk mengurangkan masalah yang terlibat dalam pembangunan projek. Hal ini demikian kerana masalah yang dihadapi dapat dikenalpasti dengan lebih awal. Fasa ini juga memberi ruang untuk menentukan tujuan, skop dan objektif projek.

ii. Fasa Rekabentuk

Sistem akan direkabentuk dalam fasa ini. Pengenalpastian cara pemapar ini beroperasi dari sudut perisian dan infrastruktur rangkaian akan dilakukan. Selain itu, rekabentuk antara muka, pangkalan data serta borang atau laporan juga dibangunkan ketika fasa ini.

iii. Fasa Pengekodan

Dalam Fasa pengekodan, sistem 2FA untuk keselamatan DICOM akan dibina dan diuji untuk membangunkan sistem yang mampu berfungsi. Fasa ini adalah fasa untuk mengenalpasti kod yang digunakan adalah sesuai dan menepati fungsinya.

iv. Fasa Pengujian

Fasa ini adalah fasa yang mana sistem akan diuji untuk mengenalpasti ralat atau kesalahan yang terdapat dalam sistem agar sistem yang dibangunkan adalah berfungsi dengan baik.

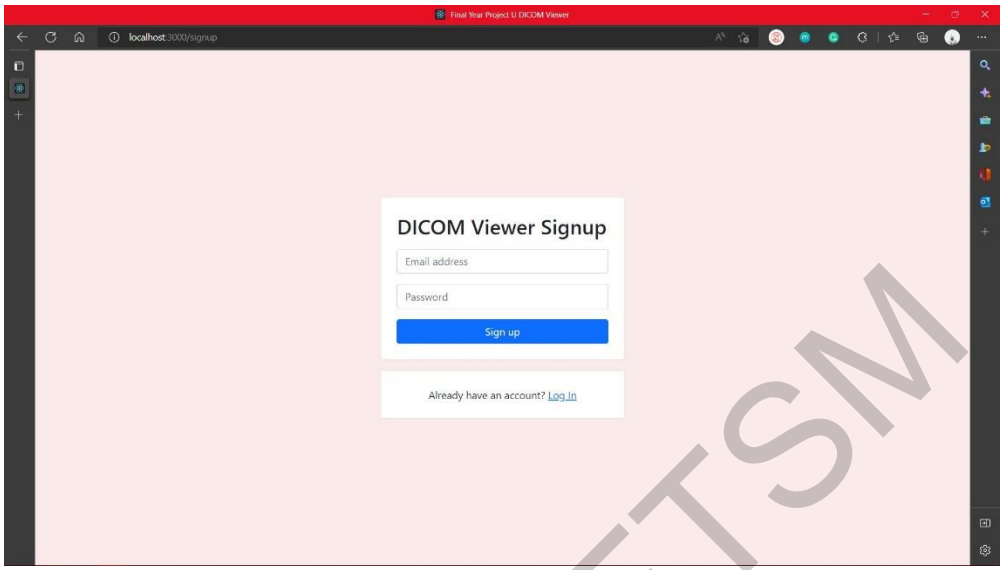
v. Fasa Penyelenggaraan

Dalam fasa penyelenggaraan, beberapa perubahan atau modifikasi dapat dilakukan sekiranya sistem masih tidak mencapai objektif. Fasa ini memberi peluang untuk menyempurnakan sistem. Fasa ini adalah fasa terakhir, maka sistem 2FA untuk keselamatan DICOM dapat dibangunkan dan digunakan dengan baik.

5 HASIL KAJIAN

Sistem ini dibangunkan dengan menggunakan bahasa pengaturcaraan JS dan HTML, dan penyimpanan data terletak di Google Firebase dan server localhost. Perisian yang digunakan ialah Visual Studio Code.

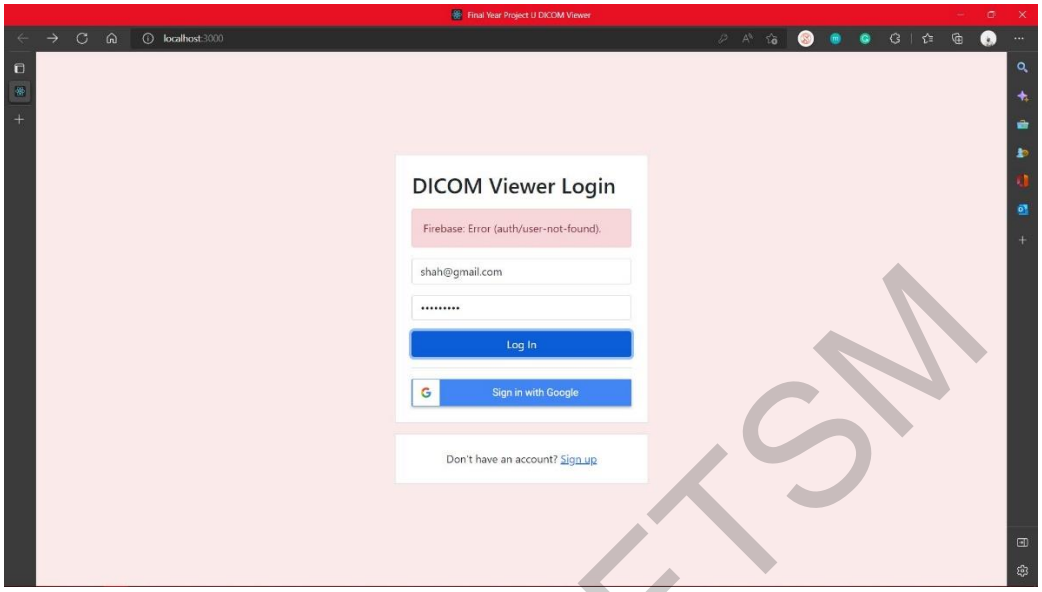
Bagi fungsi mendaftar sebagai pengguna, pengguna diharuskan untuk mengisi e-mel dan kata laluan. Selepas menekan butang ‘Sign Up’ data akan dimasukkan ke dalam Google Firebase. Rajah 1 menunjukkan antara muka bagi pendaftaran pengguna.



Rajah 1 Antara muka pendaftaran pengguna

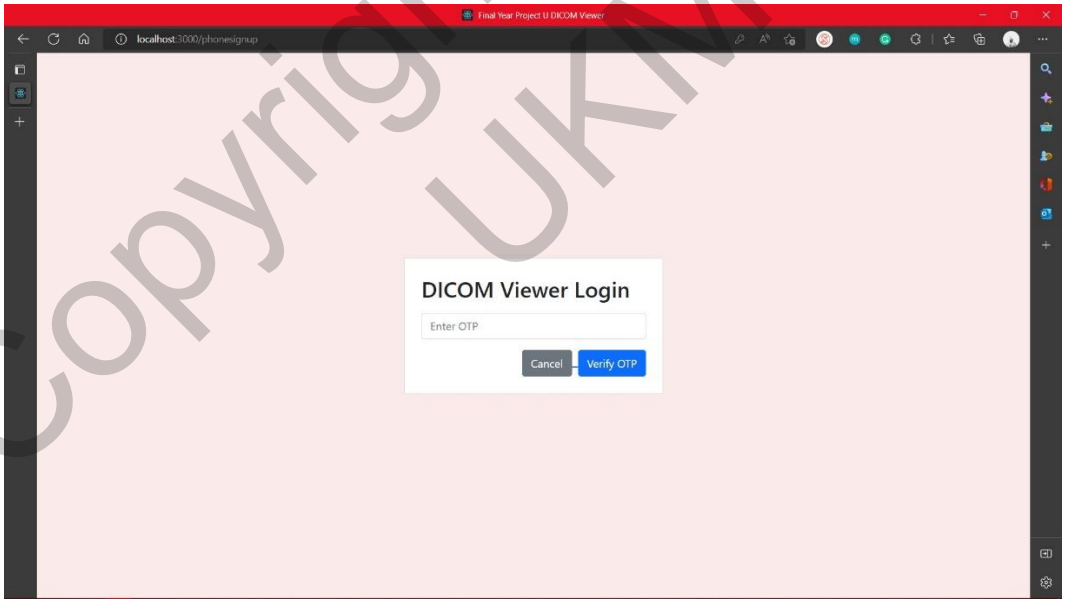
Rajah 1 Antara muka log masuk

Pengguna akan dibenarkan log masuk sekiranya sudah berdaftar sebagai pengguna. Sekiranya masih belum mendaftar, mesej yang mengatakan log masuk tidak berjaya akan dipaparkan seperti dalam Rajah 3.

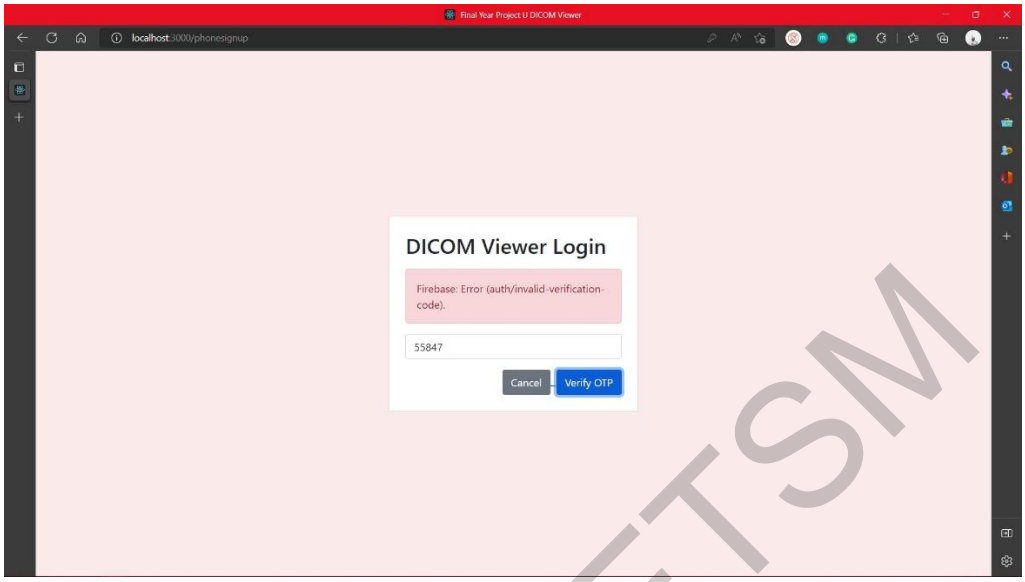


Rajah 3 Antara muka apabila log masuk tidak berjaya

Pengguna yang berdaftar akan dibawa ke antara muka yang mana pengguna diminta untuk memasukkan kod OTP yang telah dihantar.

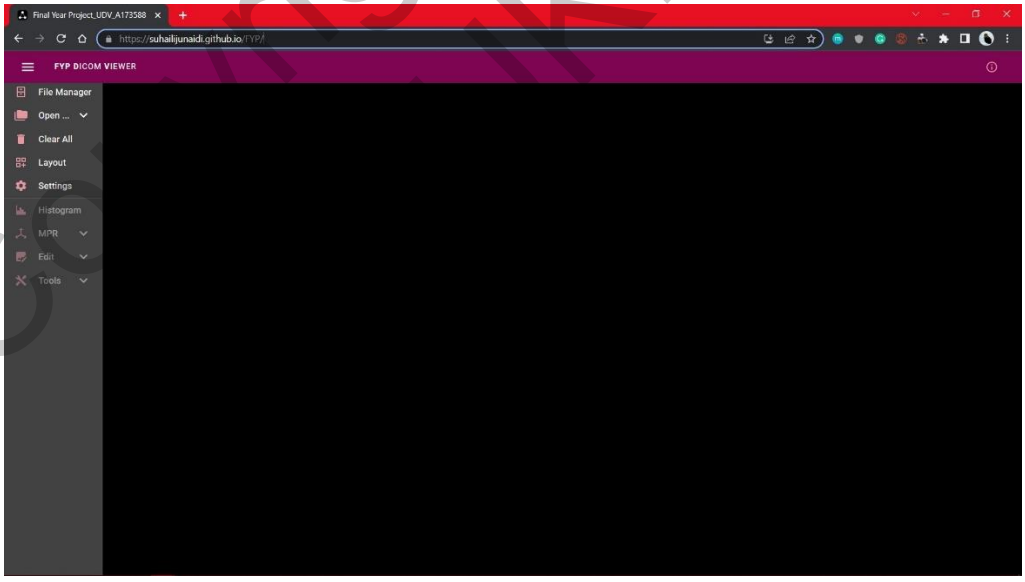


Rajah 4 Antara muka pengguna untuk memasukkan kod OTP



Rajah 5 Antara muka apabila pengesahan kod OTP tidak berjaya

Apabila pengguna memasukkan kod OTP yang tidak sah, maka antara muka seperti Rajah 5 akan dipaparkan. Sekiranya pengguna memasukkan kod OTP yang sah, maka pengguna akan dibawa ke antara muka pemapar web DICOM seperti dalam Rajah 6 dan Rajah 7 yang mana pengguna boleh memanipulasi imej DICOM.



Rajah 6 Antara muka pemapar web DICOM

Rajah 7 Antara muka pemapar web DICOM

6 KESIMPULAN

Secara keseluruhannya, sistem 2FA untuk keselamatan DICOM ini dapat dibangunkan walaupun terdapat beberapa masalah *rendering* kod aturcara. Sistem ini dapat memberi pengesahan terhadap pengguna yang memaparkan imej DICOM pada pemapar web DICOM. Walaupun terdapat beberapa kekurangan, diharapkan sistem ini dapat dijadikan titik kajian untuk kajian pada masa hadapan.

7 RUJUKAN

Guan-Tack Oh, Yun-Bae Lee, Min-Six Jung, Soon-Ja Yeom. 2008. "Design of a Robust WatermarkingAlgorithm against the Geometric Distortion for Medical Image Security," 2008 Second International Conference on Future Generation Communication and Networking Symposia, 2008, pp. 167-170, doi: 10.1109/FGCNS.2008.23.

Gutiérrez-Martínez, J. 2015. *Business Model for the Security of a Large-Scale PACS,Compliance with ISO/27002:2013 Standard*. SpringerLink. https://link.springer.com/article/10.1007/s10278-014-9746-4?error=cookies_not_supported&code=8c6ef3d0-2530-4e44-b2ce-64aa5ab7750c

Chien-Ding Lee, Kevin I. -J Ho, Wei-Bin Lee. 2011. "A Novel Key Management Solution for Reinforcing Compliance With HIPAA Privacy/Security Regulations," in IEEE

Transactions on Information Technology in Biomedicine, vol. 15, no. 4, pp. 550-556, July 2011, doi: 10.1109/TITB.2011.2154363.

Nursuhaili Binti Junaidi (A173588)
Dr Khairul Akram Bin Zainol Ariffin
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia