Sistem Kawalan Akses BYOD (*BYOD Access Control System - BACSYM*)

Faizal Bin Mat Idris
Wan Fariza Binti Fauzi

Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

"*Bring Your Own Device*" (BYOD) adalah satu kaedah atau gaya hidup di mana pekerja menggunakan peranti persendirian bagi menjalankan tugasan di pejabat. BYOD telah dipraktikkan di beberapa organisasi kerajaan dan juga swasta yang melibatkan akses kepada rangkaian dan juga sistem-sistem yang turut mengandungi data-data sulit sesebuah organisasi. Walaupun ianya satu kaedah yang memberi kemudahan kepada pekerja dan organisasi namun kebocoran dan kecurian data boleh berlaku sekiranya kawalan akses kepada rangkaian dan sistem organisasi tersebut tidak menyeluruh. Objektif projek ini adalah untuk membangunkan satu Sistem Kawalan Akses BYOD (*BYOD Access Control System*) yang dinamakan sebagai BACSYM yang akan mengawal selia akses sesuatu peranti kepada rangkaian atau sistem sesuatu organisasi. Sistem yang dibangunkan melibatkan proses pendaftaran serta pengesahan pengguna dan peranti persendirian yang digunakan secara serentak. Manakala maklumat pengguna dan peranti ini disimpan menggunakan kaedah penyulitan bagi memastikan kesahihan akses pengguna tidak di manipulasi oleh pihak tidak bertanggungjawab. Selain itu, peranti persendirian pengguna akan diimbas oleh agen sistem bagi memastikan ia bebas dari sebarang ancaman yang boleh menjejaskan keselamatan rangkaian dan data organisasi. Pembangunan sistem menggunakan metodologi *waterfall* bagi memastikan aliran proses sistem yang dibangunkan lebih jelas dan menepati objektif yang telah ditetapkan. Pengujian yang di laksanakan menunjukkan keputusan yang baik dan BACSYM ini dapat meningkatkan keselamatan data organisasi dalam persekitaran BYOD tanpa melibatkan kos implementasi yang tinggi.

Copyright@FTSM UKM

1. PENGENALAN

BYOD adalah singkatan dari ayat "*Bring Your Own Device*" iaitu dalam Bahasa Melayu adalah "membawa peranti anda sendiri" yang mula popular sekitar tahun 2011. BYOD adalah satu kaedah di mana pekerja menggunakan peranti mudah alih persendirian seperti komputer mudah alih dan telefon mudah alih bagi tugasan harian. Kaedah ini membolehkan pekerja merasa selesa dengan peralatan sendiri dan ianya juga boleh menghilangkan tekanan memandangkan sudah biasa dengan atur cara program dalam peralatan tersebut. Walaubagaimanapun terdapat juga unsur-unsur negatif setelah ianya dilaksanakan seperti kehilangan tumpuan sewaktu kerja disebabkan gangguan dengan kandungan peribadi dalam peralatan sendiri. Sesebuah organisasi juga perlu membuat

kajian dan penyelidikan berkaitan polisi, sesi kesedaran keselamatan maklumat dan latihan kepada pekerja sebelum kaedah BYOD ini di laksana. Kebanyakan organisasi di kebanyakan negara menghadapi kesukaran untuk mengaplikasikan BYOD dalam persekitaran pekerjaan. Ini kerana tanpa perancangan yang tepat dalam pelaksanaan BYOD, organisasi mungkin mendedahkan data mereka kepada ancaman (Olalere, 2015).

Berdasarkan kajian yang di buat oleh (Mahat, 2018), terdapat 4 masalah utama yang wujud dalam organisasi yang melaksanakan BYOD iaitu masalah keselamatan, kehilangan atau kecurian data dan peranti, pelanggaran privasi data, dan perisian hasad (*malware*). Sehingga kini masih belum terdapat garis panduan lengkap mengenai kawalan yang perlu dilaksanakan dan cara terbaik implementasi BYOD dalam organisasi terutamanya dari segi perkakasan, perisian dan sokongan ICT yang perlu dilaksanakan (Mahat, 2018). Memandangkan isu kritikal BYOD adalah berkaitan keselamatan data dan rangkaian, pengawalan akses oleh pengguna dan perkakasan adalah perlu dikuatkuasakan dalam sesebuah organisasi yang mempraktikkan BYOD dalam persekitaran kerja. Projek ini mencadangkan dan seterusnya membangunkan satu sistem kawalan akses dalam persekitaran BYOD dengan merujuk kepada teknik dan penyelesaian sedia ada. Ini bagi memastikan keselamatan rangkaian dan data sesebuah organisasi terjamin dalam masa yang sama dapat mengaplikasikan penggunaan BYOD.

2. PENYATAAN MASALAH

Diakui teknologi BYOD membawa banyak faedah kepada pekerja dan juga organisasi, seiring dengan cabaran dan kelemahannya yang perlu dihadapi. Tahap keselamatan maklumat bukan sahaja tertumpu pada sesuatu peranti atau maklumat di dalam organisasi, tetapi ianya juga melibatkan kawalan akses dari pengguna dan peranti ke maklumat organisasi tersebut. Organisasi perlu memastikan bahawa ketika pengguna menggunakan peranti peribadinya untuk mengakses maklumat organisasi, peranti mesti memenuhi beberapa standard pengesahan serta perlindungan terhadap perisian hasad untuk mencegah kebocoran data.

Teknik pengesahan yang menggunakan kata laluan dalam kaedah log masuk masih lagi tidak memenuhi tahap keselamatan yang optimum bagi persekitaran BYOD. Kaedah pengesahan yang

Copyright@FTSM UKM

ada di BYOD biasanya memusatkan perhatian pada pengguna atau peranti secara berasingan, sementara BYOD perlu memastikan kedua-dua peranti dan pengguna disahkan selamat untuk mengakses persekitaran organisasi (Zheng, Cao, & Chang, 2018).

Dalam persekitaran organisasi yang melaksanakan BYOD, maklumat pengguna dan peranti yang mengakses rangkaian organisasi perlu disimpan bagi tujuan keselamatan di mana ianya dapat dijadikan rujukan sekiranya terdapat aktiviti yang mencurigakan semasa sesuatu akses diberikan kepada pengguna tersebut. Penyimpanan data ini pula perlulah mematuhi Akta Perlindungan Data Peribadi *(Personal Data Protection Act 2010* : Act 709) bagi memastikan data ini tidak dikongsi bagi tujuan peribadi atau sebarang aktiviti penyalahgunaan data pengguna. Penyimpanan dan perlindungan data ini juga perlu seiring dengan standard yang telah ditetapkan oleh badan standard antarabangsa yang terkandung dalam ISO27001 (*Information Security Managemet System* – ISMS). Dalam kawalan A12.3.1 ISO/IEC 27001 telah menjelaskan data yang disimpan perlu dilindungi dari segi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi (ISO 27001 International Standard).

3. OBJEKTIF KAJIAN

Objektif umum kajian ini adalah untuk mengusulkan kawalan akses pengguna dan peranti kepada rangkaian organisasi dan mencegah kebocoran data dalam persekitaran BYOD. Ini bagi memastikan rangkaian organisasi itu terjamin dari segi keselamatan dengan pelaksanaan dan pengurusan polisi penggunaan BYOD yang lebih baik. Untuk mencapai objektif ini, kajian akan dipandu oleh objektif khusus berikut:

1. Membangunkan mekanisme kawalan akses pengguna di mana pengesahan menggunakan nama identiti (ID) dan kata laluan yang didaftarkan untuk mengelakkan kebocoran data yang mungkin terjadi akibat akses tidak sah ke sumber organisasi.

2. Membangunkan mekanisme kawalan akses peranti di mana *Media Access Control* (MAC) *address* peranti didaftarkan dan di semak padanan dengan ID pengguna bagi mengelakkan akses peranti tidak berdaftar.

Copyright@FTSM UKM

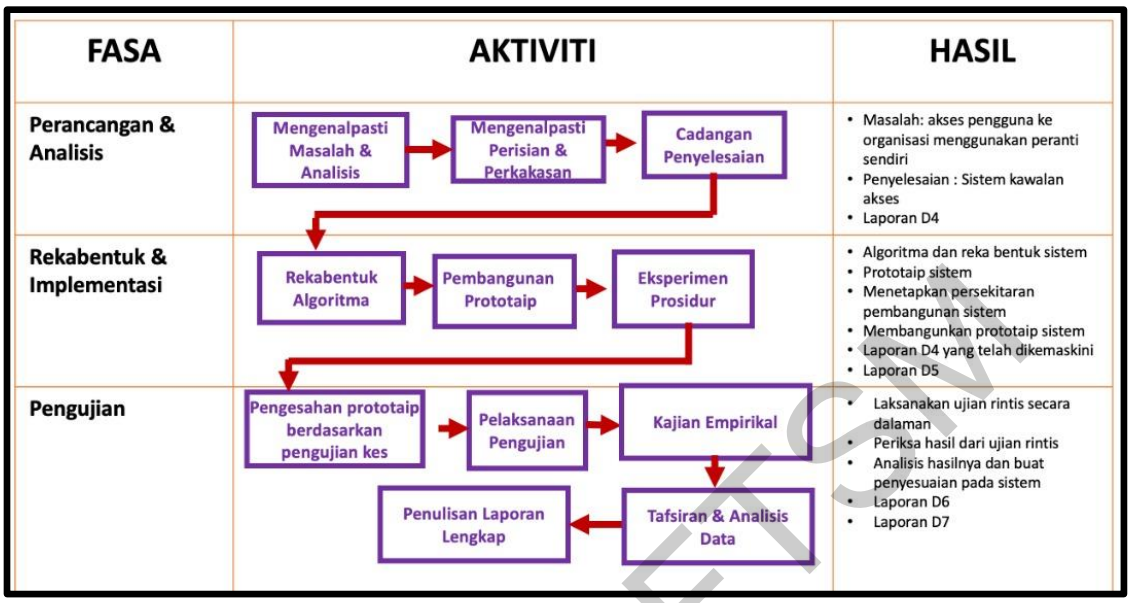
3. Membangunkan mekanisme yang dipasang pada peranti pengguna bagi mengimbas versi antivirus serta versi sistem pengoperasian (OS) untuk memastikan versi yang digunakan adalah yang terkini atau masih dalam tempoh sokongan dan mengikut spesifikasi yang ditetapkan oleh sesebuah organisasi.

4. Membangunkan mekanisme penyimpanan maklumat pengesahan pengguna dan peranti yang disimpan menggunakan kaedah penyulitan (*encryption*) bagi mencegah berlakunya manipulasi data oleh individu yang tidak bertanggungjawab dan memenuhi standard ISO27001.

4. METOD KAJIAN

Untuk melindungi persekitaran BYOD, adalah menjadi satu keperluan untuk mempunyai seni bina keselamatan BYOD yang komprehensif. Seni bina ini perlu menunjukkan hubungan antara pekerja yang menggunakan peranti peribadi, pentadbir sistem dan algoritma kawalan akses kepada rangkaian organisasi. Metodologi yang akan digunakan dalam pembangunan projek ini adalah model *Waterfall*. Model *Waterfall* dalam kejuruteraan perisian secara rasmi diperkenalkan sebagai idea yang diterbitkan oleh Winston Royce pada tahun 1970 (Royce, 1970). Model *Waterfall*, seperti namanya sendiri, adalah proses pembangunan perisian secara berurutan. Fasa pembangunan melibatkan tiga peringkat iaitu perancangan dan analisis, reka bentuk dan implementasi serta pengujian seperti Rajah 1.

Copyright@FTSM UKM



Rajah 1 : Fasa Pembangunan Sistem

4.1 Fasa Perancangan

Fasa perancangan adalah fasa pertama dalam pembangunan sistem. Fasa ini melibatkan proses mengenal pasti masalah yang akan diselesaikan dan objektif yang dicadangkan bagi penyelesaian masalah tersebut. Fasa ini juga akan menentukan skop pembangunan sistem dan kekangan yang mungkin wujud di sepanjang proses pelaksanaan.

Langkah seterusnya dalam fasa perancangan adalah melaksanakan kajian perpustakaan atau sorotan literatur. Pelaksanaan sorotan literatur ini adalah bagi mengenal pasti teknologi semasa berkaitan dengan persekitaran BYOD yang terdapat di pasaran. Kajian ini juga adalah untuk mencari masalah yang wujud dengan teknik sedia ada dan cara penyelesaian yang boleh diaplikasikan supaya sistem yang dibangunkan dapat digunakan di persekitaran cadangan. Berdasarkan bacaan dari buku, jurnal dan Internet, didapati tiga sistem sedia ada yang sesuai dijadikan rujukan dan perbandingan dalam proses pembangunan BACSYM iaitu SolarWinds RMM (Shari, 2020), AirWatch Workspace One (VMWare, 2020) dan Microsoft Intune(Lucas, 2020). Walaubagaimanapun terdapat kelemahan pada setiap sistem dan masih terdapat penambahbaikan yang boleh dilaksanakan bagi memenuhi keperluan persekitaran BYOD sesebuah organisasi.

Copyright@FTSM UKM

4.2 Fasa Analisis

Fasa ini akan menerangkan mengenai spesifikasi pembangunan Sistem BACSYM yang dibangunkan bagi organisasi yang mengamalkan persekitaran BYOD. Spesifikasi keperluan pembangunan sistem yang terdiri daripada keperluan perkakasan, perisian, keperluan fungsian, dan keperluan bukan fungsian sistem dianalisis di dalam fasa ini secara terperinci. Bagi pembangunan BACSYM, perkakasan yang digunakan adalah tiga unit komputer riba manakala perisian yang terlibat adalah sistem pengoperasian Windows, Python, PHP, Java, MySql dan Firefox.

Keperluan fungsian pula adalah keperluan yang menerangkan interaksi di antara sistem dan persekitarannya. Terdapat dua faktor keperluan fungsian yang menentukan kejayaan pembangunan sesebuah aplikasi iaitu keperluan pengguna dan keperluan sistem itu sendiri. Keperluan pengguna menjelaskan mengenai kehendak pengguna terhadap aplikasi yang dibangunkan manakala keperluan sistem adalah berkaitan dengan fungsi terperinci aplikasi yang dibangunkan. BACSYM mempunyai sepuluh keperluan fungsian iaitu Fungsi Pendaftaran Pengguna Baru, Fungsi Log Masuk, Fungsi Imbasan Agen Sistem, Fungsi Reset Kata laluan Pengguna, Fungsi Log Keluar, Fungsi Kemaskini maklumat Anti-virus dan Sistem Pengoperasian, Fungsi Paparan Laporan Log Akses Pengguna, Fungsi Simpanan Maklumat Pengguna, Fungsi Simpanan Log Akses Pengguna dan Fungsi Penyulitan (*encryption*) Data Maklumat Pengguna seperti yang diterangkan dalam Jadual 1. Keperluan bukan fungsian pula akan menentukan kualiti sesuatu sistem yang dibangunkan. Keperluan ini melibatkan faktor keselamatan, kebolehgunaan, kecekapan, kebolehpercayaan, dan ketersediaan. Fasa analisis ini adalah penting sebagai input kepada fasa reka bentuk dan pembangunan BACSYM.

Jadual 1 : Keperluan Fungsian

FUNGSI	KETERANGAN
PENGGUNA	
Pendaftaran Pengguna Baru	Fungsi ini membolehkan pengguna baru membuat pendaftaran pada sistem dengan memasukkan maklumat pengguna dan kata laluan yang dipilih.

Copyright@FTSM UKM

Log Masuk	Fungsi log masuk adalah paparan pertama yang akan dilihat oleh pengguna sedia ada. Pengguna perlu memasukkan ID - kad pengenalan dan kata laluan yang telah di daftarkan pada fungsi ini.
Imbasan Agen Sistem	Terdapat tiga fungsi yang melibatkan semakan oleh sistem apabila pengguna telah log masuk kepada sistem iaitu : • *Fungsi semakan identiti peranti* Fungsi di mana identiti peranti iaitu alamat MAC akan diperiksa dan direkodkan. • *Fungsi semakan versi anti virus peranti* Fungsi di mana versi antivirus peranti pengguna diimbas dan disemak, kemudian dibuat perbandingan dengan versi antivirus yang telah ditetapkan oleh pihak pentadbir sistem. • *Fungsi semakan versi sistem pengoperasian peranti* Fungsi di mana versi sistem pengoperasian peranti pengguna diimbas dan disemak, kemudian dibuat perbandingan dengan versi sistem pengoperasian yang telah ditetapkan oleh pihak pentadbir sistem.
Reset Kata laluan Pengguna	Fungsi ini adalah untuk set semula kata laluan sekiranya pengguna lupa kata laluan. Nombor TAC akan dihantar ke e-mel yang didaftar pengguna dan pengguna perlu memasukkan TAC ini berserta ID pengguna dan seterusnya memasukkan kata laluan baru.
Log Keluar	Fungsi membenarkan pengguna keluar dari sistem.
PENTADBIR	
Kemaskini maklumat Anti-virus dan Sistem Pengoperasian	• *Kemaskini Versi Anti-virus* Fungsi ini membolehkan pentadbir memasukkan nama perisian dan versi antivirus yang dibenarkan oleh sistem supaya ianya menjadi tanda aras bagi kawalan akses sesuatu peranti ke rangkaian organisasi. • Kemaskini Versi Sistem Pengoperasian Fungsi ini membolehkan pentadbir memasukkan nama perisian dan versi perisian pengoperasian yang dibenarkan oleh sistem supaya ianya menjadi tanda aras bagi kawalan akses peranti ke rangkaian organisasi.

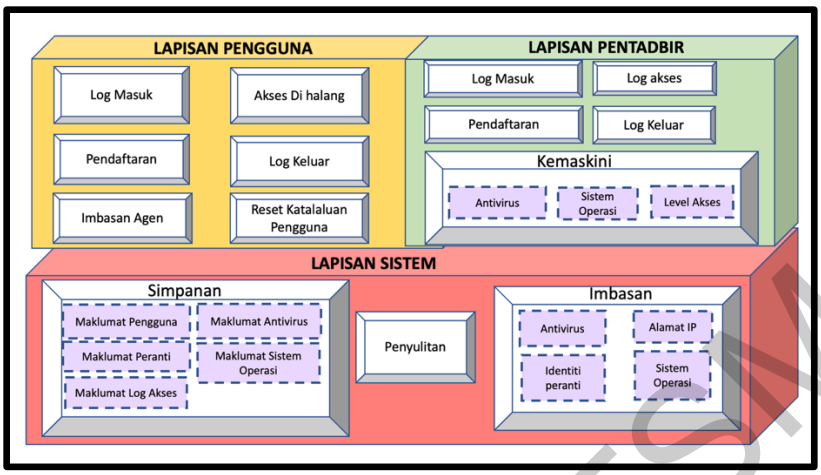
Copyright@FTSM UKM

	• Kemaskini Tahap Akses Pengguna Fungsi ini membolehkan pentadbir menukar status pengguna biasa kepada pentadbir sistem.
Paparan Laporan Log Akses Pengguna	Fungsi ini memaparkan maklumat pengguna log masuk ke sistem dan status akses sama ada berjaya atau tidak melalui tapisan versi antivirus dan versi sistem pengoperasian. Log yang dipaparkan adalah ID pengguna, alamat *Internet Protocol* (IP) dan masa log masuk.
Log Keluar	Fungsi ini membenarkan pentadbir keluar dari sistem.
Sistem	
Simpanan Maklumat Pengguna	Fungsi ini melaksana simpanan maklumat peribadi pengguna dan peranti dalam pangkalan data.
Simpanan Log Akses Pengguna	Fungsi ini membuat simpanan log akses pengguna ke sistem. Maklumat yang di simpan adalah ID pengguna, masa log masuk dan alamat IP pengguna. Status pengguna sama ada dibenarkan akses atau dihalang akses ke sistem juga akan disimpan di sini.
Penyulitan (*encryption*) Data Maklumat Pengguna	Semua maklumat peribadi pengguna seperti nama, e-mel, nombor kad pengenalan dan kata laluan serta maklumat peranti pengguna seperti *MAC address* akan dibuat penyulitan (*encryption*) iaitu kaedah Hash dan SHA-2 sebelum di simpan di dalam pangkalan data menggunakan fungsi ini.

4.3 Fasa Reka Bentuk dan Pembangunan

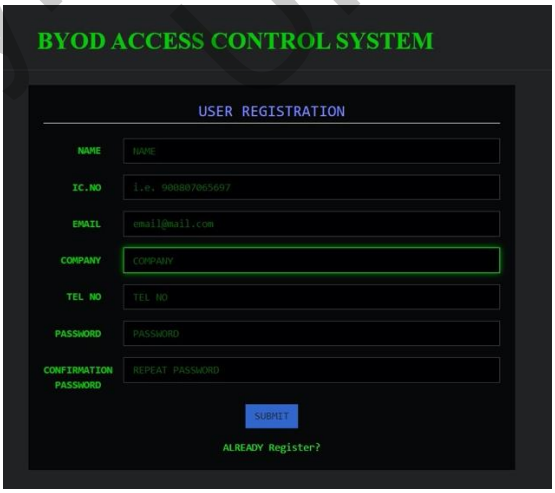
Fasa reka bentuk memperincikan mengenai reka bentuk aplikasi sistem yang dibangunkan. Fasa reka bentuk adalah fasa bagi merancang penyelesaian masalah bagi spesifikasi keperluan sistem. Fasa ini adalah langkah permulaan untuk terjemahkan dari domain masalah kepada domain penyelesaian. Reka bentuk sistem adalah faktor kritikal yang menentukan kualiti sistem dan mempunyai kesan besar kepada aktiviti pembangunan sistem. Fasa ini menerangkan mengenai reka bentuk seni bina, reka bentuk pangkalan data, reka bentuk antara muka dan reka bentuk algoritma bagi Sistem BACSYM. Fasa reka bentuk pembangunan Sistem BACSYM ini dihuraikan dengan lebih lanjut yang merangkumi gambar rajah konteks, rajah kes guna, gambar rajah ERD, rajah aktiviti dan reka bentuk seni bina BACSYM seperti Rajah 2.

Copyright@FTSM UKM



Rajah 2 : Seni bina BACSYM

Seterusnya adalah proses penyediaan reka bentuk antara muka bagi sistem yang dibangunkan. Penyediaan reka bentuk antara muka adalah proses untuk menentukan kaedah interaksi di antara pengguna dengan sistem yang dibangunkan. Antara muka pengguna yang dibangunkan perlu dipadankan dengan medan-medan data di dalam jadual pangkalan data. Pemetaan data ini bertujuan untuk memudahkan pembangun sistem mengetahui senarai medan data yang diperlukan bagi satu-satu antara muka pengguna yang dibangunkan. Contoh antara muka bagi BACSYM di tunjukkan dalam Rajah 3.



Rajah 3 : Antara muka BACSYM

Setelah selesai pelaksanaan reka bentuk, fasa pembangunan dimulakan. Fasa ini dijalankan berasaskan perancangan dan keperluan sistem yang telah diusulkan dalam metodologi kajian. Segala proses pembangunan dalam fasa ini dilaksana secara persekitaran dalaman (*localhost*) yang

Copyright@FTSM UKM

melibatkan pemasangan perisian-perisian tertentu sebelum ianya dipindahkan ke persekitaran pengujian. Persekitaran dalaman merujuk kepada rangkaian antara server dan peranti-peranti pengguna sahaja tanpa melibatkan akses internet. Sistem BACSYM dibangunkan melalui tiga bahagian secara berperingkat iaitu peringkat 1: Pemasangan Perisian bagi Persekitaran Pembangunan Dalaman (*local environment*), Peringkat 2: Pembangunan Reka Bentuk Antara Muka dan Peringkat 3: Kod Pengaturcaraan Bagi Fungsi-fungsi Penting Sistem BACSYM. Setelah dibangunkan setiap peringkat, ke semua peringkat ini akan di integrasikan antara satu sama lain bagi mewujudkan satu sistem yang dikehendaki.

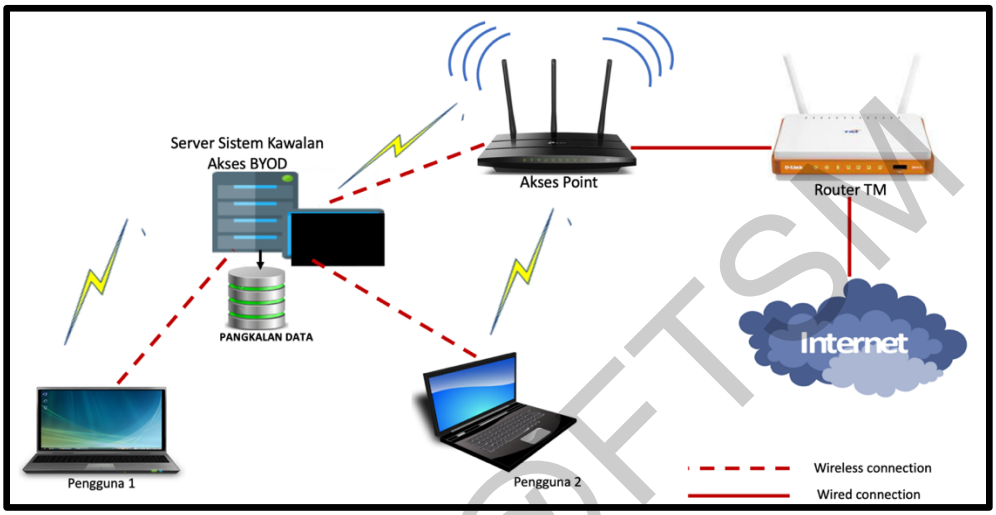
4.4 Fasa Pengujian

Fasa ini menerangkan mengenai pengujian yang di laksana bagi Sistem BACSYM. Fasa pengujian merupakan fasa penting untuk memastikan fungsi sistem yang diusulkan sebelum ini dapat dibuktikan melalui beberapa kes pengujian. Pengujian ini memfokuskan kepada ujian keperluan fungsi sistem dengan menetapkan kaedah pengujian kotak hitam (*black box*) iaitu teknik Ujian Peralihan Keadaan (*State Transition Testing*) dalam mengenal pasti keberkesanan setiap fungsi berdasarkan kes guna yang dibangunkan. Pengujian ini adalah pengujian dalam satu kitaran sahaja iaitu dari proses log masuk hinggalah kepada proses log keluar sistem dengan senario kemasukan data yang berbeza pada peranti yang berbeza. Kriteria penamatan pengujian adalah berdasarkan pematuhan kepada prosedur proses data bagi setiap kes guna serta status ‘Berjaya’ bagi setiap kes guna tersebut.

Proses pengujian ini juga cuba meminimumkan ralat daripada wujud di dalam sistem ketika pengguna menggunakan sistem. Fasa ini melibatkan pengujian secara persekitaran dalaman (*Local Area Network* - LAN) tanpa wayar (*wireless*) di mana dua (2) buah peranti iaitu komputer riba yang berfungsi sebagai pengguna (c*lient)* seperti Rajah 4. Komputer riba ini dilabel sebagai peranti A dan peranti B. Kedua-dua peranti ini akan cuba mengakses internet melalui rangkaian tanpa wayar manakala kawalan akses sistem adalah dengan menggunakan kaedah nyahaktif peranti rangkaian (*disable network adapter*) komputer riba tersebut. Nyahaktif *network adapter* ini akan dilaksana oleh agen sistem sekiranya sistem pengoperasian (OS) atau antivirus di peranti A dan B

Copyright@FTSM UKM

tidak mengikut spesifikasi versi OS dan antivirus yang telah didaftarkan oleh pentadbir sistem di pelayan (*server*) iaitu peranti C.



Rajah 4 : Persekitaran Pengujian BACSYM

Skop pengujian yang dilaksanakan adalah hanya memfokuskan kepada Pengujian Tahap Sistem (*System Testing*) di mana pengujian ini memberi perhatian terhadap keperluan fungsi (*test type*) sesebuah sistem berjalan seperti mana yang diharapkan bagi memastikan aplikasi yang dibangunkan mencapai objektif. Jadual 2 menunjukkan senarai kes guna (F1 hingga F9) dan perincian berkaitan pengujian yang akan dilaksanakan serta keputusan pengujian.

Jadual 2 : Pengujian BACSYM

KES GUNA	KEPERLUAN FUNGSI	PERINCIAN PENGUJIAN	HASIL PENGUJIAN
F1	Pemasangan Agen dan Pendaftaran Pengguna	Menguji pemasangan agen (*byod.exe*) dan pendaftaran akaun pengguna.	1. Sistem memaparkan mesej "*Registration Success*". 2. Sistem memaparkan halaman "*Login*".
F2	Log Masuk	Menguji data log masuk pengguna dengan memasukkan no. kad pengenalan dan kata laluan.	**Senario 1 :** Mesej ' *Success to login*' dipaparkan. Halaman imbasan dengan mesej '*Scanning in progress*' dipaparkan.

Copyright@FTSM UKM

			Senario 2 : Mesej '*Unsuccessful login. Please check your ID & Password*' dipaparkan. *Wifi adapter* peranti akan dinyahaktifkan(*disable*).
F3	Mengenal pasti Identiti Peranti	Menguji setiap peranti hanya boleh diakses oleh pengguna yang mendaftar menggunakan peranti tersebut sahaja. Satu peranti hanya untuk satu ID pengguna sahaja. Pengguna yang mendaftar di peranti A tidak dapat akses kepada sistem sekiranya menggunakan peranti B semasa proses log masuk.	**Senario 1:** Untuk peranti A, sistem melaksanakan proses imbasan keselamatan. **Senario 2:** Untuk peranti B, mesej '*Unsuccessful login. The device did not match with your ID*' dipaparkan. *Wifi adapter* peranti akan dinyahaktifkan(*disable*).
F4	Imbasan Keselamatan Peranti	Menguji fungsi imbasan agen bagi menyemak versi Sistem Pengoperasian Windows dan versi antivirus peranti A dan peranti B adalah mengikut spesifikasi keselamatan yang telah didaftar oleh pentadbir sistem.	**Senario 1:** Mesej *'Your device meet the security requirement, you can access to organization network'* dipaparkan. **Senario 2 :** Mesej '*Failed*' dipaparkan. Klik ok dan Mesej *'Your device did not meet the security requirement '* *Your Windows already update. Please update your ESET Endpoint Secuirty into this version :* *Wifi adapter* peranti akan dinyahaktifkan(*disable*). **Senario 3:** Mesej '*Failed*' dipaparkan. Klik ok dan Mesej *'Your device do not meet the security requirement '* *Please update your windows 10 into latest windows 10* *Your Antivirus already update*

Copyright@FTSM UKM

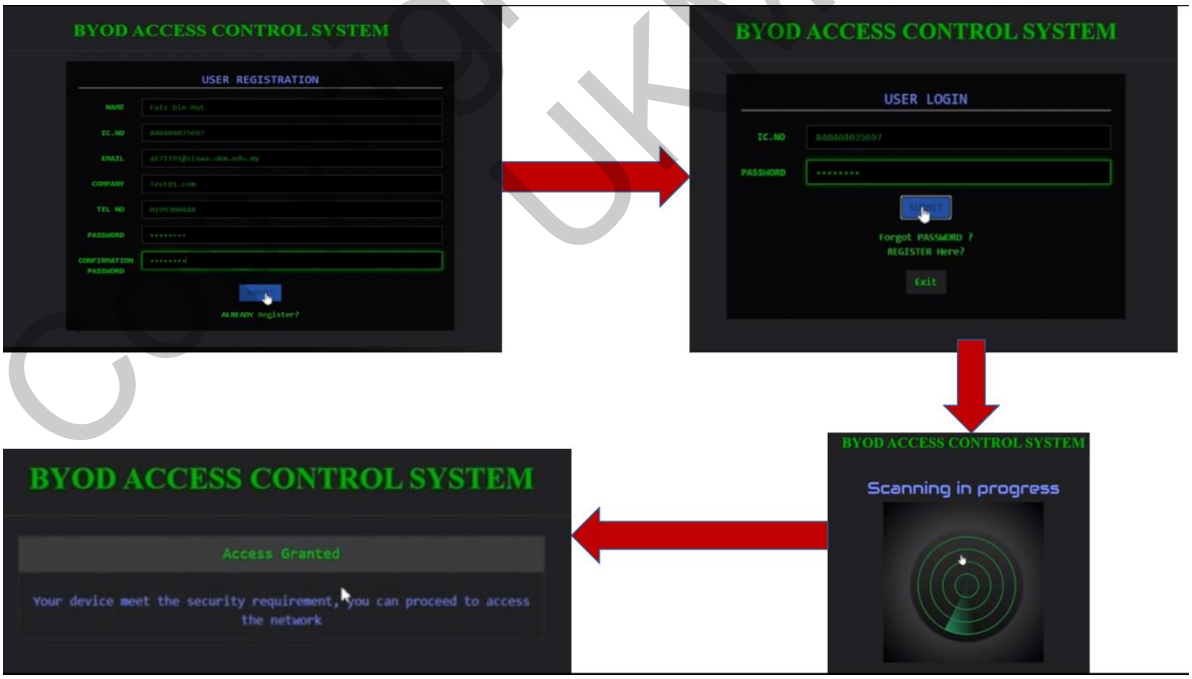
			Wifi adapter peranti akan diputuskan (*disconnected*). **Senario 4:** Mesej '*Failed*' dipaparkan. Klik ok dan Mesej *'Your device did not meet the security requirement '.* *Please update your windows 10 into latest windows 10.* *Please install antivirus.* *Wifi adapter* peranti akan dinyahaktifkan(*disable*).
F5	Kemaskini	Menguji fungsi pengemaskinian versi Sistem Pengoperasian Windows, versi perisian Antivirus dan Tahap Akses Pengguna oleh pentadbir sistem.	**Senario 1:** Mesej "*Success update for antivirus version*" dipaparkan. **Senario 2:** Mesej "*Success update for Operating System version*" dipaparkan. **Senario 3:** Status kolum level pengguna bertukar dari *User* kepada *Admin*.
F6	Penyulitan dan Penyimpanan Data	Menguji setiap maklumat data pengguna dan data peranti disulitkan (*encrypted)* dan berjaya disimpan di dalam pangkalan data.	Maklumat pengguna disimpan secara penyulitan (*encryption*) data.
F7	Jana Laporan Log Akses	Menguji penjanaan laporan log akses pengguna.	Laporan Log Akses Pengguna dipaparkan
F8	Log Keluar	Menguji fungsi butang log keluar untuk keluar daripada sistem.	Pengguna dapat log keluar dari sistem
F9	Reset Kata laluan Pengguna	Menguji notifikasi kepada pengguna melalui e-mel berkaitan reset kata laluan sistem.	1. Nombor TAC dihantar ke e-mel pengguna 2. Kata laluan baru pengguna dikemaskini

Copyright@FTSM UKM

5. HASIL KAJIAN

Kelebihan sistem ini adalah ianya dibangunkan secara dalaman dan segala proses penyelenggaraan tidak melibatkan kos yang tinggi di mana ianya tidak melibatkan lesen langganan berdasarkan unit komputer dan juga lesen sokongan teknikal. Segala penambahbaikan hanya melibatkan faktor masa dan kepakaran individu dalam bidang pengaturcaraan dan rangkaian. BACSYM juga berjaya meningkatkan keselamatan organisasi yang mengamalkan BYOD. BACSYM berfungsi sebagai kawalan akses kepada peranti persendirian yang di bawa.

Pengguna baru yang ingin mengakses rangkaian organisasi perlu membuat pendaftaran dengan memasukkan maklumat yang diperlukan. Pada masa yang sama, agen akan dipasang pada peranti pengguna. Pengguna kemudian perlu melog masuk dengan ID iaitu kad pengenalan dan kata laluan yang telah didaftarkan. Peranti pengguna akan diimbas bagi memastikan memenuhi ciri-ciri keselamatan yang ditetapkan oleh polisi organisasi. Kemudian peranti pengguna dibenarkan mengakses rangkaian organisasi. Proses ini ditunjukkan seperti Rajah 5.



Rajah 5 : Proses Pendaftaran dan Log masuk

Copyright@FTSM UKM

Rajah 6 menunjukkan aliran proses bagi akses pengguna yang dihalang kerana tidak mematuhi polisi keselamatan organisasi. Peranti pengguna akan diimbas dari segi versi antivirus dan versi sistem pengoperasian. Pengguna yang tidak mempunyai versi perisian terkini akan dihalang akses dan peranti rangkaian komputer riba tersebut akan dinyahaktif (*disable network adapter*).

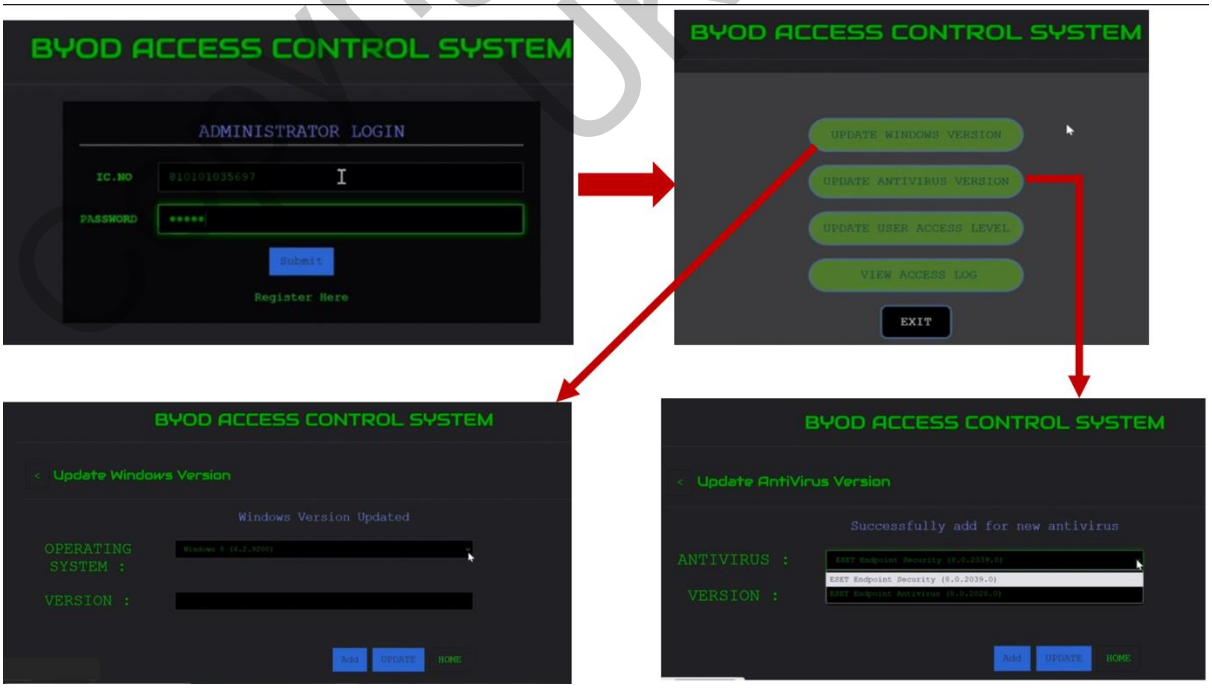
Rajah 6 : Proses Akses Dihalang

Sistem ini juga boleh membuat padanan antara ID pengguna (kad pengenalan) dan ID peranti (alamat MAC). Pengguna yang berdaftar perlu menggunakan peranti yang didaftarkan. Sekiranya pengguna melog masuk menggunakan peranti berbeza, akses pengguna akan disekat dan peranti rangkaian komputer riba tersebut akan dinyahaktif (*disable network adapter*) seperti Rajah 7.

Copyright@FTSM UKM

Rajah 7 : Proses Padanan ID Pengguna dan ID Peranti

BACSYM juga mempunyai fungsi pentadbir di mana pentadbir boleh membuat kemaskini versi atau tambahan sistem pengoperasian atau perisian antivirus mengikut polisi organisasi seperti Rajah 8. Data ini akan digunakan oleh agen semasa mengimbas peranti pengguna.



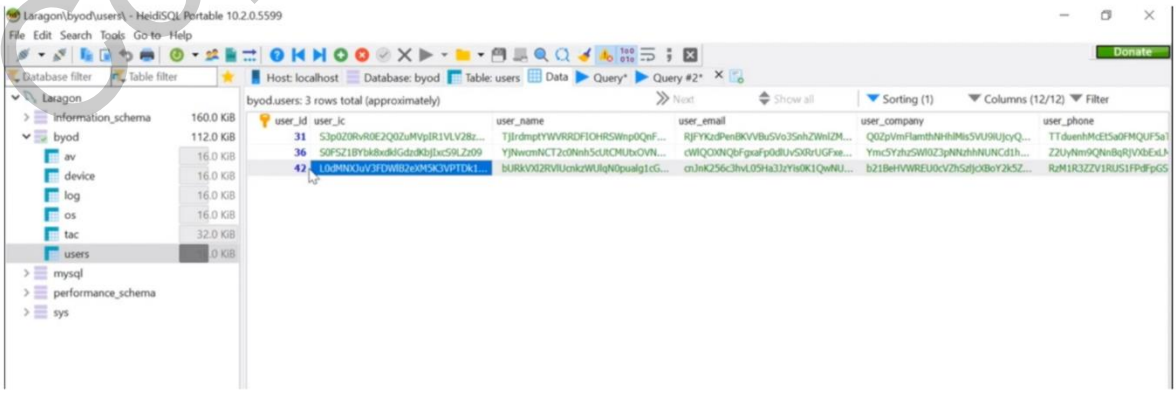
Rajah 8 : Kemaskini OS dan Antivirus

©Copyright@FTSM UKM

Pentadbir boleh menukar tahap akses pengguna dari pengguna biasa kepada pentadbir seperti Rajah 9. BACSYM juga boleh memaparkan log akses pengguna yang mengakses rangkaian organisasi.

Rajah 9 : Tahap Akses dan Log Akses Pengguna

BACSYM juga menitik beratkan keselamatan data pengguna di mana semua maklumat peribadi pengguna seperti nama, e-mel, nombor kad pengenalan dan kata laluan serta maklumat peranti pengguna seperti *MAC address* akan di buat penyulitan (*encryption*) iaitu kaedah Hash dan SHA-2 sebelum di simpan di dalam pangkalan data seperti Rajah 10.



Rajah 10 : Penyulitan Maklumat Pengguna

Copyright@FTSM UKM

Secara keseluruhannya, sistem ini berjaya mencapai objektif yang disasarkan di mana tapisan keselamatan sesuatu peranti melibatkan tiga perkara iaitu pendaftaran identiti pengguna, pendaftaran identiti peranti yang dipadankan dengan identiti pengguna serta kawalan versi sistem pengoperasian Windows dan antivirus yang digunakan mestilah terkini mengikut polisi keselamatan organisasi. Objektif ini telah berjaya dicapai dan dibuktikan dengan keputusan dari hasil pengujian yang dilaksanakan. Di samping itu juga sistem yang dibangunkan ini tidak akan mengganggu data-data peribadi pengguna di dalam peranti memandangkan fokus operasinya adalah untuk membuat tapisan keselamatan berdasarkan objektif yang dijelaskan sebelum ini. Justeru dari segi integriti sistem di peringkat pengguna adalah terjamin.

6. KESIMPULAN

Kesimpulannya, projek pembangunan Sistem BACSYM ini dibangunkan supaya dapat menyelesaikan masalah keselamatan data dan pada masa yang sama memberi kebenaran pengguna untuk menggunakan peranti persendirian. Laporan ini menerangkan secara terperinci mengenai keseluruhan fasa pembangunan sistem. Proses pengujian menunjukkan sistem ini telah mencapai objektif yang disasarkan dan memberi keputusan yang positif.

Sistem ini boleh ditambah baik dari segi keselamatan sistem terutama bagi keselamatan pangkalan data bagi memenuhi keperluan ISO27001 yang menjelaskan data yang disimpan perlu dilindungi dari segi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi (ISO 27001 International Standard). Selain itu, sistem ini boleh diuji pada persekitaran organisasi sebenar yang disambungkan kepada pelbagai peranti rangkaian dan keselamatan. Ini bagi menunjukkan keupayaan sebenar sistem dalam membenarkan dan menyekat akses pengguna ke internet atau data sulit organisasi. Spesifikasi pelayan dan peranti yang digunakan juga boleh ditambahbaik bagi mempercepatkan proses imbasan agen dan penyambungan antara peranti dan sistem.

Sistem juga dapat ditambah baik dengan mempunyai fungsi untuk integrasi dengan mana-mana laman web yang mempunyai maklumat versi Windows dan versi antivirus terkini yang terdapat di pasaran agar data-data versi itu dapat disimpan di pangkalan data Sistem BACSYM secara

Copyright@FTSM UKM

langsung tanpa memerlukan pentadbir sistem melakukan proses pendaftaran bagi maklumat-maklumat tersebut. Sistem juga boleh ditambahbaik dengan menyediakan fungsi pemasangan agen secara langsung ke peranti pengguna selepas proses pendaftaran agar interaksi pengguna dengan sistem lebih efisien.

Umumnya, Sistem BACSYM ini boleh ditambah baik di masa hadapan bagi mengoptimumkan fungsinya dalam persekitaran BYOD. Seterusnya, diharap sistem ini dapat dijadikan asas dan rujukan dalam pembangunan sistem yang berkaitan agar keselamatan rangkaian dan data organisasi yang membenarkan pelaksanaan BYOD terjamin.

7. RUJUKAN

Lucas Mearian. 2020. Microsoft's Intune is now Endpoint Manager: What is it, and how well does the UEM tool work? https://www.computerworld.com/article/3304583/what-is-microsofts-intune-and-how-well-does-it-really-work.html [16 Disember 2020]

Mahat, N., & Ali, N. 2018. Empowering Employees through BYOD : Benefits and Challenges in Malaysian Public Sector. International Journal of Engineering & Technology Website, 7, 643–649.

Olalere, M., Abdullah, M.T, & Abdullah, A. 2015. A Review of Bring Your Own Device on Security Issues. SAGE Open, pp. 1–11.

Shari Barnett. 2020. New collaboration connects SolarWinds MSP remote monitoring and management solutions with Microsoft 365 https://www.solarwindsmsp.com/blog/solarwindsmsp-collaborates-with-microsoft [16 Disember 2020]

Royce, W. W. 1970. Managing the Development of Large Software Systems (1970). Ideas That Created the Future, (August), 321–332.

Wmware. 2018. Five Important Buying Criteria To Enable A Totally Mobile Workforce White Paper https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/company/vmw-five-buying-criteria-enable-totally-mobile-workforce-whitepaper.pdf [15 Disember 2020]

Zheng, Y., Cao, Y., & Chang, C. H. 2018. Facial biohashing based user-device physical unclonable function for bring your own device security. 2018 IEEE International Conference on Consumer Electronics, ICCE 2018, 2018-Janua, 1–6.

Copyright@FTSM UKM