SISTEM PERKONGSIAN FAIL SECARA SULIT MENGGUNAKAN 256- BIT *ADVANCED ENCRYPTION STANDARD* (AES)

SYAFIQAH IZZATI MOHD SHAFIEE

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Kajian ini bertujuan untuk membangunkan sebuah sistem perkongsian fail selamat yang menggunakan *Advanced Encryption Standard* (AES) 256-bit di mana ia akan memberikan tahap perlindungan yang tinggi untuk fail yang ditukar. Dengan menggunakan kunci 256-bit, kaedah *Advanced Encryption Standard* (AES) mengubah teks atau data biasa menjadi cipher di mana ianya menjadi praktikal hingga tidak dapat ditembusi. Dengan panjang kunci 256-bit, sistem ini akan dapat menghasilkan sejumlah besar kunci berpotensi, menjadikannya sangat aman terhadap serangan *brute-force*. Sistem ini mungkin akan memasukkan pengenalan dan kebenaran pengguna sehingga hanya pengguna yang diberi kuasa yang dapat mengakses fail yang dikongsi. Ini akan menghalang akses tanpa izin ke fail bersama dan menjaga kerahsiaan dan integriti maklumat. Sistem perkongsian fail selamat berasaskan AES 256-bit akan menawarkan tahap keselamatan yang tinggi untuk fail yang dihantar. Data bersama akan dilindungi dari akses tanpa izin berkat penggunaan enkripsi AES, pengenalan dan kebenaran pengguna, dan protokol selamat. Tidak ada yang dapat menguraikan kandungan fail kerana fail tersebut akan dienkripsi sepenuhnya dan hanya sistem yang dicadangkan sahaja akan dapat menyahsulitkan fail tersebut. Pembangunan aplikasi sistem ini melibatkan penggunaan *Visual Studio 2019* dan *Microsoft Access*. Kajian ini menggunakan pendekatan *Iterative Waterfall Model* untuk membangunkan sistem ini. Pendekatan ini mempunyai beberapa peringkat termasuk peringkat pengumpulan keperluan, analisis, reka bentuk, pembangunan, pengujian dan penyelenggaraan. Kesimpulannya, sistem ini mudah untuk digunakan dan mesra pengguna.

1 PENGENALAN

Penyulitan adalah penting untuk keselamatan internet secara keseluruhan. Terdapat sistem penyulitan yang berbeza yang digunakan hari ini, tetapi semuanya secara amnya berfungsi dengan mengacak data dengan bantuan algoritma matematik, menyulitkan maklumat ke dalam kod. Salah satu piawaian penyulitan yang paling biasa hari ini ialah *Advanced Encryption Standard* (AES). Ia adalah varian sifir blok Rijndael dan tersedia dalam tiga saiz utama: 128, 192 dan 256 bit. Konsep asas penyulitan ialah sifir menggantikan setiap unit maklumat dengan yang lain, bergantung kepada kunci keselamatan. Sebagai contoh, AES-256 melengkapkan 14 pusingan penyulitan, menjadikannya sangat selamat.

Advanced Encryption Standarad (AES) ialah sifir blok simetri yang dipilih oleh kerajaan Amerika Syarikat untuk melindungi maklumat terperingkat. AES dilaksanakan dalam perisian dan perkakasan di seluruh dunia untuk menyulitkan data sensitif. Ia penting untuk keselamatan komputer kerejaan, keselamatan siber dan perlindungan data elektronik. *National Institute of Standards and Technology* (NIST) memulakan pembangunan AES pada tahun 1997 apabila ia mengumumkan keperluan untuk alternatif kepada *Data Encryption Standard* (DES)

yang mula menjadi terdedah kepada serangan kekerasan. NIST menyatakan bahawa algoritma AES yang lebih baharu adalah tidak diklasifikasikan dan mesti mampu untuk melindungi maklumat sensitif kerajaan dengan baik pada abad ke-21.

Perkongsian fail merupakan satu tindakan berkongsi satu fail komputer dengan seseorang di rumah yang sama, ahli pasukan di tempat kerja atau rakan di negara lain. Perkongsian fail ini juga boleh digunakan untuk mengakses fail tersebut di mana-mana sahaja. Ia adalah pengedaran data atau sumber peribadi atau awam dalam rangkaian dengan tahap keistimewaan perkongsian yang berbeza. Perkongsian fail ini adalah ciri perkhidmatan komputer pelbagai guna yang berkembang daripada media boleh tanggal melalui protokol rangkaian seperti *File Transfer Protocol* (FTP). Banyak mekanisme perkongsian fail telah diperkenalkan termasuk FTP dan *Internet Relay Chat* (IRC) pada awal tahun 1990-an. Kebanyakkan tugas perkongsian fail menggunakan dua aset asas kriteria rangkaian iaitu Perkongsian Fail *Peer-to-Peer* dan Perkhidmatan Pengehosan Fail (*File Hosting Services*).

Perkongsian Fail *Peer-to-Peer* (P2P) adalah kaedah perkongsian fail yang paling popular tetapi kontroversial kerana penggunaan perisian *peer-to-peer*. Pengguna komputer rangkaian mencari data yang dikongsi dengan perisian pihak ketiga. Perkongsian fail P2P membolehkan pengguna mengakses terus, memuat turun dan mengedit fail. Sesetengah perisian pihak ketiga memudahkan perkongsian P2P dengan mengumpul dan membahagikan fail besar kepada kepingan yang lebih kecil. Namun begitu, perkongsian fail tidak begitu selamat kerana ia sering menggunakan keselamatan kata laluan semata-mata yang membolehkan penggodam dengan mudah memecahkan kod dan mencuri fail di mana ia akan melibatkan pelanggaran data (*data breaches*). Fail akan menjadi lebih selamat jika ia disulitkan dengan algoritma 256-bit *Advanced Encryption Standard* (AES). ‘Rangkaian permutasi-penggantian’ menyokong AES kerana ia terdiri daripada urutan operasi yang dipautkan, sebahagian daripadanya melibatkan penggantian input dengan output tertentu (penggantian) dan lain-lain yang memerlukan bit bergerak di sekeliling (permutasi).

Salah satu isu yang sangat diperdebatkan dalam keselamatan terbenam dan komputer ialah sama ada kunci simetri 256-bit yang digunakan untuk AES adalah selamat dari segi pengiraan terhadap serangan kekerasan. Walaupun terdapat beberapa kesilapan yang wujud AES, kerajaan dan syarikah melaburkan kepercayaan yang besar dengan andaian bahawa ia adalah sangat selamat sehingga kunci keselamatannya tidak boleh dikompromi (Nitin Dahad,

2012). Ini adalah sebab mengapa projek ini menggunakan kunci simetri 256-bit *Advanced Encryption Standard* (AES).

National Institute of Standards and Technology (NIST) memilih algoritma Rijndael (disebut "Anak patung Rhine") oleh ahli kriptografi Belgium Joan Daemen dan Vincent Rijmen pada Oktober 2000 sebagai pemenang dalam pertandingan untuk menggantikan *Data Encryption Standard* (DES). Walaupun pada asalnya ia diluluskan untuk penyulitan hanya data kerajaan yang tidak berperingkat, AES telah diluluskan untuk digunakan bagi maklumat sulit Rahsia dan Rahsia Besar kerjaan Amerika Syarikat pada tahun 2003. AES ialah sifir blok simetri, beroperasi pada blok data bersaiz tetap. Matlamat AES bukan sahaja untuk memilih algoritma sifir baharu tetapi juga untuk meningkatkan secara mendadak kedua-dua blok dan saiz kunci berbanding DES. Salah satu kelebihan AES ialah tiada kekunci "lemah" atau "separuh lemah" untuk dielakkan (seperti dalam DES, yang mempunyai 16 daripadanya).

Sistem perkongsian fail ini menggunkan algoritma Rijndael yang merupakan sifir blok yang baru-baru ini dipilih oleh National Institute of Standards and Technology (NIST) sebagai Advanced Encryption Standard (AES). Pilihannya adalah berdasarkan analisis yang teliti dan komprehensif tentang ciri keselamatan dan kecekapan algoritma Rijndael. Algoritma yang dibangunkan telah direka bentuk sebagai struktur matematik yang mudah difahami dan boleh dipecahkan kepada komponen yang mudah. Daemen dan Rijmen menulis dalam cadangan kepada AES bahawa Rijndael telah direka berdasarkan tiga kriteria iaitu penentangan terhadap semua serangan yang diketahui, kelajuan dan kekompakan kod pada pelbagai platform dan juga kesederhanaan reka bentuk. AES telah diterima untuk pemindahan data penting oleh beberapa organisasi. Di luar kekuatan kriptografinya, AES direalisasikan dengan cekap dalam perkakasan dan perisian, satu pertimbangan penting memandangkan penggunaannya yang meluas.

Kekangan yang mungkin dihadapi dalam membangunkan sistem ini adalah kekurangan sumber. Hal ini demikian kerana pembangunan sesebuah sistem yang selamat dan efisien boleh mengambil masa dan memerlukan sumber yang cukup spserti pakar sistem, pengaturcara dan cara penyelidikan. Selain itu, kekangan masa kerana sepanjang tempoh kajian ini dilakukan sambil perlu menyiapkan tugasan subjek lain dan juga tugasan persatuan. Peraturan dan standard industri juga merupakan kekangan bagi sistem ini kerana sistem yang dibangunkan mestilah memenuhi standard industri yang berkenaan dengan keselamatan data.

2 PENYATAAN MASALAH

Sistem perkongsian fail yang saat ini digunakan oleh organisasi seringkali tidak cukup selamat dan boleh menyebabkan risiko kepada keselamatan data. Terdapat keperluan untuk mengembangkan sistem perkongsian fail yang lebih selamat yang dapat melindungi fail dari akses yang tidak sah dan mengekalkan integriti data. Oleh itu, permasalahan yang ingin diselesaikan adalah bagaimana untuk mengembangkan sistem perkongsian fail yang selamat dengan menggunakan 256-bit *Advanced Encryption Standard* (AES).

Terdapat banyak sebab mengapa fail yang dilindungi kata laluan tidak boleh digunakan, termasuk penyelenggaraan kata laluan, kerana kata laluan PDF yang kuat sukar untuk disediakan dan digunakan. Oleh kerana kata laluan dihantar dalam format yang boleh dibaca, ia mudah dikongsi dengan pengguna yang tidak dibenarkan. Kata laluan mudah dicuri kerana ia sering dibiarkan boleh diakses dalam dokumen teks biasa untuk dipanggil semula atau disalin/tampal dengan mudah. Dalam sejam, 16 karakter ASCII kata laluan boleh direkak.

Apabila tiada kata laluan biasa dipilih, hanya mengambil masa 1 jam untuk memecahkan kata laluan ASCII 16 aksara (pemecah kata laluan menyemak senarai kata laluan yang biasa digunakan dahulu). Ia mengambil masa beberapa saat atau minit jika kata laluan yang kerap digunakan digunakan. Kesimpulannya, kata laluan PDF tidak berkesan untuk melaksanakan keselamatan PDF kerana ianya sukar dikawal dan mudah dikalahkan.

Secara keseluruhannya, permasalahan yang ingin diselesaikan adalah bagaimana untuk mengembangkan sistem perkongsian fail yang selamat dengan menggunakan 256-bit Advanced Encryption Standard (AES) yang meliputi mekanisme pengesahan pengguna, pemberian kebenaran, protokol yang selamat dan akses kawalan berdasarkan peranan. Ini akan memastikan fail-fail PDF yang dikongsikan adalah selamat dari akses yang tidak sah dan mengekalkan integriti data.

3 OBJEKTIF KAJIAN

Objektif kajian bagi pembangunan Sistem Perkongsian Fail Secara Sulit menggunakan 256-bit Advanced Encryption Standard (AES) adalah untuk mengesahkan pengguna dengan selamat dan membuat profil pengguna yang disahkan dimana pengguna perlu membuat akaun dan perlu log masuk ke dalam sistem sebelum dapat berkongsi fail. Hal ini untuk menyediakan platform

penghantaran fail yang selamat untuk pengguna. Selain itu, sistem ini dibangunkan untuk melindungi fail dari akses yang tidak sah dengan menggunakan algoritma penyulitan AES 256-bit dan juga untuk memberikan mekanisme pengesahan pengguna yang kuat untuk memastikan hanya pengguna yang sah sahaja yang boleh mengakses fail yang dikongsikan.

4 METOD KAJIAN

Metodologi yang digunakan untuk membangunkan Sis\stem Perkongsian Fail secara Sulit menggunakan AES 256-bit ini adalah *Iterative Waterfall Model*, dalam kitaran hayat pembangunan *(Software Development System Life Cycle, SDLC)*. SDLC ialah proses yang diikuti untuk projek perisian dalam organisasi perisian. Ia terdiri daripada pelan terperinci yang menerangkan cara membangunkan, menyelenggara, menggantikan dan mengubah atau meningkatkan perisian tertentu. Metodologi yang dipilih ini menyediakan saluran maklum balas dari setiap fasa ke fasa sebelumnya. Apabila masalah ditemui kemudian saluran maklum balas membenarkan fasa di mana pengubahsuaian ralat dilakukan dan pengubahsuaian ini ditunjukkan dalam fasa berikutnya. Fasa yang terdapat dalam metodologi ini adalah Fasa Pengumpulan Keperluan, Analisis, Reka Bentuk, Pembangunan, Pengujian serta Penyelenggaraan.

4.1 Fasa Pengumpulan Keperluan

Fasa Pengumpulan Keperluan merupakan fasa yang terpenting dalam pembangunan Sistem Perkongsian Fail secara Sulit menggunakan *Advanced Encryption Standard* (AES) dimana perancangan dalam membangunkan sistem ini adalah jelas dan kajian awal terhadap sistem dititikberatkan. Semasa fasa ini, keperluan terperinci sistem perisian yang akan dibangunkan akan dikumpulkan. Masalah yang berkaitan dengan projek yang akan dibangunkan akan dikenal pasti. Pada fasa ini, penentuan tajuk dan kaedah membina sistem akan dijalankan. Setelah penentuan tajuk, kajian kesusasteraan akan diadakan untuk mengenal pasti masalah serta mengkaji latar belakang masalah. Perbandingan antara sistem yang sedia ada turut dijalankan bagi memahami keperluan sistem. Pada pengakhiran fasa ini, Carta Gantt akan dihasilkan bagi memastikan kerja-kerja dapat disiapkan pada masa yang ditetapkan. Skop dan objektif projek juga ditetapkan dalam fasa ini. Pengumpulan data dibuat melalui bahan ilmiah seperti artikel dan juga laman sesawang.

4.2 Fasa Analisis

Analisis sistem sangat penting untuk memahami kelemahan sistem semasa. Tujuan mempelajari sistem ini adalah untuk mengembangkan sistem yang dapat memenuhi keperluan dan kehendak pengguna. Perisian-perisian yang akan digunakan dalam pembangunan projek juga ditentukan pada fasa ini demi membangunkan sistem dengan baik. Kajian dijalankan dalam bentuk sorotan susastera terhadap sistem atau aplikasi sedia ada untuk membuat perbandingan terhadap kelemahan yang dimiliki. Seterusnya, setiap kemungkinan keperluan sistem terperinci untuk dibangunkan dianalisa dan didokumentasikan dalam dokumen spesifikasi keperluan. Pada pengakhiran fasa ini, keperluan dan fungsi aplikasi dikenal pasti.

4.3 Fasa Reka Bentuk

Pada fasa ini Sistem Perkongsian Fail secara Sulit menggunakan 256-bit *Advanced Encryption Standard* (AES) akan direka bentuk. Sistem beroperasi dari segi perkakasan, perisian, dan infrastruktur rangkaian iaitu antara muka, bentuk, laporan, dan pangkalan data juga dititikberatkan. Perisian *Visual Studio 2019* digunakan untuk mengembangkan antara muka dan pangkalan data sistem tersebut. Tinjauan akan dilakukan untuk mengumpulkan maklum balas pengguna mengenai antara muka yang dirancang untuk memastikan bahawa antara muka yang dirancang mudah difahami dan mesra pengguna. Fasa reka bentuk ini adalah fasa yang penting bagi *Iterative Waterfall Model* kerana ia memastikan sistem yang dibangunkan akan sesuai dengan spesifikasi yang diperlukan dan dapat digunakan dengan mudah oleh pengguna. Pada pengakhiran fasa ini, reka bentuk antara muka seluruh sistem, carta alir, rajah jujukan dan rajah kes guna akan terhasil.

4.4 Fasa Pembangunan

Fasa pembangunan ini menjelaskan reka bentuk kepada kajian ini. Fasa ini merupakan fasa yang kritikal, mencabar dan sangat penting untuk dititikberatkan bagi setiap pembangun sistem. Fasa ini memerlukan tempoh yang lama untuk menyiapkan fasa ini kerana bahan-bahan yang telah dikumpulkan dan dikaji akan diguna pakai dalam fasa ini. Hasil akhir projek ini bergantung pada fasa ini kerana sekiranya sistem ini dapat berfungsi dengan baik tanpa sebarang masalah, maka, sistem ini merupakan sistem yang telah berjaya dihasilkan. Pembangun sistem perkongsian fail telah mula dilakukan berdasarkan apa yang telah dirancang melalui fasa ini.

4.5 Fasa Pengujian

Pada fasa pengujian, setelah Sistem Perkongsian Fail secara Sulit menggunakan 256-bit *Advanced Encryption Standard* (AES) selesai dibangunkan, sistem tersebut akan diuji secara keseluruhan. Ujian dilakukan bersama dengan penyelia dan pengguna untuk memastikan bahawa aplikasi yang dibina dapat memenuhi keperluan pengguna. Pengujian turut dilaksanakan untuk memastikan tiada sebarang ralat sepanjang penggunaan aplikasi. Pada pengakhiran fasa ini, maklum balas daripada pengguna juga dicatat dan penambahbaikan aplikasi akan dijalankan berdasarkan maklum balas pengguna yang diperolehi. Sistem ini diuji bagi memastikan produk yang dihasilkan dapat mencapai keperluan yang dinyatakan di dalam objektif.

4.6 Fasa Penyelenggaraan

Terdapat beberapa isu yang timbul dalam persekitaran pengguna. Penyelengaraan dilakukan untuk menyampaikan perubahan ini dalam persekitaran pengguna dalam memastikan keperluan pengguna dicapai seperti yang telah dinyatakan di dalam objektif dan cadangan penyelesaian bagi permasalahan tersebut.

5 HASIL KAJIAN

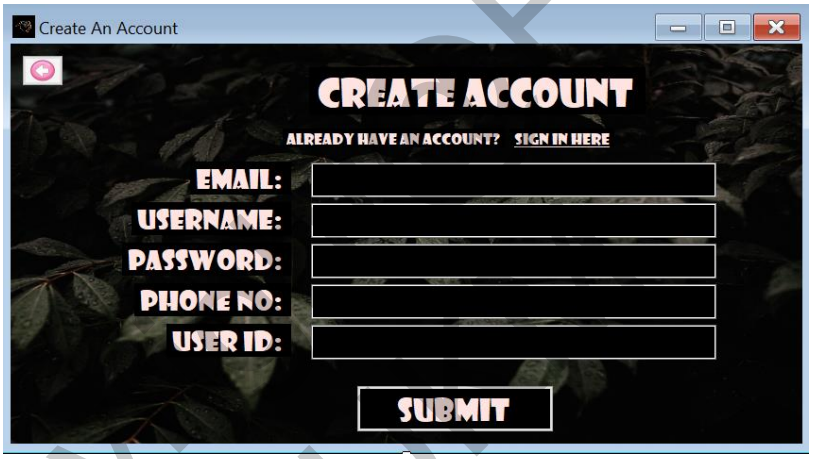
Pembangunan sistem telah dijalankan berdasarkan keperluan-keperluan dan reka bentuk yang telah ditetapkan. *Visual Studio 2019* merupakan Persekitaran Pembangunan Bersepadu juga dikenali sebagai *Integrated Development Environment* (*IDE*) utama untuk pembangunan sistem. *Microsoft Access* telah digunakan sebagai sistem pengurusan pangkalan data. Hasil pembangunan akan dibincangkan berdasarkan modul yang dikenal pasti. Hasil pembangunan akan dibincangkan berdasarkan modul yang dikenal pasti. Untuk log masuk pengguna, Email/Password Sign-In digunakan.

5.1 Pembangunan Fungsi Membuat Akaun dan Log Masuk

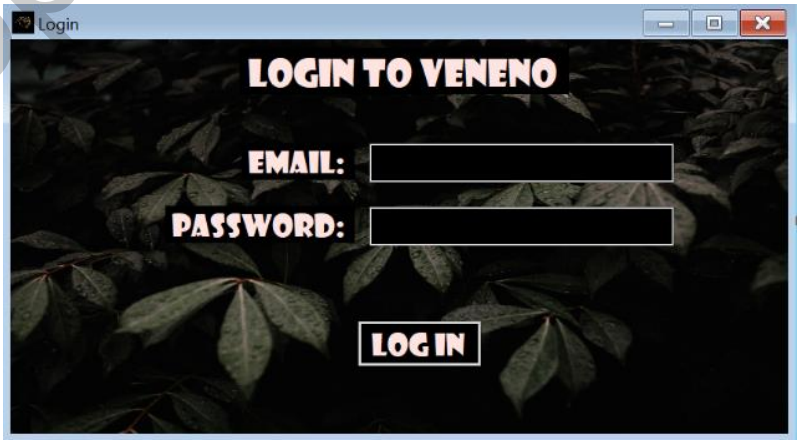
Proses membuat akaun merupakan proses di mana pengguna baharu mencipta akaun dalam sistem. Ia melibatkan maklumat yang diperlukan sepeti nama pengguna (*username*), alamat e-mel, nombor telefon, dan mencipta kata laluan. Tujuan pendaftaran adalah untuk mewujudkan identity pengguna dan mencipta akaun peribadi yang boleh digunakan untuk berinteraksi masa depan

dengan sistem. Manakala log maasuk pula dirujuk sebagai proses pengesahan di mana pengguna mengakses akaun mereka ke dalam sistem. Ia melibatkan bukti kelayakan (*authentication*) yang dibuat sebelum ini, biasanya nama pengguna atau alamat e-mel bersama dengan kata laluan sepadan.

Proses pendaftaran yang berlaku dalam aplikasi menggunakan fungi Create Account. Pengguna perlu mengisi InputField yang memerlukan nama unik, alamat e-mel, kata lauan, nombor telefon. Sekiranya penciptaan akaun berjaya, pengguna akan melihat mesej "Registration Successful". Manakala bagi aktiviti log masuk, pengguna perlu mengisi InputField yang memerlukan alamat e-mel berdaftar serta kata laluan. Sekiranya log masuk berjaya, penggunakan akan melihat paparan mesej "You are successfully logged in" dan akan di bawa ke halaman utama.



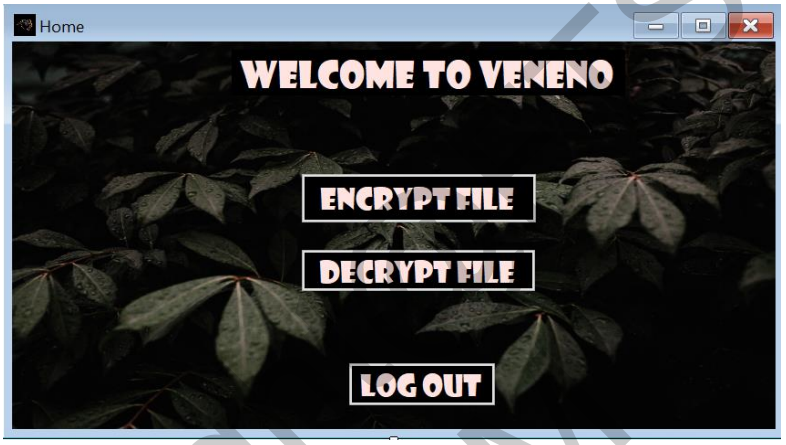
Rajah 1 Antara Muka Membuat Akaun



Rajah 2 Antara Muka Log Masuk

5.2 Pembangunan Halaman Utama

Halaman utama merujuk kepada paparan setelah pengguna log masuk ke aplikasi. Matlamat pembangunan paparan skrin utama pengguna aplikasi ini adalah untuk menghasilkan antara muka pengguna yang mudah, cekap dan mesra pengguna serta membolehkan mengendalikan aplikasi dengan kebolehgunaan maksimum. Pengguna boleh mendapat petunjuk yang jelas tentang apa yang boleh dicapai seperti *Encrypt File*, *Decrypt File* dan *Log Out* melalui paparan skrin utama. Para pengguna hanya perlu menekan butang fungsi yang mereka ingini kemudian halaman tersebut akan dibuka. Rajah 3 menunjukkan antara muka paparan halaman utama.



Rajah 3 Antara Muka Halaman Utama

5.3 Pembangunan Fungsi Penyulitan dan Penyahsulitan Fail

Pembangunan fungsi ini merupakan pembangunan yang paling sulit. Hai ini demikian kerana kekurangan sumber mengenai algoritma kriptografi yang digunakan. Bagi fungsi ini, para pengguna boleh memilih sama ada ingin menyulitkan fail yang diingini atau memilih untuk menyahsulitkan fail. Rajah 4 menunjukkan antara muka bagi fungsi penyulitan dan penyahsulitan fail.

Rajah 4 Antara Muka Penyulitan dan Penyahsulitan Fail

5.4 Pengujian

Pendekatan Pengujian Kes Guna *(Use Case Testing)* digunakan untuk memastikan keberkesanan aplikasi Sistem Perkongsian Fail secara Sulit menggunakan 256-bit *Advanced Encryption Standard* (AES).

Dalam Pengujian Kes Guna *(Use Case Testing)* bagi Sistem Perkongsian Fail secara Sulit menggunakan 256-bit *Advanced Encryption Standard* (AES), kes guna yang berkaitan dikenal pasti berdasarkan keperluan aplikasi, seperti membuat akaun bagi pengguna baharu, log masuk ke aplikasi, penyulitan fail, penyahsulitan fail, dan sebagainya. Senario ujian dicipta untuk merangkumi kawasan dan variasi yang berbeza dalam setiap kes guna. Kes ujian kemudiannya direka bentuk, termasuk data ujian yang diperlukan, hasil yang dijangkakan, dan sebarang prasyarat. Kes ujian ini dilaksanakan secara sistematik, membandingkan keputusan sebenar dengan hasil yang dijangkakan. Isu atau masalah yang dihadapi semasa ujian dicatat untuk penyelesaian kelak. Pengujian kes guna membantu memastikan aplikasi berfungsi seperti yang diharapkan serta memenuhi keperluan pengguna dengan berkesan.

Hasil pengujian menunjukkan bahawa modul ini dan setiap fungsi yang diliputi oleh modul ini boleh berfungsi dengan lancar.

6 KESIMPULAN

Secara keseluruhannya, sistem perkongsian fail secara sulit menggunakan 256-bit *Advanced Encryption Standard* (AES) berjaya dibangunkan mengikut perancangan masa yang ditetapkan. Melalui setiap fasa, sistem perkongsian fail secara sulit ini telah berjaya melalui fasa mengikut model air terjun yang dicadangkan dalam peringkat analisis keperluan, reka bentuk sistem, pelaksanaan atau implementasi, dan pengujian. Sistem perkongsian fail secara sulit ini diharapkan agar dapat menyempurnakan objektif kajian iaitu mengesahkan pengguna dengan selamat dan membuat profil pengguna yang disahkan dimana pengguna perlu membuat akaun dan perlu log masuk ke dalam sistem sebelum dapat berkongsi fail. Hal ini untuk menyediakan platform penghantaran fail yang selamat untuk pengguna. Selain itu, dapat melindungi fail dari akses yang tidak sah dengan menggunakan algoritma penyulitan AES 256-bit dan juga dapat memberikan mekanisme pengesahan pengguna yang kuat untuk memastikan hanya pengguna yang sah sahaja yang boleh mengakses fail yang dikongsikan.

Kekuatan bagi sistem perkongsian fail secara sulit termasuk melindungi fail dari akses yang tidak sah dengan menggunakan algoritma penyulitan AES 256-bit. Pengguna yang tidak sah tidak akan dapat mengakses fail yag telah dimuat naik malahan tidak dapat untuk melihat kandungan fail tersebut. Pengguna dapat menggunakan sistem ini tanpa perlu risau akan ancaman-ancaman lain yang berkemungkinan akan mengancam keselamatan fail. Namun begitu, sistem ini mempunyai beberapa kekangan di mana pengguna perlu mempunyai semua fail dan kod bagi membolehkan pengguna untuk menggunakan sistem ini. Hal ini sedikit sebanyak mengganggu objektif utama pembangunan sistem ini iaitu untuk menyediakan platform penghantaran fail yang selamat untuk pengguna.

Bagi menyempurnakan projek pembangunan sistem perkongsian fail secara sulit pada masa akan datang, beberapa cadangan penambahbaikan boleh dipertimbangkan untuk diimplementasi dalam fasa pembangunan seterusnya. Antara penambahbaikan yang boleh dilakukan adalah membuat lebih banyak penyelidikan tentang bagaimana AES 256-bit berfungsi dan bagaimana ingin menghasilkan algoritma kriptografi itu dengan jayanya. Hal ini dapat membuatkan sistem tersebut mencapai semua objektif yang diingini dalam penghasilan sistem.

Cadangan yang seterusnya adalah membuat sistem ini dengan menggunakan Android Studio atau menjadikan sistem ini sebagai Web Based Application. Hal ini demikian kerana para pengguna dapat mengakses sistem tersebut dengan mudah tanpa perlu memuat naik folder yang perlu dimuat naik bagi membolehkan sistem itu berfungsi.

Melalui pelaksanaan cadangan-cadangan penambahbaikan yang disenaraikan, diharapkan sistem perkongsian fail secara sulit menggunakan 256-bit Advanced Encryption Standard (AES) dapat meningkatkan prestasi keberkesanan dan kebolehgunaan aplikasi dalam kalangan pengguna. Para pengguna juga boleh mempercayai sistem yang telah dibangunkan tanpa sebarang keraguan terhadap keselamatan sistem tersebut.

7 PENGHARGAAN

Syukur Alhamdulillah kepada Allah S.W.T kerana memberikan saya kesihatan yang cukup, masa dan kematangan fikiran untuk menyiapkan kajian ini dalam bentuk sebegini rupa. Jutaan terima kasih yang rasanya tidak saya mampu untuk balas kembali hingga ke akhir hayat saya kepada penyelia utama Prof. Madya Dr. Ravie Chandren A/L Muniyandi atas bantuan yang begitu besar, bimbingan, teguran dan nasihat yang begitu berguna sepanjang kajian ini.

Selain itu, saya juga mnegucapkan ribuan terima kasih kepada ibu saya iaitu Puan Salbiah Ibrahim dan juga bapa saya iaitu Encik Mohd Shafiee M. Salleh yang memberi saya segala kemudahan, semangat, sokongan moral yang tidak terhingga sehingga saya dapat menyiapkan kajian ini dengan jayanya. Tidak lupa juga, ucapan penghargaan ini saya tujukan kepada rakan-rakan seperjuangan yang turut memberi peringatan dan sebagai pemudahcara. Mereka membantu saya dengan menjawab setiap kemusykilan umum yang saya utarakan.

Selain itu, saya juga ingin memberi ucapan penghargaan kepada Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia kerana memberi saya ruang dan peluan untuk meneruskan perjuangan pembelajaran dalam Ijazah Sarjana Muda Sains Komputer dengan Kepujian. Terima kasih juga kerana membenarkan saya membuat kajian bagi memperoleh ijazah tersebut.

Akhir kata, saya ucapkan terima kasih kepada semua yang terlibat secara lansung mahupun tidak lansung sepanjang pembikinan kerja kursus ini. Sekali lagi saya mengucapkan ribuan terima kasih. Saya amat menghargainya.

Sekian, terima kasih.

SYAFIQAH IZZATI MOHD SHAFIEE

8 RUJUKAN

A Brief History of Encryption. (2010, July 19). TechNewsWorld. https://www.technewsworld.com/story/a-brief-history-of-encryption-70437.html

adegeo. (n.d.). *What is Windows Forms - Windows Forms .NET*. Learn.microsoft.com. https://learn.microsoft.com/en-us/dotnet/desktop/winforms/overview/?view=netdesktop-7.0

AES Encryption | 256-Bit | Rijindael | Security | Protection | Encrypt | Decrypt | VB.net. (n.d.). Www.youtube.com. Retrieved July 22, 2023, from https://www.youtube.com/watch?v=QVUsxciGcKU

File Security System Java Project - 1000 Projects. (2018, May 3). https://1000projects.org/file-security-system-java-project.html [4 Disember 2022].

File sharing in Hybrid Model based P2P System Project Abstract - 1000 Projects. (2012, January 28). https://1000projects.org/file-sharing-in-hybrid-model-based-p2p-system-project-abstract.html [2 Januari 2023].

Intro to The AES-256 Cipher | HackerNoon. (n.d.). Hackernoon.com. Retrieved July 22, 2023, from https://hackernoon.com/intro-to-the-aes-256-cipher

Kaspersky. (2020). *How Data Breaches Happen*. Kaspersky. https://www.kaspersky.com/resource-center/definitions/data-breach [5 Disember 2022].

Nitin Dahad. (2012, May 7). How secure is AES against brute force attacks? EETimes. https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/ [6 Disember 2022].

NIST. (2001). FIPS PUB 197: Advanced Encryption Standard (AES) [6 Januari 2023].

NIST. (1977). Data Encryption Standard (DES) [6 Januari 2023].

NIST. (1999). Recommendation for Block Cipher Modes of Operation [6 Januari 2023].

ORPALIS. (n.d.). Password Protect PDF: Free, Secure & Encrypted | AvePDF. Password Protect PDF: Free, Secure & Encrypted | AvePDF. Retrieved January 11, 2023, from https://avepdf.com/lock-pdf [11 Januari 2023].

PDF Password Protection: How to Protect PDF Files without Passwords. (n.d.). Locklizard. Retrieved January 10, 2023, from https://www.locklizard.com/pdf-password-protection/ [10 Januari 2023].

Peterson, R. (2022, August 25). *DBMS Architecture: 1-Tier, 2-Tier & 3-Tier*. Www.guru99.com. https://www.guru99.com/dbms-architecture.html [31 Disember 2022].

RIJNDAEL. (n.d.). Www.cs.mcgill.ca. https://www.cs.mcgill.ca/~kaleigh/computers/crypto_rijndael.html

Secure File Sharing System Java Project – 1000 Projects. (n.d.). 1000projects.org. https://1000projects.org/secure-file-sharing-system-java-project.html [7 Disember 2022].

What is Rijndael Encryption? (2023, June 9). Easy Tech Junkie. https://www.easytechjunkie.com/what-is-rijndael-encryption.htm#comments

Syafiqah Izzati binti Mohd Shafiee (A181059)
Prof. Madya Dr. Ravie Chandren A/L Muniyandi
Fakulti Teknologi & Sains Maklumat,
Universiti Kebangsaan Malaysia