PENYIMPANAN DATA SULIT DALAM PERSEKITARAN BERBILANG AWAN

DINESWARAN A/L NAVARASAN
ASSOC. PROF. DR. ELANKOVAN A. SUNDARARAJAN

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

Abstrak

Pengkomputeran awan telah berkembang selama bertahun-tahun untuk mengatasi kekangan pengiraan dan penyimpanan peranti mudah alih. Walaupun pengkomputeran awan mempunyai faedahnya, kebimbangan keselamatan mengenai data pengguna masih wujud. Data yang disimpan di dalam awan dihantar melalui Internet dimana pengguna tidak mempunyai kawalan dan terdedah kepada pelanggaran data yang disebabkan oleh perisian hasad atau serangan orang dalam. Kajian ini bertujuan untuk memastikan keselamatan data dalam berbilang awan awam dengan pelbagai jenis penyulitan, teknik penghirisan dan juga panduan penggunaan aplikasi tersedia untuk pengguna. Aplikasi yang dicadangkan akan menyulitkan data di mana berbilang algoritma penyulitan disediakan dan ia juga memberi pilihan kepada pengguna untuk memilih jenis teknik penghirisan yang hendak digunakan. Selepas menghiris, pelbagai segmen akan dihiris di mana setiap segmen akan menjalani proses perawakkan dan dimuat naik secara rawak pada berbilang storan awan yang berbeza. Pengguna yang masih baru dalam dunia digital akan dibekalkan dengan beberapa maklumat dan penjelasan ringkas tentang apa itu penyulitan dan cara teknik penghirisan berfungsi pada data mereka. Langkah keselamatan yang dilaksanakan akan menghalang pelanggaran data pada awan walaupun salah satu akaun awan digodam. Ia juga memberi pengguna kebebasan untuk memilih jenis penyulitan dan teknik penghirisan untuk digunakan pada fail peribadi mereka, memberikan lapisan keselamatan tambahan untuk mengelakkan data mereka daripada dicuri ataupun hilang.

Kata kunci: [Penyulitan, Penghirisan, Storan Awan, Penyimpanan Data Sulit]

Pengenalan

Dengan peningkatan penggunaan data, kemunculan pengkomputeran awan telah membolehkan individu dan organisasi perniagaan menggunakan sumbernya tanpa batasan penyimpanan yang terdapat dalam peranti mudah alih. Pengkomputeran awan membolehkan pengguna menyimpan data, aplikasi dan perkhidmatan melalui Internet. Pelbagai jenis data termasuk fail,imej dan video boleh disimpan di awan dan dicapai oleh aplikasi mudah alih atau komputer (Noh, 2013). Pengkomputeran awan boleh dikategorikan kepada Awan Persendirian, Awan Hibrid, Awan Awam, dan Awan Komuniti. Antara contoh storan awan awam adalah DropBox, Google Cloud dan juga Google Drive. Dengan pengkomputeran awan, persekitaran ujian telah siap disesuaikan mengikut keperluan pengguna di hujung jari mereka dan sering digabungkan dengan penyediaan automatik sumber fizikal dan maya. Penyulitan data ialah kaedah keselamatan di mana maklumat disulitkan dan hanya boleh diakses atau dinyahsulit oleh pengguna dengan kunci penyulitan yang betul. Data yang disulitkan, juga dikenali sebagai teks sifer, tidak boleh dibaca oleh seseorang yang mengakses tanpa kebenaran.

Penyataan Masalah

Walaupun pengkomputeran awan memberi banyak faedah, aspek keselamatan pengkomputeran awan menjadi kebimbangan kerana pengguna tidak mempunyai kawalan ke atas data apabila disimpan di storan awan menjadikannya terdedah kepada pencerobohan data. Penyimpanan data di dalam storan awan juga menjadi kebimbangan di mana serangan orang dalaman storan awan mampu berlaku di mana pekerja dalaman storan awan yang mampu mengakses data-data pengguna. Untuk menangani masalah ini, Avinesh membina perisian dengan teknik penghirisan secara dinamik. Kedua, aplikasi mudah alih Android yang dibina oleh Kareesma pula menyediakan teknik penghirisan dan juga penyulitan serta memuat naik data ke dalam 3 storan awan yang berbeza. Namun, pengguna tidak mempunyai fleksibiliti untuk memilih cara fail mereka dihiriskan. Pengguna

juga tiada fleksibiliti untuk memilih teknik penyulitan yang berbeza. Bukan semua pengguna tahu tentang teknik penyulitan dan jenis penghirisan yang akan disediakan di dalam aplikasi.

Cadangan Penyelesaian

Bagi memastikan tiada sebarang pencerobohan berlaku secara mudah ke atas data yang disimpan, pelbagai lapisan keselamatan yang bertahap tinggi harus digunakan. Teknik penghirisan data adalah antara cara penyelesaian masalah dan boleh dilakukan secara mendatar, menegak dan juga bercampur. Kemudian, kepingan data akan melalui proses penyulitan di mana tiga jenis teknik penyulitan disediakan dan pengguna boleh memilih mengikut kehendak mereka dan fail yang dinyahsulit dan dihiris akan dimuat naik ke tiga storan awan yang berbeza. Selain itu, panduan dan info ringkas akan disediakan supaya pengguna dapat mengetahui, memahami dan mempunyai fleksibiliti untuk memilih jenis penghirisan dan teknik penyulitan yang sesuai sebelum memuat naik fail mereka.

Objektif Kajian

Matlamat utama kajian ini dilakukan adalah untuk memastikan data yang disimpan 3 di storan awan awam adalah selamat tanpa sebarang serangan pencerobohan dengan memberi pilihan kepada pengguna untuk memilih tahap keselamatan yang disediakan. Bagi mencapai matlamat ini, objektif berikut digariskan:

1. Untuk membangunkan aplikasi yang dapat menyediakan tiga jenis penghirisan yang berbeza.
2. Menyediakan tiga jenis teknik penyulitan berbeza yang mempunyai ciriciri dan kelebihan yang berbeza.
3. Memaparkan info-info ringkas tentang jenis penghirisan dan teknik penyulitan yang ingin digunakan oleh pengguna yang tidak berpengetahuan sebagai panduan.

Skop Kajian

Aplikasi yang dibina ini akan menggunakan tiga penyedia perkhidmatan awan awam untuk menyimpan data iaitu Google Cloud Storage, Microsoft Azure Storage dan Amazon AWS S3. Fail jenis dokumen, video dan imej boleh dimuat naik ke dalam setiap storan awan tersebut. Penggunaan aplikasi mudah alih ini akan berfokus kepada Android.

Kekangan Kajian

Kekangan yang mungkin dihadapi adalah kerumitan projek akibat penggunaan pelbagai jenis teknik keselamatan yang dapat melambatkan proses debugging. Kelajuan Internet yang tidak stabil boleh memanjangkan proses pengujian memuat naik dan memuat turun fail yang bersaiz besar. Selain itu, setiap storan awan yang digunakan mempunyai storan percuma dan bilangan fail untuk dimuat naik yang terhad sahaja.

Sorotan Kesusasteraan

Pengkomputeran awan menawarkan pelbagai perkhidmatan kepada pengguna dan telah banyak berkembang sejak hari awalnya. Antara kegunaan perkhidmatan awan paling popular adalah storan awan di mana pengguna dapat menyimpan data serta dapat mengaksesnya dari mana-mana lokasi di dunia. Pelbagai ciri keselamatan telah dilaksanakan untuk menjaga keselamatan data pengguna storan awan. Namun, terdapat sedikit kebimbangan apabila data sensitif disimpan di storan awan. Antara isu yang menjadi kerisauan ialah pekerja di pihak penyedia perkhidmatan awam yang mampu mengusik dan mengganggu data dengan niat yang tidak baik (rogue employee) dan potensi kebocoran data semasa dalam transit ke pusat data. Apabila pengguna memuat naik data ataupun fail peribadi ke dalam storan awan, keselamatan data pengguna menjadi tanda persoalan kepada ramai terutamanya pengguna baharu storan awan. Terdapat banyak pendekatan yang diambil oleh penyelidik untuk meningkatkan keselamatan penyimpanan data di awan menggunakan pelbagai teknik.

1. Berdasarkan Rupesh R Bobde et al. (2015) keselamatan data boleh dilaksanakan melalui gabungan penggunaan algoritma penyulitan dan teknik penghirisan data. Teknik penghirisan data dilaksanakan dengan menggunakan 3 teknik hirisan yang terdiri daripada penghirisan menegak, mendatar atau bercampur. Dalam pendekatan ini, data dihiris ke dalam 3 kepingan dan disulitkan menggunakan 3 algoritma penyulitan yang berbeza sebelum dimuat naik di awan. Tiga jenis teknik penyulitan yang digunakan ialah AES, DES dan 3DES yang memastikan tahap keselamatan yang lebih baik pada data berbanding dengan algoritma penyulitan tunggal.

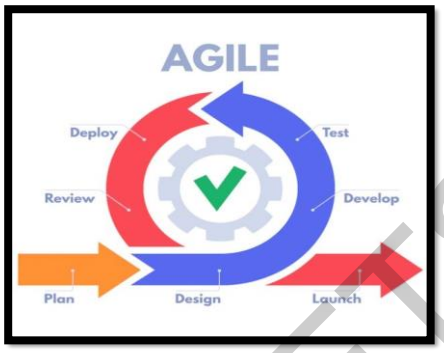
2. Berdasarkan Manoj V. Bramhe et al. (2019), penyimpanan data sulit pada pelbagai awan boleh dicapai dengan menggunakan teknik kriptografi. Sistem yang dicadangkan terdiri daripada beberapa modul termasuk pendaftaran dan log masuk, tetapan FTP, muat naik dan muat turun, penyulitan dan penyahsulitan dan modul penghirisan dan penggabungan. Modul pengurusan FTP digunakan untuk menulis dan membaca pelbagai fail ke pelayan dan dari pelayan. Tiga awan digunakan untuk storan di mana bahagian pertama fail disimpan dalam pelayan aplikasi tempatan (pelayan storan) dan bahagian kedua dan ketiga fail disimpan pada awan awam. Modul memuat naik digunakan untuk memuat naik fail manakala fungsi peta pelayan mengambil semula laluan pelayan untuk memuat naik data. Modul muat turun membolehkan pengguna mendapatkan semula fail dari storan awan menggunakan jadual pemetaan. Penyulitan dilakukan pada fail sebelum atau selepas memisahkan fail kepada kepingan. Teknik penyulitan yang digunakan adalah penyulitan simetri dan pelbagai algoritma seperti DES, 3DES, AES, Blowfish dan RC4 telah diuji. Proses penyulitan AES dilengkapi dengan kekunci keselamatan yang dijana secara rawak yang digunakan untuk menjana fail yang disulitkan dan mendapatkan semula fail untuk menyahsulitkannya. Modul penghirisan dan penggabungan memisahkan fail kepada kepingan semasa memuat naik dan menggabungkannya semasa muat turun. Metadata fail disimpan dalam pelayan aplikasi tempatan.

Berdasarkan kajian kesusasteraan yang dilaksanakan, sebanyak tiga jenis teknik penyulitan akan disediakan kepada pengguna iaitu DES, 3DES dan AES di mana pengguna boleh memilih jenis algoritma penyulitan yang ingin digunakan. Pelbagai teknik penghirisan akan disediakan kepada pengguna iaitu secara menegak, mendatar dan juga secara bercampur agar pengguna boleh menentukan bilangan kepingan dihiris dan cara fail mereka dihiris. Dengan ini, keselamatan fail akan melonjak naik kerana hanya pengguna sahaja akan tahu tentang bilangan kepingan fail dan teknik penghirisan yang digunakan. Bukan itu sahaja, kepingan-kepingan ini akan dimuat naik secara rawak ke dalam tiga storan awan yang berbeza iaitu Google Cloud Storage, Amazon AWS S3 dan Microsoft Azure. Tahap keselamatan yang tinggi sebegini mampu mengelakkan pekerja penyangak di pihak penyedia perkhidmatan awam untuk mengusik fail yang dimuat naik oleh pengguna. Bagi pengguna yang tidak berpengetahuan tinggi, info-info teknik penghirisan dan teknik penyulitan akan dipaparkan untuk membolehkan pengguna mudah memahami dan memilik teknik yang sesuai bagi mereka.

Methodologi Kajian

Bahagian kajian ini akan membincangkan lebih lanjut mengenai keperluan dan reka bentuk sistem aplikasi yang dicadangkan untuk menyelesaikan masalah penyimpanan selamat pada peranti mudah alih seperti yang dibincangkan serta keperluan yang merangkumi definisi keperluan pengguna dan spesifikasi keperluan sistem. Aplikasi yang akan dibangunkan adalah aplikasi mudah alih untuk Penyimpanan Data Sulit dalam Persekitaran Berbilang Awan. Aplikasi ini sangat sesuai untuk individu yang sering menyimpan dokumen kerja, fail sulit, imej dan video peribadi mereka pada peranti mudah alih mereka dan asyik bimbang tentang isu keselamatan. Aplikasi yang dicadangkan adalah penyelesaian yang sesuai untuk pengguna yang mencari penyelesaian keselamatan untuk fail yang disimpan dalam peranti mudah alih dan storan awan.

Model Kitar Hayat adalah metodologi yang konseptual untuk membimbing peringkat 4 pembangunan aplikasi ini iaitu perancangan dan analisis, reka bentuk, pengekodan dan ujian. Model agil dipilih untuk projek ini kerana ia merupakan model yang sudah difahami dan senang untuk menyesuaikan diri dengan perubahan.



Rajah 1: Model Kitaran Hayat Agil

Seperti rajah di atas, Model Kitaran Hayat Agil digunakan di mana projek ini dirancang terlebih dahulu, mereka bentuk antara muka aplikasi, membangunkan aplikasi dengan menambah fungsi dan ciri-ciri aplikasi seperti dinyatakan di dalam objektif kajian dan kemudian menguji aplikasi tersebut dan memastikan tiada apa-apa masalah yang akan dihadapi oleh pengguna. Empat fasa utama model agil adalah seperti berikut:

Fasa Pengumpulan dan Analisis Keperluan

Fasa ini ditumpukan kepada pengenalpastian masalah, pengumpulan maklumat serta keperluan seperti objektif, skop, masalah, dan kekangan yang akan dihadapi. Kajian kesusasteraan diadakan dan sumber lain seperti Internet digunakan untuk mencari maklumat serta melakukan penyelidikan lebih lanjut tentang teknik penghirisan dan proses penyulitan.

Fasa Reka bentuk

Bahagian ini membincangkan keperluan fungsian aplikasi. Keperluan fungsian bertujuan untuk menjadi asas untuk merancang reka bentuk aplikasi. Ia mentakrifkan proses dan aktiviti yang dilakukan oleh aplikasi. Keperluan fungsian ditakrifkan seperti di bawah:

Keperluan Fungsian	Keterangan
Pendaftaran dan Log Masuk Akaun	Aplikasi ini harus membenarkan pengguna mendaftar untuk akaun dan log masuk ke akaun mereka. Butiran dan proses log masuk dikendalikan oleh *Google Firebase.*
Muat Naik Fail	Aplikasi ini harus membolehkan pengguna memuat naik fail jenis dokumen, imej dan video dari peranti mudah alih mereka ke penyimpanan awan. Antara Muka Pengaturcaraan Aplikasi (API) perkhidmatan storan awan digunakan untuk memuat naik data ke *AWS, Google Cloud Service* ,dan *Microsoft Azure Storage.*
Penghirisan Fail	Aplikasi ini harus menghiris fail secara dinamik berdasarkan bilangan kepingan dan cara penghirisan yang ditentukan oleh pengguna iaitu secara menegak, mendatar atau pepenjuru.
Penyulitan Fail	Aplikasi ini patut membolehkan pengguna untuk memilih jenis penyulitan yang sesuai bagi menyulitkan setiap kepingan fail .
Perawakkan Fail	Aplikasi harus memastikan susunan fail dalam storan awan adalah secara rawak dan tidak tersusun.
Muat Turun Fail	Aplikasi ini harus membolehkan pengguna memuat turun fail dari penyimpanan awan berdasarkan kod laluan atau biometrik yang dimasukkan oleh pengguna. Antara Muka Pengaturcaraan Aplikasi (API) perkhidmatan penyimpanan awan digunakan untuk memuat turun data dari *Amazon Web Services, Google Cloud Storage,* dan *Microsoft Azure Storage.*
Penyahsulitan Fail	Aplikasi ini harus menyahsulit hirisan fail yang dimuat turun dari storan awan.
Pembinaan Semula Fail	Aplikasi harus menggabungkan kepingan fail berdasarkan indeks untuk membina semula fail asal.

Memadam Fail	Aplikasi ini harus membolehkan pengguna memadam fail dari penyimpanan awan berdasarkan kod laluan atau biometrik yang dimasukkan oleh pengguna. Antara Muka Pengaturcaraan Aplikasi (API) perkhidmatan penyimpanan awan digunakan untuk memadam data dari *Amazon Web Services, Google Cloud Storage,* dan *Microsoft Azure Storage*.
Log Keluar Akaun	Sistem ini harus membenarkan pengguna log keluar dari akaun.

Jadual 2: Keperluan Fungsian Sistem Aplikasi

Bahagian ini membincangkan keperluan bukan fungsian aplikasi. Keperluan bukan fungsian mentakrifkan sifat dan kekangan aplikasi dan menerangkan tingkah laku aplikasi. Keperluan tidak berfungsi ditakrifkan seperti di bawah:

Keperluan Bukan Fungsian	Keterangan
Kebolehgunaan	Aplikasi ini sepatutnya mudah digunakan. Reka bentuk antara muka aplikasi harus mudah untuk memastikan pengguna tidak mempunyai masalah mengendalikan aplikasi. Frasa dan fungsi dalam aplikasi harus mudah untuk memastikan memudahkan penggunaan.
Ketersediaan	Aplikasi ini harus sentiasa tersedia di hampir semua peranti mudah alih dan aplikasi itu harus diakses di mana sahaja dengan adanya sambungan Internet.
Keselamatan	Aplikasi ini harus menghalang pengguna yang tidak dibenarkan daripada mengakses aplikasi. Aplikasi ini harus memastikan fail hanya boleh dimuat turun dengan kebenaran kod laluan.
Kebolehpercayaan	Aplikasi ini sepatutnya dapat berfungsi tanpa sebarang ralat.

Kecekapan	Aplikasi ini harus berfungsi tanpa memakan masa yang lama dengan adanya sambungan Internet yang baik.

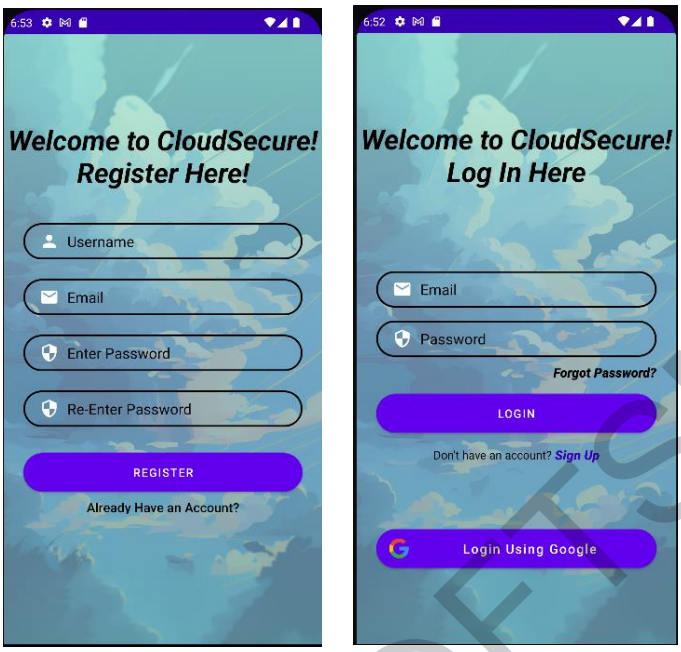
Jadual 2: Keperluan Bukan Fungsian Aplikasi

Bahagian ini membincangkan keperluan keselamatan siber untuk aplikasi ini. Aplikasi yang akan dibangunkan memberi tumpuan kepada aspek keselamatan data, oleh itu prinsip keselamatan data dibincangkan seperti di bawah:

Prinsip	Keterangan
Integriti	Aplikasi ini hendaklah memastikan bahawa data yang disimpan di awan tidak diusik. Penghirisan dan penyulitan fail memastikan kesahihan fail yang disimpan dalam awan.
Kerahsiaan	Aplikasi ini harus memastikan bahawa data tidak diusik oleh pengguna atau orang dalaman yang tidak dibenarkan semasa di awan. Penyulitan fail memastikan kerahsiaan data.
Pengesahan	Aplikasi ini harus memastikan pengguna boleh mengakses aplikasi dan memuat turun fail dengan pengesahan kod laluan.

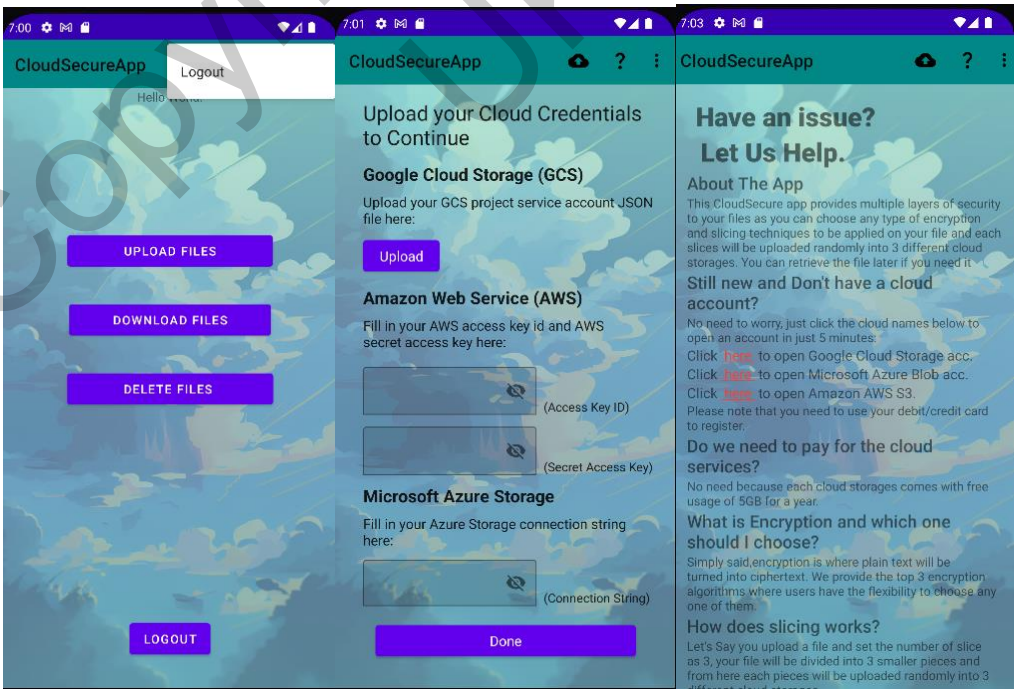
Jadual 3 : Keperluan Keselamatan Siber Aplikasi

Aplikasi ini terdiri daripada antara muka log masuk dan daftar masuk di mana pengguna boleh log masuk ke akaun sedia ada meraka ataupun mendaftar sebagai pengguna baharu. Pengguna juga boleh menggunakan akaun Google untuk mendaftar masuk ke dalam aplikasi.



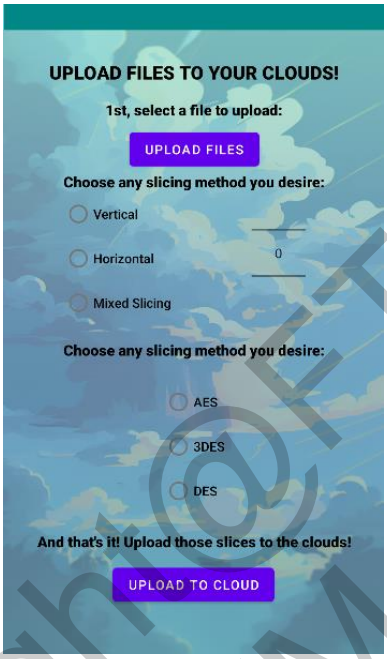
Rajah 2: Rajah Antara Muka Log Masuk,Daftar Masuk & Log Masuk Akaun *Google*

Setelah pengguna log masuk, antara muka utama dipaparkan di mana pengguna boleh memilih untuk memuat naik, memuat turun, atau memadam fail mereka. Mereka juga boleh log keluar akaun mereka, mengetahui lebih lanjut tentang aplikasi ini di halaman *FAQ* dan juga menguruskan butiran akaun mereka di halaman utama.



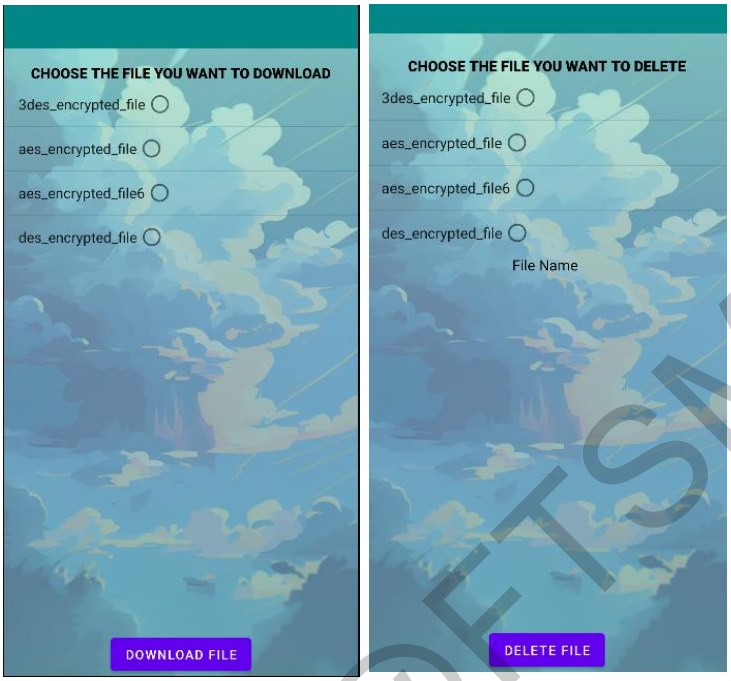
Rajah 3: Rajah Antara Muka Halaman Utama, Urusan Butiran Akaun dan *FAQ'*

Dalam antara muka muat naik fail, pengguna boleh memilih fail yang ingin dimuat naik dari peranti mudah alih mereka. Mereka kemudian mempunyai fleksibiliti untuk memilih jenis hirisan, bilangan hirisan dan teknik penyulitan mengikut kehendak mereka. Seterusnya, mereka boleh klik butang *Upload to Cloud* bagi memuat naik kepingan fail secara rawak ke tiga storan awan berbeza.



Rajah 4: Rajah Antara Muka Muat Naik Fail

Dalam antara muka muat turun fail, pengguna boleh memilih fail untuk dimuat turun daripadasenarai fail yang dimuat naik. Sebaik sahaja pengguna memilih fail, fail diambil dari storan awan. Pengguna kemudian boleh klik butang muat turun untuk menyelesaikan proses muat turun. Dalam antara muka memadam fail, pengguna boleh memilih fail yang ingin mereka padamkandan klik butang padam.



Rajah 5: Rajah Antara Muka Muat Turun dan Memadam Fail

Fasa Pengekodan

Bahagian kajian ini membincangkan pelaksanaan aplikasi berdasarkan keperluan dan spesifikasi reka bentuk yang dicadangkan di bahagian sebelumnya. Fasa pelaksanaan adalah sebahagian daripada metodologi penyelidikan agil di mana tumpuannya adalah pada pembangunan aplikasi menggunakan platform pelaksanaan yang dibincangkan, bahasa pengaturcaraan, dan pelbagai dokumentasi penyimpanan awan untuk mencapai fungsi aplikasi yang dirancang. Selain itu, bahagian ini menerangkan proses pembangunan aplikasi mudah alih untuk Penyimpanan Data Sulit dalam Persekitaran Berbilang Awan yang merangkumi modul, komponen, libraries, dan pangkalan data penting.

Pelaksanaan aplikasi dicapai menggunakan Android Studio yang merupakan persekitaran pembangunan bersepadu yang dioptimumkan secara eksklusif untuk Pembangunan Android. Bahasa yang digunakan untuk pelaksanaan ialah Java. Dokumentasi yang digunakan untuk persekitaran berbilang awan termasuk dokumentasi Firebase untuk Storan Awan Google, Microsoft Azure, dan API Dokumentasi yang digunakan untuk persekitaran berbilang awan termasuk dokumentasi Firebase

untuk Storan Awan Google, Microsoft Azure, dan API Google Drive. Semua kebergantungan dan perpustakaan dilaksanakan menggunakan Gradle berdasarkan dokumentasi yang disediakan di laman web rasmi platform awan. Antara dependencies dan libraries yang penting ialah **amplifyframework:aws-storage-s3, com.google.cloud:google-cloud-storage, firebase-database, firebase-auth, azurestorage-android, drive-api-v3, , com.google.cloud:libraries-bom dan com.android.tools:desugar_jdk_libs.** Semua dependencies dan libraries ini digunakan dalam aplikasi untuk pengesahan pengguna, storan awan untuk muat naik, muat turun dan memadam fail pengguna.

Fasa Pengujian

Objektif ujian untuk aplikasi Penyimpanan Data Sulit dalam Persekitaran Berbilang Awan adalah untuk menguji komponen aplikasi yang penting untuk fungsi utama yang melindungi data pengguna menggunakan teknik seperti penghirisan dan penyulitan. Ujian tahap sistem juga dilakukan berdasarkan aspek fungsi dan tidak berfungsi aplikasi. Jenis ujianyang akan dilakukan untuk ujian berfungsi adalah Ujian Kotak Hitam yang memberi tumpuan kepada fungsi aplikasi manakala untuk aspek tidak berfungsi, Ujian Keselamatan akan dilaksanakan untuk memeriksa sama ada pengesahan, kerahsiaan, dan integriti fail pengguna dicapai. Pelaksanaan ujian dijalankan untuk jenis fail pelbagai saiz. Ujian keselamatan dilakukan secara serentak untuk memeriksa sama ada pengesahan, kerahsiaan, dan integriti fail pengguna dicapai melalui pelaksanaan langkah-langkah keselamatan. Ujian ini dijalankan pada jenis fail dan saiz fail seperti di bawah:

	Saiz Fail			
Jenis Fail	100 KB	500 KB	5 MB	10 MB
Fail Teks (.txt)	✓	✓		
Fail Dokumen (.docx)	✓	✓	✓	
Fail PDF (.pdf)	✓	✓	✓	
Fail PowerPoint (.pptx)	✓	✓	✓	
Fail Imej (.jpg)	✓	✓	✓	

Fail Imej (.png)	✓	✓	✓	
Fail Video (.mp4)		✓	✓	

Jadual 4: Jenis Fail dan saiz Fail yang disulitkan oleh aplikasi

Keputusan dan Perbincangan

Pelaksanaan ujian dijalankan untuk jenis fail pelbagai saiz. Ujian keselamatan dilakukan secara serentak untuk memeriksa sama ada pengesahan, kerahsiaan, dan integriti fail pengguna dicapai melalui pelaksanaan langkah-langkah keselamatan. Ujian Kotak Hitam yang memberi tumpuan kepada fungsi aplikasi dan ujian ini dijalankan pada jenis fail dan saiz fail seperti di bawah:

Kes Ujian	Pelaksanaan Ujian	Keputusan Pelaksanaan	Keputusan kriteria lulus/gagal
Aplikasi ini harus membenarkan pengguna baru mendaftar.	Pengguna baru mendaftar dengan butiran yang diminta.	Pendaftaran berjaya selepas memasukkan kod pengesahan yang betul. Butiran pengguna direkodkan dalam *Firebase Authentication.*	Lulus
Aplikasi ini membenarkan pengguna sedia ada mendaftar masuk.	Pengguna log masuk dengan nama pengguna dan kata laluan berdaftar.	Daftar masuk berjaya untuk pengguna dengan nama pengguna dan kata laluan yang betul. Daftar masuk tidak berjaya dengan nama pengguna atau kata laluan yang salah.	Lulus

Aplikasi harus menyulitkan fail menggunakan algoritma AES.	Fail yang disimpan dalam folder sementara digunakan.	Fail berjaya disulitkan dan disimpan dalam folder sementara dengan sambungan .crypt, dan dalam format tidak boleh dibaca.	Lulus
Aplikasi harus menyulitkan fail menggunakan algoritma 3DES.	Fail yang disimpan dalam folder sementara digunakan.	Fail berjaya disulitkan dan disimpan dalam folder sementara dengan sambungan .crypt, dan dalam format tidak boleh dibaca.	Lulus
Aplikasi harus menyulitkan fail menggunakan algoritma DES.	Fail yang disimpan dalam folder sementara digunakan.	Fail berjaya disulitkan dan disimpan dalam folder sementara dengan sambungan .crypt, dan dalam format tidak boleh dibaca.	Lulus
Aplikasi harus menghiris fail secara mendatar dengan bilangan kepingan yang dipilih oleh pengguna dari senarai juntai.	Fail dimuat naik oleh pengguna dan bilangan kepingan yang dipilih dari senarai juntai adalah 6.	Fail ini berjaya dihiris kepada 6 keping tetapi gagal untuk dimuat naik ke dalam storan awan	Lulus
Aplikasi harus menghiris fail secara menegak dengan bilangan kepingan yang dipilih oleh pengguna dari senarai juntai.	Fail dimuat naik oleh pengguna dan bilangan kepingan yang dipilih dari senarai juntai adalah 6.	Fail ini berjaya dihiris kepada 6 keping tetapi gagal untuk dimuat naik ke dalam storan awan	Lulus

Aplikasi harus menghiris fail secara bercampur (mendatar dan menegak) dengan bilangan kepingan yang dipilih oleh pengguna dari senarai juntai.	Fail dimuat naik oleh pengguna dan bilangan kepingan yang dipilih dari senarai juntai adalah 6.	Fail ini berjaya dihiris kepada 6 keping tetapi gagal untuk dimuat naik ke dalam storan awan	Gagal
Aplikasi ini dapat memuat naik fail yang disulitkan secara rawak ke storan awan.	Fail yang disulitkan disimpan dalam folder sementara dan dimuat naik.	Fail dimuat naik secara rawak dan dimuat naik ke AWS, GCS, dan Azure Blob Storage.	Lulus
Fail yang disimpan dalam storan awan hendaklah dalam kepingan untuk memastikan fail tidak boleh diakses jika storan awan digodam.	Muat naik kepingan fail ke storan awan.	Fail tidak dapat disimpan dalam format kepingan secara rawak dalam AWS, GCS dan Azure Blob Storage.	Lulus
Fail yang disimpan dalam storan awan harus disulitkan untuk memastikan fail tidak dalam format yang boleh dibaca apabila disimpan dalam awan.	Muat naik fail yang disulitkan ke storan awan.	Fail ini dalam format yang tidak boleh dibaca dalam AWS, GCS dan Azure Blob Storage.	Lulus

Aplikasi ini harus meminta kod laluan untuk memuat turun dan memadam fail untuk mengelakkan penceroboh daripada mengakses fail pada peranti.	Fail dari senarai fail yang dimuat naik dipilih untuk dimuat turun. Fail dari senarai fail yang dimuat naik dipilih untuk dipadam.	Fail berjaya dimuat turun menggunakan kod laluan yang betul, dan muat turun gagal dengan butiran yang salah. Fail berjaya dipadamkan apabila menggunakan kod laluan yang betul, dan pemadaman gagal dengan butiran yang salah.	Lulus
Aplikasi ini sepatutnya dapat memuat turun kepingan fail dari storan awan ke aplikasi.	Fail yang dimuat naik dipilih untuk dimuat turun dari senarai.	Kepingan fail yang disulitkan berjaya dimuat turun dari storan awan dan disimpan dalam folder sementara.	Lulus
Aplikasi harus menggabungkan kepingan fail dan membina semula fail.	Kepingan fail yang digabungkan yang disimpan dalam folder sementara digunakan.	Potongan fail gagal digabungkan dan disimpan dalam folder sementara.	Lulus
Aplikasi harus menyahsulit fail yang dimuat turun mengikut sambungan.crypt.	Fail yang disulitkan yang dimuat turun dari storan awan dinyahsulitkan.	Kepingan fail yang disulitkan berjaya dinyahsulit, boleh dibaca dan fail asal disimpan ke peranti dan berada dalam format yang betul dan boleh diakses.	Lulus
Aplikasi ini harus meminta kod laluan atau biometrik untuk memuat turun dan	Fail dari senarai fail yang dimuat naik dipilih untuk dimuat turun.	Fail berjaya dimuat turun menggunakan kod laluan yang betul, dan muat turun gagal dengan	Lulus

memadam fail untuk mengelakkan penceroboh daripada mengakses fail pada peranti.	Fail dari senarai fail yang dimuat naik dipilih untuk dipadam.	butiran yang salah. Fail berjaya dipadamkan apabila kod laluan yang betul, dan pemadaman gagal dengan butiran yang salah.	

Jadual 5.3: Kes Ujian, Pelaksanaan Ujian, Keputusan Pelaksanaan dan Keputusan Kriteria Lulus/Gagal Aplikasi

Semasa fasa pelaksanaan, banyak cabaran dihadapi kerana kekurangan dokumentasi dalam platform awan tertentu untuk pembangunan Android. Aplikasi ini memerlukan butiran projek storan awan pengguna seperti fail JSON untuk mendapatkan Google Cloud Credential, secretkey dan access key untuk AWS dan connection string untuk Azure Storage. Skop projek adalah besar dan terdapat beberapa faktor yang perlu dipertimbangkan seperti kerumitan pengetahuan, dokumentasi kompleks, keselamatan awan dan banyak lagi. Aplikasi ini dilaksanakan menggunakan amalan terbaik berdasarkan penyelidikan dan kajian. Terdapat pengubahsuaian tertentu yang dibuat semasa fasa pelaksanaan berdasarkan dokumentasi yang ada, keutamaan pengguna dan kebimbangan keselamatan. Walaubagaimanapun, terdapat sebahagian kecil pengujian aplikasi ini gagal melaksanakan fungsi penghirisan sepertimana yang dirancang.

Kekangan

Terdapat beberapa batasan aplikasi dan salah satunya termasuk penggunaan minimum penyedia penyimpanan awan. Aplikasi ini memberi tumpuan kepada pembangunan Android yang menghadkan pengguna kepada pengguna Android. Aplikasi ini tidak boleh digunakan oleh pengguna lain seperti pengguna iOS dan Windows. Selain itu, terdapat had saiz fail kerana fail besar mungkin melambatkan proses aplikasi. Penghirisan fail juga mempunyai batas kerana algoritma untuk menghiris fail jenis dokumen dan fail jenis binari (video dan imej) adalah berbeza dan rumit untuk digunakan sewaktu proses penghirisan.

Cadangan Masa Hadapan

Cadangan pertama untuk penambahbaikan masa hadapan adalah menggunakan lebih daripada tiga storan awan untuk meningkatkan keselamatan dan juga memberi fleksibiti kepada pengguna untuk memilih storan awan yang ingin digunakan. Kedua, platform pembangunan yang menggunakan platform pembangunan hibrid seperti Flutter untuk membolehkan skop pengguna yang lebih luas seperti pengguna iOS dan Windows. Selain itu, teknik penyulitan yang digunakan seperti 3DES dan DES adalah berdasarkan sistem warisan dan mungkin tidak dapat digunakan kelak hari nanti. Oleh itu, teknik penyulitan tidak simetri juga boleh menggantikan teknik penyulitan yang lama seperti 3DES dan DES.

Kesimpulan

Bahagian kertas ini membincangkan kesimpulan penyelidikan yang dilakukan pada penyimpanan data sulit untuk peranti mudah alih menggunakan persekitaran berbilang awan. Penyelidikan ini dimulakan dengan mengenal pasti masalah dan kebimbangan keselamatan diikuti dengan pernyataan objektif dan skop projek. Hampir kesemua objektif kajian telah dicapai kecuali penghirisan secara bercampur kerana proses pengekodan tersebut adalah agak sukar untuk dijalankan terhadap fail kerana teknik penghirisan secara menegak dan mendatar adalah dua aspek yang berbeza dan susah untuk menghiris menggunakan kedua-dua teknik tersebut. Langkah-langkah keselamatan dan penyelesaian untuk projek ini ditentukan dengan mengkaji pelaksanaan berdasarkan kertas penyelidikan lain yang dibincangkan dalam kajian kesusasteraan. Kertas ini membincangkan lagi spesifikasi aplikasi yang merangkumi keperluan pengguna dan sistem, keperluan fungsiandan tidak berfungsi, keperluan perkakasan, dan perisian. Reka bentuk aplikasi yang akan dibangunkan dibincangkan dari segi seni bina, dan reka bentuk antara muka aplikasi. Seterusnya, pembangunan dan pengujian aplikasi dibincangkan untuk mengenal pasti segmen kod kritikal dan memastikan aplikasi berfungsi dengan baik tanpa kesilapan.

Penghargaan

Terlebih dahulu, saya ingin mengucapkan ribuan terima kasih kepada penyelia saya iaitu Assoc. Prof. Dr. Elankovan A. Sundararajan kerana sudi memberikan bimbingan dan idea dalam melaksanakan projek ini. Beliau juga sentiasa memberikan galakan dan nasihatdalam proses menambahbaik dan menulis laporan projek serta proses pembangunan aplikasi. Saya juga ingin mengambil kesempatan untuk memberi penghargaan kepada ahli keluarga dan rakan-rakan saya yang sentiasa memberikan motivasi serta dorongan dalam proses melaksanakan projek ini. Terima kasih kepada kawan sekelas saya yang sentiasa memberikan idea dan dorongan kepada saya semasa proses pembangunan aplikasi. Akhir sekali, saya amat bersyukur kepada Tuhan kerana mengurniakan saya kesihatan dan kekuatan untuk menyiapkan projek tahun akhir ini dengan baik tanpa halangan.

RUJUKAN

10.1: Room, LiveData, and ViewModel · GitBook, Google-developer-training.github.io, https://google-developer-training.github.io/android-developer-fundamentals-course-concepts- v2/unit-4-saving-user-data/lesson-10-storing-data-with-room/10-1-c-room-livedata-viewmodel/10-1-c-room-livedata-viewmodel.html [9 DISEMBER 2022]

7 Kegunaan Umum Pengkomputeran awan. AXO Technologies. https://axotechnologies.com/7-kegunaan-umum-pengkomputeran-awan/ [NOVEMBER 12, 2022]

Alatalo, P., Järvenoja, J., Karvonen, J., Keronen, A., & Kuvaja, P. (2002, December). Mobile application architectures. In International Conference on Product Focused Software Process Improvement (pp. 572-586).

Avinesh Leo a/l Adrian Fernandez. 2021. Perlindungan Storan Melalui Berbilang Awan Dengan Penghirisan Data. FTSM. Universiti Kebangsaan Malaysia.

Balasaraswathi V.R. & Manikandan.S. 2014. Enhanced Security for Multi-Cloud Storage using Cryptographic Data Splitting with Dynamic Approach. IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT): 1190 – 1194. DOI: 10.1109/ICACCCT.2014.7019286.

Cryptography - Data Encryption Standard (DES) | C# Corner. https://www.c-sharpcorner.com/article/cryptography-data-encryption-standard-des/ [NOVEMBER 30, 2022]

Get started with Cloud Storage on Android | Firebase Documentation, Google https://firebase.google.com/docs/storage/android/start [DECEMBER 15, 2022]

Hardik, & Santhosh K. (2022). AWS vs azure vs google cloud - detailed cloud comparison. Intellipaat Blog https://intellipaat.com/blog/aws-vs-azure-vs-google-cloud/ [DECEMBER 5, 2022]

IBM Education, What is Three-Tier Architecture, dari https://www.ibm.com/cloud/learn/three-tier-architecture [6 DISEMBER 2022]

K. Subramanian & F. Leo John. 2017. Dynamic and secure unstructured data sharing in multi-cloud storage using the hybrid crypto-system. International Journal of Advanced and Applied Sciences ,5(1): 15-23. DOI: 10.21833/ijaas.2018.01.003

Kareesma A/P P.Nageswaran. 2021. Penyimpanan Data Sulit Dalam Persekitaran Berbilang Awan. FTSM. Universiti Kebangsaan Malaysia.

Larson, M. (n.d.). What are the differences between DES and AES encryption? What are the Differences Between DES and AES Encryption? https://info.townsendsecurity.com/bid/72450/what-are-the-differences-between-des-and-aes-encryption [DECEMBER 5, 2022]

Manoj V. Bramhe, Milind V. Sarode & Meenakshi S. Arya. 2019. Multi-Cloud Secure Data storage using Cryptographic Techniques. International Journal of Research in Advent Technology, Vol.7, No.1: 484 - 487.

Mobile Device Security in the Workplace: 5 Key Risks and a Surprising Challenge, EDGE Sirius https://edge.siriuscom.com/security/mobile-device-security-in-the-workplace-5-key- risks-and-a-surprising-challenge/ [DECEMBER 18, 2022]

Mobile Device Security in the Workplace: 5 Key Risks and a Surprising Challenge, EDGE Sirius, https://edge.siriuscom.com/security/mobile-device-security-in-the-workplace-5-key-risks-and-a-surprising-challenge [17 NOVEMBER 2022]

Noh, M. bte M. Teknologi cloud computing. Catatan Tugas. Dari http://catatantugasan.blogspot.com/2013/02/teknologi-cloud- computing.html [NOVEMBER 12, 2022]

Nonfunctional Requirements, Scaled Agile Framework https://www.scaledagileframework.com/nonfunctional-requirements/ [10 JANUARI 2023]

Online Mockup, Wireframe & UI Prototyping Tool · Moqups https://moqups.com/ [10 Januari 2023]

Peng Xu, Xiaqi Liu, Zhenguo Sheng, Xuan Shan & Kai Shuang. 2015. SSDS-MC: Slice- based Secure Data Storage in Multi-Cloud Environment. 11th EAI International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (QSHINE) : 304 - 309. DOI: 10.410S/eai.19-S-2015.2260679.

Rupesh R Bobde, Amit Khaparde & M.M.Raghuwanshi. 2015. Combined Use Of Encryption Algorithm & Data Slicing Technique For Securing Data On Cloud. IEEE Sponsored 2nd International Conference on Innovations in Information, Embedded and Communication systems (ICIIECS).

Save data in a local database using Room | Android Developers, https://developer.android.com/training/data-storage/room[9 Disember 2022]

Singh, V. (2022). 10 benefits of cloud storage. Cloud Academy. https://cloudacademy.com/blog/10-benefits-of-using-cloud-storage/ [December 5, 2022]

Uses SDK, Android Developers, https://developer.android.com/guide/topics/manifest/uses-sdk-element#ApiLevels [17 Disember 2022]

What is Data Encryption? Forcepoint. (2021, October 28). https://www.forcepoint.com/cyber-edu/data-encryption [12 November 2022]

Dineswaran A/L Navarasan (A180763)
Assoc. Prof. Dr. Elankovan A. Sundararajan
Fakulti Teknologi & Sains Maklumat,
Universiti Kebangsaan Malaysia