

# Penyimpanan Data Sulit dalam Persekitaran Berbilang Awan

## *Securing Data Storage on a Multi-cloud Environment*

Dineswaran Navarasan  
<sup>1</sup>Elankovan A. Sundararajan

Program Sains Komputer  
Fakulti Teknologi dan Sains Maklumat  
Universiti Kebangsaan Malaysia

Correspondence e-mail: <sup>1</sup>elan@ukm.edu.my

### ABSTRAK

*Pengkomputeran awan telah berkembang selama bertahun-tahun untuk mengatasi kekangan pengiraan dan penyimpanan peranti mudah alih. Kekangan storan boleh diatasi melalui storan awan dengan ketersediaan sambungan internet. 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 penyalahgunaan 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 fail disulitkan, fail akan dihiris kepada segmen-segmen kecil di mana ia 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 penyalahgunaan 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, Perawakkan, Berbilang Awan, Penyimpanan Data Sulit*

### ABSTRACT

Cloud computing has been growing over the years to overcome compute and storage constraints of mobile devices. Storage constraints can be addressed through cloud storage with the availability of internet connections. Although cloud computing has its benefits, security concerns about user data are still present. Data stored on the cloud are transmitted over the Internet which users have no control and are susceptible to data breaches caused by malware or insider attacks. This study aims to ensure data security in multiple public clouds with various encryption types, slicing techniques and some guidance provided for users. The proposed application encrypts the data where multiple encryption algorithms will be provided plus it also gives users to choose which type of slicing technique to use. After slicing, various segments will be created where each segment will undergo randomization process and are uploaded randomly on multiple different cloud storages. Users who are still new to the digital world will be provided with some information and a brief explanation on what encryptions

are and how slicing techniques work on their data. The security measures implemented will prevent data breaches on the cloud even if the respective cloud account is hacked. It also gives users the freedom to choose the type of encryption and slicing techniques to be applied on their private files, giving more layers of security to prevent their data from being stolen or lost.

**Keywords:** *Encryption, Slicing, Randomization, Multi-Cloud, Secure Data Storage*

## 1. 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 menawarkan pelbagai perkhidmatan kepada pengguna di mana data boleh disimpan di dalam storan awan serta dapat mengaksesnya dari mana-mana lokasi. 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.

Untuk menangani masalah ini, aplikasi yang menyediakan teknik penghirisan secara dinamik telah dibina dan segmen fail akan dimuat naik ke dalam dua storan awan berbeza (Avinesh Leo, 2021). Seterusnya, aplikasi tersebut diubah suai bagi menyediakan teknik penghirisan dan juga penyulitan serta memuat naik segmen fail ke dalam tiga storan awan yang berbeza (Kareesma, 2021). 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, jenis penghirisan dan cara penggunaan storan awan dalam aplikasi tersebut.

Untuk menangani masalah tersebut, tiga objektif digariskan iaitu membangunkan aplikasi yang dapat menyediakan tiga jenis penghirisan yang berbeza, menyediakan tiga jenis teknik penyulitan yang berbeza serta pengguna yang masih baru dalam dunia digital akan dibekalkan dengan maklumat dan info ringkas tentang penyulitan, teknik penghirisan dan cara menyimpan data di dalam storan awan. Langkah keselamatan yang dilaksanakan akan menghalang pelanggaran data pada awan walaupun salah satu akaun awan digodam. 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 11 dan ke atas.

## 2. Tinjauan Literatur

### 2.1 Pendahuluan

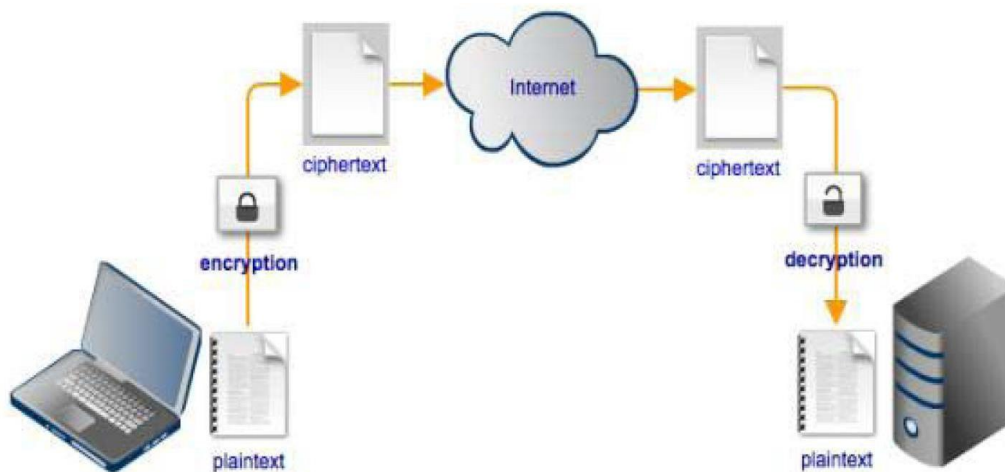
Kajian kesusasteraan membincangkan langkah-langkah keselamatan untuk penyimpanan data yang selamat dalam persekitaran berbilang awan. Perbincangan ini merangkumi analisis pelbagai teknik yang digunakan dan perbandingan antara teknik untuk menentukan penyelesaian terbaik. Pengkomputeran awan sememangnya telah mengubah dunia dari segi penyimpanan data dan kuasa pengkomputeran. Penggunaan storan awan bukan sahaja terhad kepada organisasi besar tetapi juga boleh digunakan oleh mana-mana individu. Storannya menawarkan banyak kelebihan seperti penjimatan kos, skalabiliti, kebolehcapaian dan perkhidmatan keselamatan (Singh, V).

## 2.2 Latar Belakang

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 awan yang mampu mengusik dan mengganggu data dengan niat yang tidak baik (rogue employee) dan potensi kebocoran data semasa dalam transit ke pusat data.

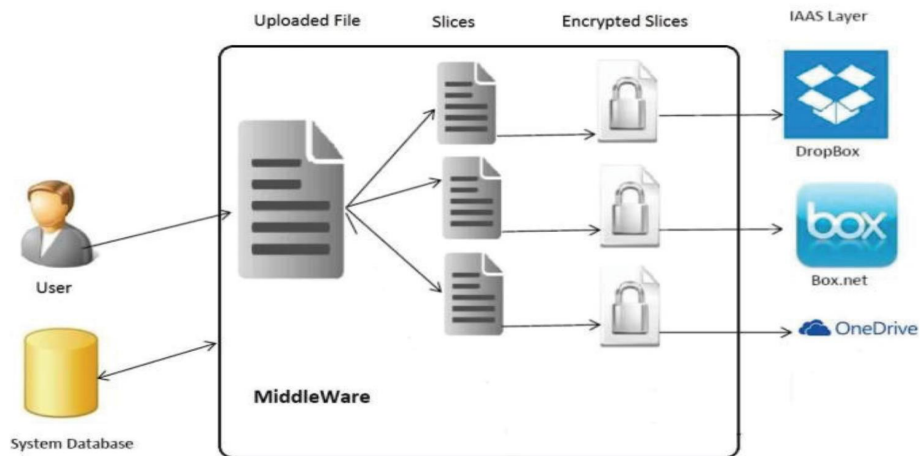
## 2.3 Perbandingan dan Perbezaan

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.



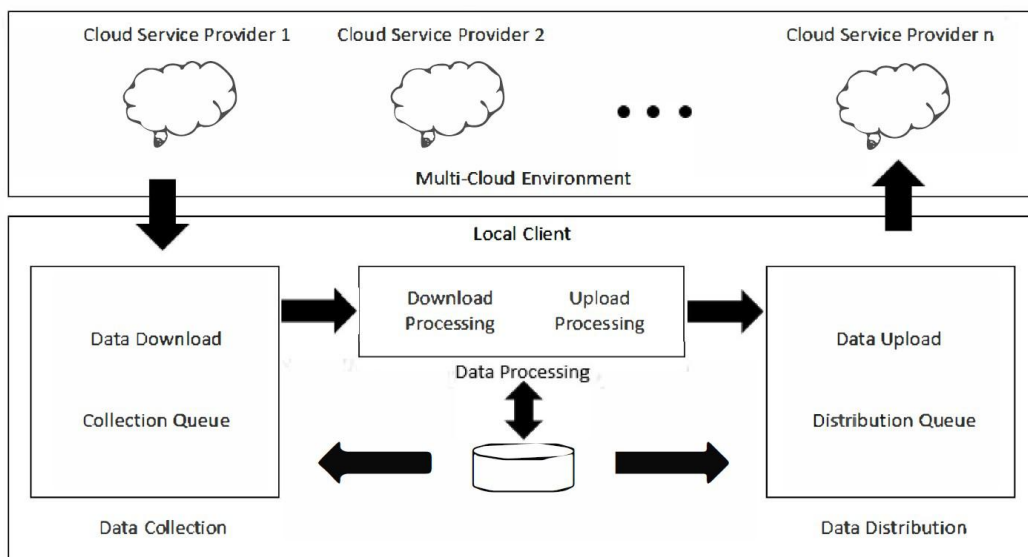
RAJAH 2.1. Seni Bina Teknik Penyulitan

2. Sandeep Nehe et al. (2015) memberi cadangan sebuah kerangka perisian tengah yang mengesahkan pengguna, membahagikan fail kepada beberapa kepingan, menyulitkan kepingan fail tersebut, dan memuat naik setiap kepingan ke storan awan yang berlainan. Kerangka ini mempunyai tiga peringkat seni bina iaitu Pengguna, Lapisan IaaS (Infrastructure-as-a-Service), dan Perisian Tengah Sistem. Semua perkhidmatan awan yang digunakan iaitu DropBox, Box.net dan OneDrive merupakan Lapisan IaaS. Perisian tengah inilah yang menghubungkan semua komponen kerangka. Perisian ini dihoskan dalam awan persendirian untuk mendapat 10 kawalan penuh atas segala pengurusan keselamatan. Perisian tengah ini membahagikan data kepada tiga segmen yang mempunyai saiz sama. Proses penyulitan data juga berlaku pada peringkat ini menggunakan algoritma AES. Proses muat naik dan turun data dilaksanakan dengan API setiap perkhidmatan awan masing-masing.



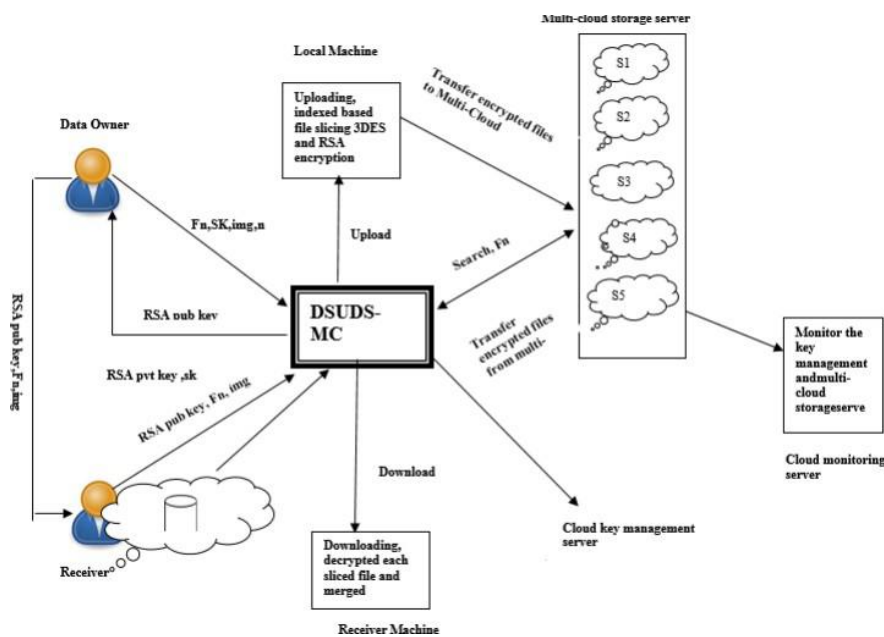
RAJAH 2.2. Kerangka 3 Lapisan Perisian Pertengahan

3. Peng Xul et al. (2015) mencadangkan sebuah model SSDS-MC: Slice-based Secure Data Storage in Multi-Cloud Environment. Model ini berfungsi menghiris data kepada beberapa kepingan selepas disulitkan dan dimuat naik secara berasingan ke storan awan yang berlainan masing-masing. Reka bentuk model ini menunjukkan empat komponen utama yang membahagikan fungsi masing-masing. Komponen-komponen tersebut ialah Data Processing (DP), Data Distribution (DD), Data Collection (DC) and Metadata Table (MT). Komponen pertama, DP, mempunyai dua fungsi iaitu menyulitkan dan menghiris data sebelum memuat naik, dan membina semula dan menyahsulit data selepas dimuat turun. Proses memuat naik data kepada setiap awan yang berbeza dikendalikan oleh komponen seterusnya iaitu DD. DC pula bertanggungjawab memuat turun kepingan data dari awan-awan berdasarkan rekod dalam MT. Beberapa sandaran (backups) juga disediakan sekiranya mana-mana storan awam mengalami gangguan perkhidmatan. Akhirnya, MT menyimpan rekod lokasi setiap kepingan data.



RAJAH 2.3. Seni Bina SSDS-MC

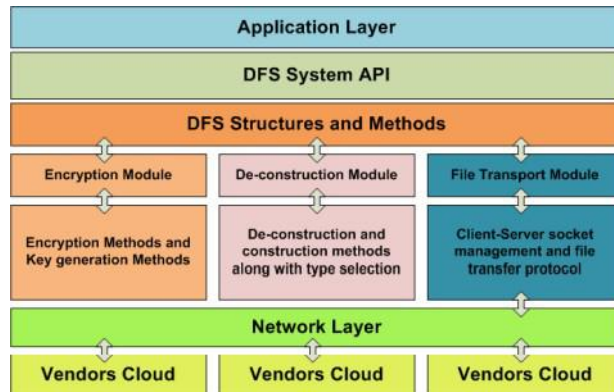
4. K. Subramanian et al. (2018) mencadangkan perkongsian data yang dinamik dan selamat dalam storan multi-cloud (DSUDS-MC) menggunakan sistem kriptu hibrid. Rangka kerja DSUDS-MC berfungsi sebagai perisian tengah atau API web untuk menyambung ke pelayan berbilang awan. Rangka kerja ini terdiri daripada beberapa tugas. Pertama, pemilik data memuat naik fail termasuk maklumat seperti bilangan hirisan untuk fail, kunci peribadi dan imej melalui antara muka rangka kerja. Sebaik sahaja fail dimuat naik, fail dihiris berdasarkan input nombor oleh pemilik data dan disulitkan menggunakan algoritma 3DES sebelum diedarkan ke storan berbilang awan. Kekunci rahsia juga disulitkan menggunakan algoritma RSA. Proses muat turun fail oleh penerima adalah proses terbalik di mana kelayakan yang diperlukan untuk mencapai fail diberikan oleh pemilik data. Setelah pengesahan berjaya, fail akan didapatkan semula, dinyahsulitkan dan dicantumkan. Pendekatan ini menggunakan penghirisan dinamik yang meningkatkan kepercayaan dan memastikan serangan orang dalaman dan serangan hasad terhadap fail tidak berlaku.



RAJAH 2.4. Seni Bina DSUDS-MC

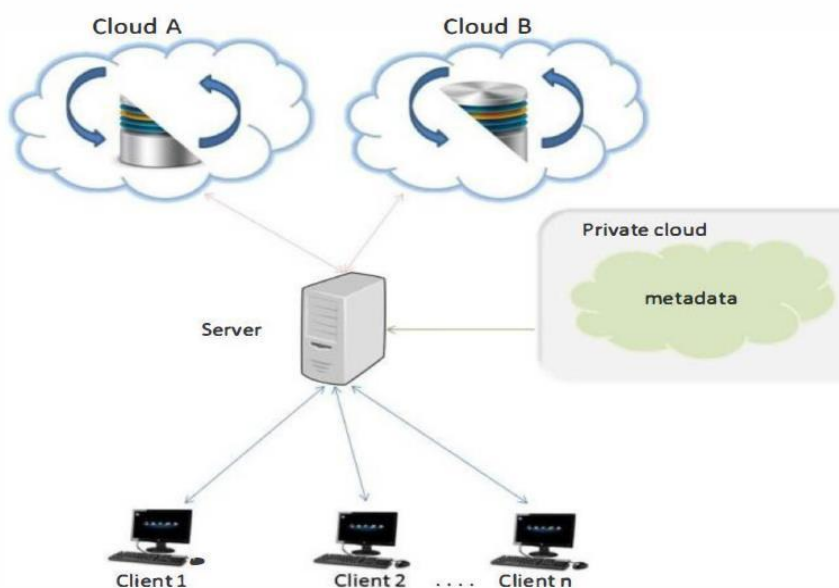
5. Berdasarkan Manoj V. Bramhe et al. (2019), penyimpanan data sulit pada pelbagai awan boleh dicapai dengan menggunakan teknik kriptografi. Sistem yang dicadangkan terdiri daripada beberapa modul termasuk pendaftaran dan log masuk, tetapan FTP, muat naik dan muat turun, penyulitan dan penyahsulitan 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.



RAJAH 2.5. Seni Bina Sistem Penyimpanan Keselamatan Berbilang Awan

6. Balasaraswathi V.R. et al. (2014) mencadangkan seni bina yang terdiri daripada empat komponen iaitu: server yang berfungsi melaksanakan proses penghirisan dan penyulitan, dua perkhidmatan storan awan yang masing-masing menyimpan separuh daripada kepingan sesebuah fail, dan satu lagi perkhidmatan awan ketiga yang berperanan menyimpan maklumat metadata fail. Menurut kajian yang dijalankan, fail tidak berstruktur seperti gambar, video dan dokumen teks tidak dapat dihiris dengan sewenang-wenangnya. Namun, dengan penggunaan kaedah kriptografi, penghirisan data dapat dilakukan atas fail tidak berstruktur tersebut. Kaedah penghirisan ini juga membolehkan fail dihiris secara dinamik dan merupakan meningkatkan keselamatan integriti data. Proses penyulitan dilaksanakan dalam pelayan tempatan (local server). Kepingan fail melalui proses penyulitan AES dengan saiz kunci 256 bit yang disimpan dalam storan awan ketiga. Kaedah penyulitan AES dipilih atas sebab kepantasan pemprosesan. Cadangan penambahbaikan penyelidikan adalah seperti penambahan teknologi perlindungan salinan data di storan awan. Dengan ini, menjadikannya sukar untuk penceroboh menemui lokasi kepingan fail di storan awan yang diperlukan untuk membina semula fail.



RAJAH 2.6. Seni Bina Penyimpanan Berbilang Awan Khas

Berdasarkan kajian yang dilakukan, terdapat pelbagai pendekatan keselamatan yang digunakan untuk memastikan data yang dimuat naik adalah selamat dan tidak mudah dicerobohi oleh penggodam.

Pendekatan pertama adalah penggunaan teknik penghirisan yang berbeza iaitu secara menegak, mendatar dan bercampur untuk menghiris data kepada 3 kepingan dan diikuti dengan 3 teknik penyulitan yang berbeza. Namun demikian, pendekatan ini hanya menggunakan satu perkhidmatan storan awan sahaja untuk menyimpan ketiga-tiga kepingan data tersebut. Pendekatan kedua pula menggunakan 3 storan awan yang berbeza untuk menyimpan kepingan data yang dihiris dan disulitkan. Algoritma penyulitan simetri yang telah digunakan adalah AES bagi kesemua kepingan data yang dihiris. Pendekatan ketiga juga menggunakan teknik penyulitan AES dan teknik penghirisan yang sama untuk menyimpan data di dalam persekitaran awan berbilang tetapi tidak sesuai untuk fail-fail yang besar. Pendekatan keempat menggunakan teknik penghirisan dinamik serta menggunakan teknik penyulitan AES untuk menyediakan tahap keselamatan yang tinggi. Kunci peribadi yang digunakan akan disulitkan menggunakan algoritma RSA untuk meningkatkan tahap keselamatan. Pendekatan kelima adalah menggunakan FTP untuk berkomunikasi dengan perkhidmatan storan awan. Sebanyak tiga storan awan digunakan di mana satu storan awan adalah pelayan tempatan manakala dua lagi akan disimpan dalam pelayan awan. Pendekatan keenam menggunakan dua storan awan yang berbeza untuk menyimpan kepingan data dan satu awan peribadi untuk menyimpan metadata. Storannya memudahkan proses pengambilan dan penggabungan fail tetapi mungkin boleh dikompromi. Pendekatan-pendekatan yang dicadangkan ini dapat membantu meningkatkan ciri-ciri keselamatan berdasarkan pendekatan akhir.

### **3. Metodologi dan Kawasan Kajian**

#### **3.1 Pengenalan**

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. Bahagian ini akan membincangkan keperluan sistem merangkumi definisi keperluan pengguna serta spesifikasi keperluan sistem yang mengandungi keperluan fungsian dan bukan fungsian sistem tersebut. Model sistem aplikasi juga akan dibincangkan. Model berorientasikan objek telah dipilih untuk model sistem yang akan membincangkan penggunaan gambar rajah kes guna dan gambar rajah aktiviti untuk menunjukkan aliran urutan aplikasi.

#### **3.2 Definisi Keperluan Pengguna**

Bahagian ini membincangkan keperluan fungsian pengguna aplikasi. Pengguna sistem ini adalah individu yang ingin menyimpan data mereka dalam peranti mudah alih di awan dengan cara yang selamat. Aplikasi yang dicadangkan membolehkan pengguna menyimpan fail mereka dalam storan awan dengan langkah-langkah keselamatan. Keperluan fungsi pengguna adalah seperti di bawah:

Keperluan Pengguna	Keterangan
Pendaftaran dan Log Masuk Akaun	Aplikasi ini harus membenarkan pengguna baru mendaftar untuk akaun dan membenarkan pengguna sedia ada log masuk ke akaun mereka menggunakan butiran akaun.
Muat Naik Fail	Aplikasi ini harus membolehkan pengguna memuat naik fail dari peranti mudah alih ke dalam storan awan. Aplikasi ini juga harus membenarkan pengguna memilih bilangan kepingan yang akan digunakan untuk penghirisan fail secara dinamik.
Muat Turun Fail	Aplikasi ini harus membolehkan pengguna memuat turun fail dari storan awan. Aplikasi ini harus meminta kod laluan atau biometrik untuk membenarkan muat turun fail.
Memadam Fail	Aplikasi ini harus membenarkan pengguna untuk memadam fail dari storan awan. Aplikasi ini harus meminta kod laluan atau biometrik untuk membenarkan memadam fail.
Log Keluar Akaun	Aplikasi ini harus membenarkan pengguna log keluar dari akaun selepas tempoh tidak aktif yang diberikan.

JADUAL 3.1. Keperluan Fungsian Pengguna Aplikasi

### 3.3 Spesifikasi Keperluan Sistem

#### 3.3.1 Keperluan Fungsian

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 <i>AWS Amplify Auth</i> .
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 <i>AWS</i> , <i>Google Cloud Service</i> , dan <i>Microsoft Azure Storage</i> .
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 <i>Amazon Web Services</i> , <i>Google Cloud Storage</i> , dan <i>Microsoft Azure Storage</i> .
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 <i>Amazon Web Services</i> , <i>Google Cloud Storage</i> , dan <i>Microsoft Azure Storage</i> .
Log Keluar Akaun	Sistem ini harus membenarkan pengguna log keluar dari akaun.

JADUAL 3.2. Keperluan Fungsian Sistem Aplikasi

### 3.3.2 Keperluan Bukan Fungsian

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
Kebolegunaan	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 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 atau biometrik.
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 3.3. Keperluan Bukan Fungsian Aplikasi

### 3.3.3 Spesifikasi Keperluan Perkakasan dan Perisian

Bahagian ini membincangkan keperluan perkakasan dan perisian untuk pembangun aplikasi untuk membangunkan aplikasi dan penggunaan untuk pengguna aplikasi.

Keperluan perkakasan diperlukan untuk memastikan proses yang lancar semasa pembangunan dan pengaturcaraan. Keperluan Perkakasan Pembangunan adalah seperti berikut:

- Operasi Microsoft Windows 8 dan ke atas (64-bit)
- Pemproses Intel Core i5 atau ke atas
- 8GB RAM atau ke atas
- Rangkaian Internet kelajuan 10Mbps dan ke atas

Keperluan perisian adalah perlu untuk memastikan alat perisian yang betul digunakan untuk mencapai matlamat pembangunan. Keperluan Perisian Pembangunan adalah seperti berikut:

- Java JDK 17
- Android Studio

- Android SDK
- Google Firebase Realtime Database digunakan untuk menyimpan data mengenai butiran fail yang dimuat naik ke persekitaran berbilang awan dan Google Authentication digunakan untuk simpan maklumat pengguna.
- Penggunaan Amplify Auth untuk kebenaran dan pengesahan permohonan aplikasi.
- API Google Cloud Storage(GCS)
- API Microsoft Azure Storage
- API AWS Storage (AWS S3)

Semua API storan awan membolehkan menyimpan dan menguruskan kandungan yang dijana pengguna seperti foto, video, dan fail dengan selamat di dalam awan.

Keperluan Penggunaan Pengguna:

- Peranti Android dengan OS Android 11.0 dan ke atas
- Rangkaian Internet dengan kelajuan 10Mbps dan ke atas

Penggunaan API memerlukan pengguna untuk mempunyai peranti dengan Android 11.0 dan ke atas. Penggunaan versi Android di bawah 11.0 tidak serasi dengan API dan versi SDK untuk aplikasi berfungsi.

### 3.3.4 Keperluan Keselamatan Siber

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 diakses oleh pengguna 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 atau biometrik.

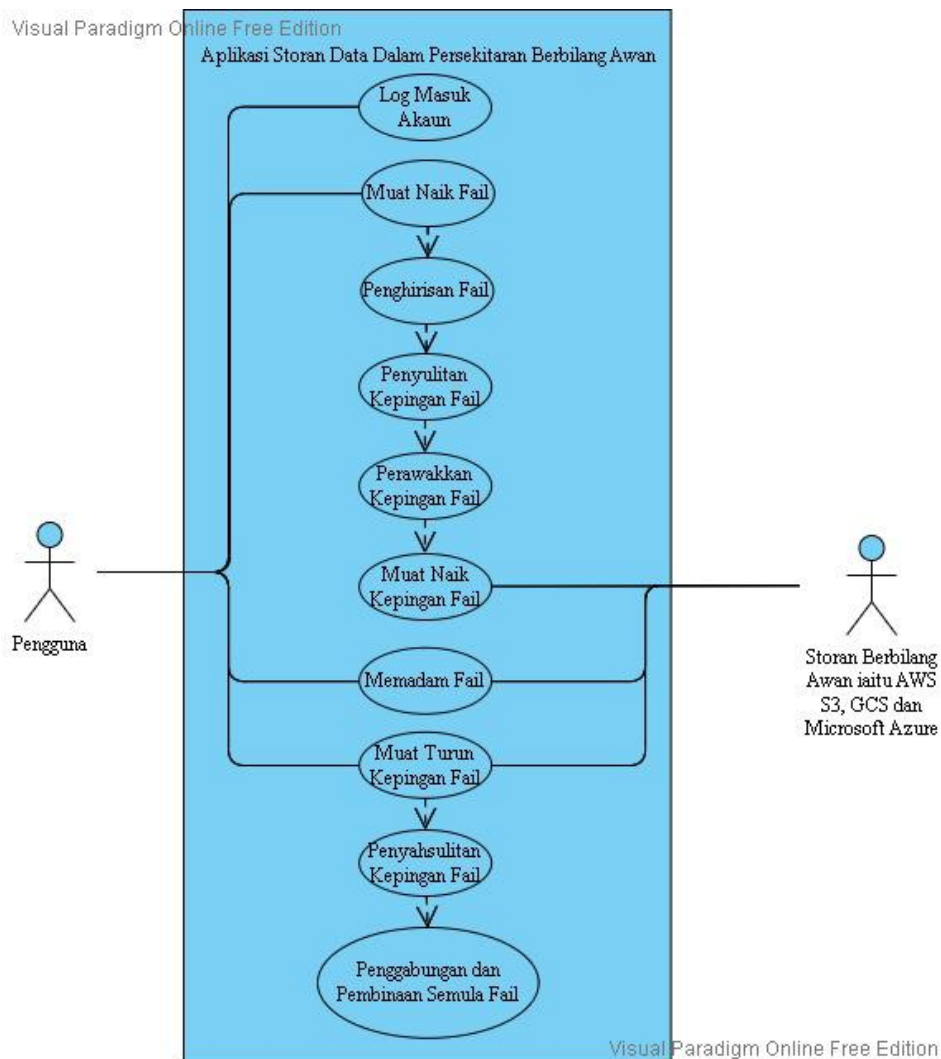
JADUAL 3.4. Keperluan Keselamatan Siber Aplikasi

Storan awan masing-masing mempunyai aspek keselamatan mereka sendiri untuk memastikan keselamatan data pengguna semasa berada di platform awan. AWS memberikan fleksibiliti dalam menentukan ciri keselamatan untuk storan Amazon S3. Semua sumber S3 bersifat peribadi dan hanya boleh diakses oleh pemilik sumber atau pentadbir akaun apabila ia dicipta. Kelas storan S3 Standard direka untuk ketersediaan 99.99%. Google Cloud juga membolehkan penyimpanan dan pengambilan data pada bila-bila masa dengan ketersediaan kira-kira 99.9%. Dengan Storannya Awan Google, data dilindungi oleh salah satu rangkaian peribadi terbesar di dunia, meminimumkan pendedahan kepada internet awam. Dasar dan ciri keselamatan dalam storan awan ini juga memastikan keselamatan data yang disimpan dalam awan.

### 3.4 Model Sistem

#### 3.4.1 Gambar Rajah Kes Guna

Gambar rajah kes guna adalah alat untuk pemodelan sistem aplikasi atau subsistem. Gambar rajah kes guna menggambarkan keupayaan khusus sistem. Gambar rajah 3.1 menunjukkan gambar rajah kes penggunaan untuk aplikasi Storan Data Sulit dalam Persekitaran Berbilang Awan.



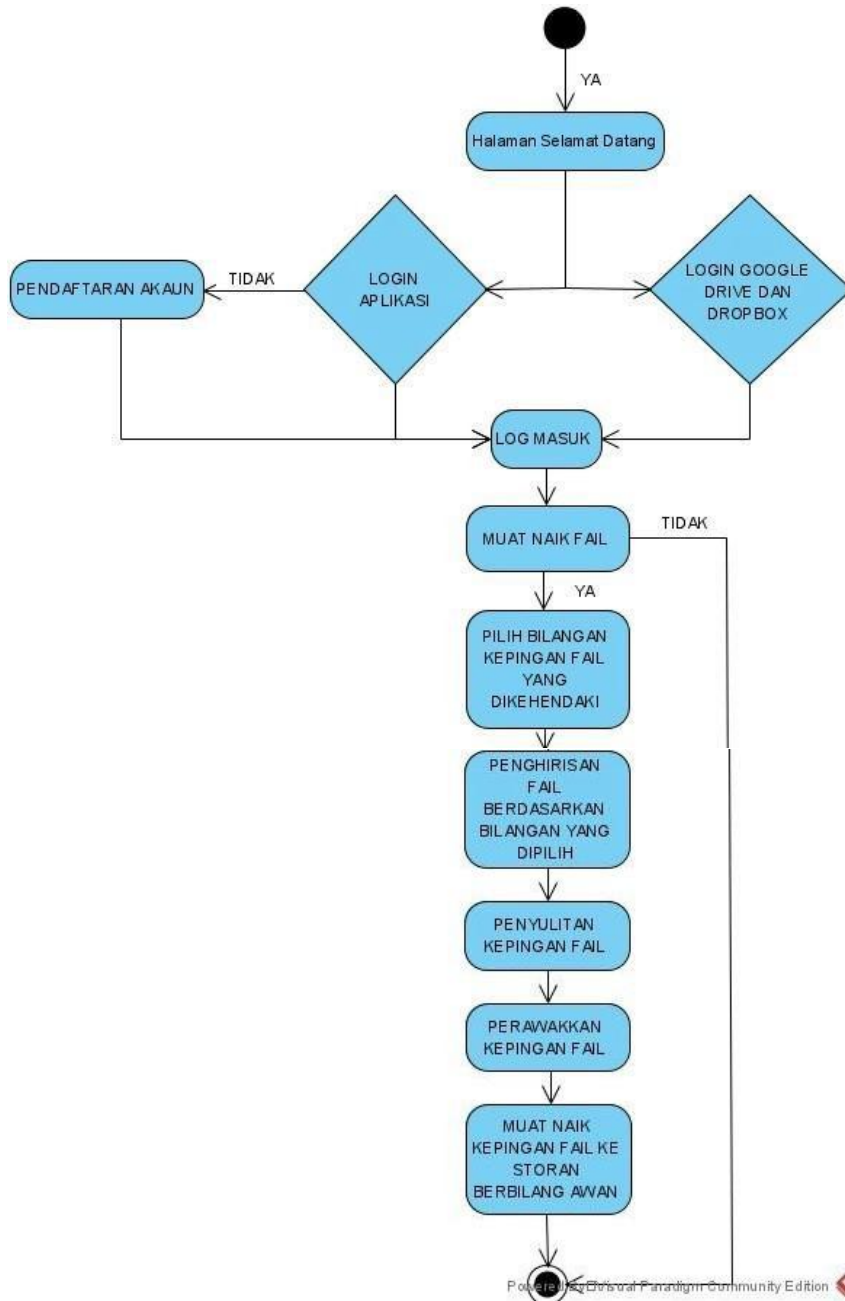
RAJAH 3.1. Rajah Kes Guna Aplikasi

#### 3.4.2. Gambar Rajah Aktiviti

Gambar rajah aktiviti ialah carta aliran yang menggambarkan pergerakan maklumat daripada satu tindakan ke tindakan seterusnya. Tindakan boleh digambarkan sebagai operasi sistem. Ia menggambarkan tingkah laku dinamik sistem. Gambar rajah berikut menunjukkan gambar rajah aktiviti untuk aplikasi Storan Data Sulit dalam Persekitaran Berbilang Awan.

Gambar rajah 3.2 menunjukkan aktiviti proses muat naik. Proses ini bermula dengan pengguna log masuk ke aplikasi untuk memuat naik fail mereka. Sekiranya pengguna tidak

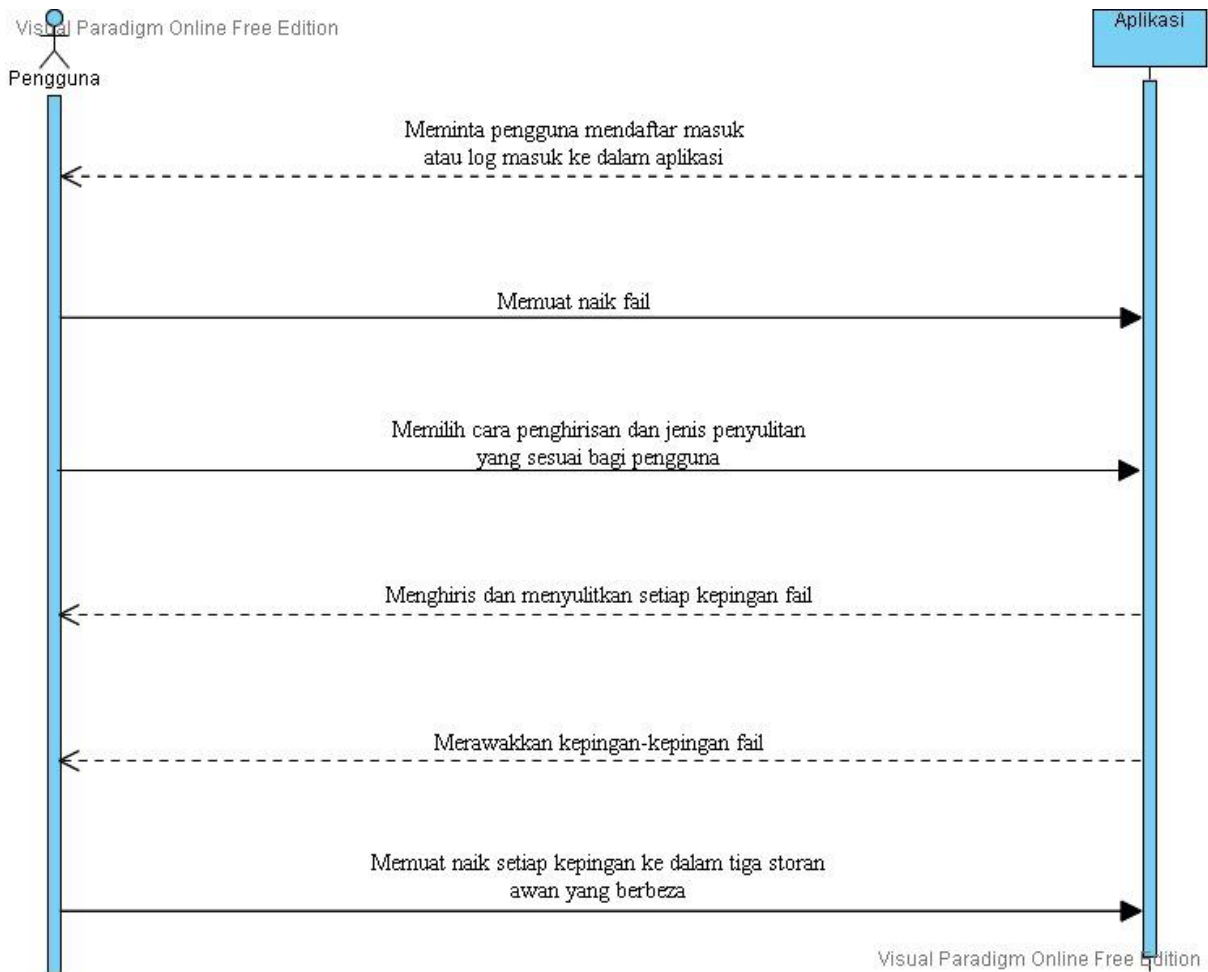
didaftarkan, aplikasi ini memerlukan pengguna mendaftarkan akaun terlebih dahulu. Pengguna kemudian boleh memuat naik fail mereka dan menentukan bilangan kepingan yang dikehendaki untuk penghirisan fail. Aplikasi itu kemudian akan menghiris fail berdasarkan input pengguna, menyulitkan setiap kepingan, merawakkan kepingan dan memuat naiknya ke storan awan.



RAJAH 3.2. Gambar Rajah Aktiviti Muat Naik Fail Aplikasi

### 3.4.3 Gambar Rajah Jujukan

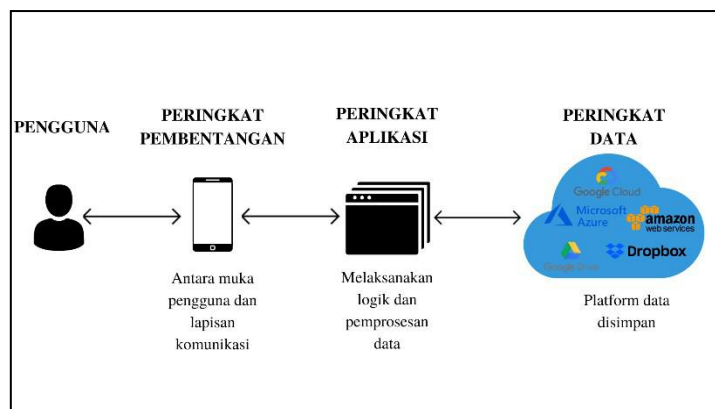
Rajah jujukan ialah rajah yang menggambarkan urutan mesej antara objek dalam interaksi. Gambar rajah jujukan terdiri daripada sekumpulan objek yang diwakili oleh talian hayat, dan pertukaran mesej berlaku antara pengguna dengan aplikasi yang dari semasa ke semasa sewaktu interaksi.



RAJAH 3.3. Gambar Rajah Jujukan Memuat Naik Fail Aplikasi

#### 4. Reka Bentuk Seni Bina

Reka bentuk seni bina yang akan digunakan untuk membangunkan aplikasi ini adalah seni bina tiga peringkat (seni bina berlapis). Tiga peringkat terdiri daripada peringkat persembahan, peringkat aplikasi, dan peringkat data. Kelebihan seni bina ini adalah setiap peringkat mempunyai keperibadian sendiri dan terpisah daripada peringkat yang lain.

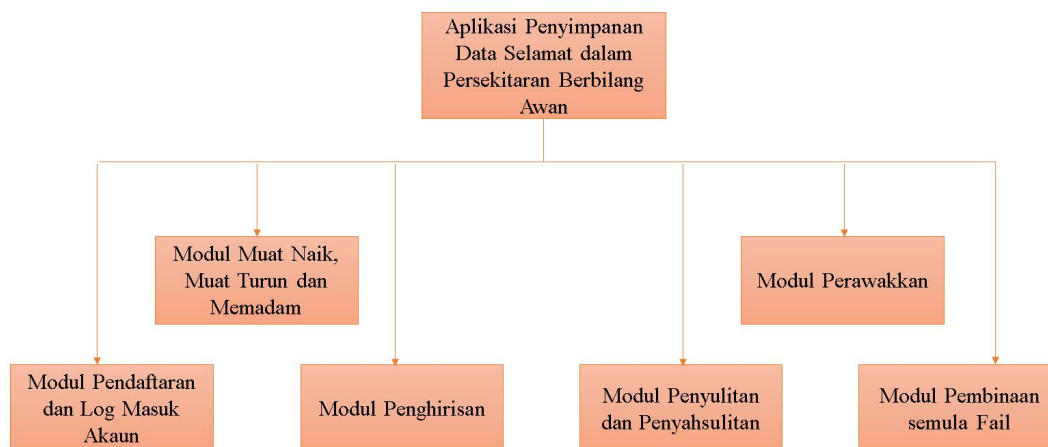


RAJAH 4.1. Reka Bentuk Seni Bina Tiga Peringkat Aplikasi

Peringkat pembentangan aplikasi akan membolehkan pengguna berinteraksi dengan antara muka pengguna yang akan menyediakan fungsi untuk mendaftar / log masuk, memuat naik fail dan memuat turun fail. Pengguna boleh berinteraksi dengan unsur seperti butang untuk memilih dan kotak teks untuk mengisi maklumat yang diperlukan. Peringkat aplikasi akan melaksanakan operasi pada data yang memenuhi fungsi dan matlamat aplikasi. Peringkat ini bertanggungjawab untuk pemrosesan data yang merangkumi cara penghirisan, jenis penyulitan, perawakkan kepingan data untuk proses muat naik. Proses muat turun termasuk penyahsulitan dan pembinaan semula fail. API storan awan digunakan untuk proses muat naik dan muat turun. Peringkat data bertanggungjawab untuk penyimpanan data selepas pemrosesan data dalam lapisan aplikasi. Penyedia perkhidmatan awan iaitu *Google Cloud Storage*, *AWS S3* dan *Microsoft Azure Storage* bertanggungjawab menyimpan kepingan data. *AWS Amplify* dan *Google Firebase* akan bertanggungjawab untuk menguruskan maklumat pengguna untuk log masuk dan pendaftaran.

#### 4.1 Carta Hierarki Modul

Aplikasi ini terdiri daripada beberapa modul berdasarkan setiap fungsi. Setiap fungsi dipisahkan ke dalam modul untuk memudahkan proses pengekodan dan juga memastikan setiap fungsi dapat diuruskan secara berasingan. Modul yang termasuk dalam aplikasi ini adalah Log Masuk dan Pendaftaran, Muat Naik, Muat Turun dan Memadam, Menghiris, Penyulitan dan Penyahsulitan, Perawakkan dan Pembinaan Semula Fail.



RAJAH 4.2. Carta Hierarki Modul Aplikasi

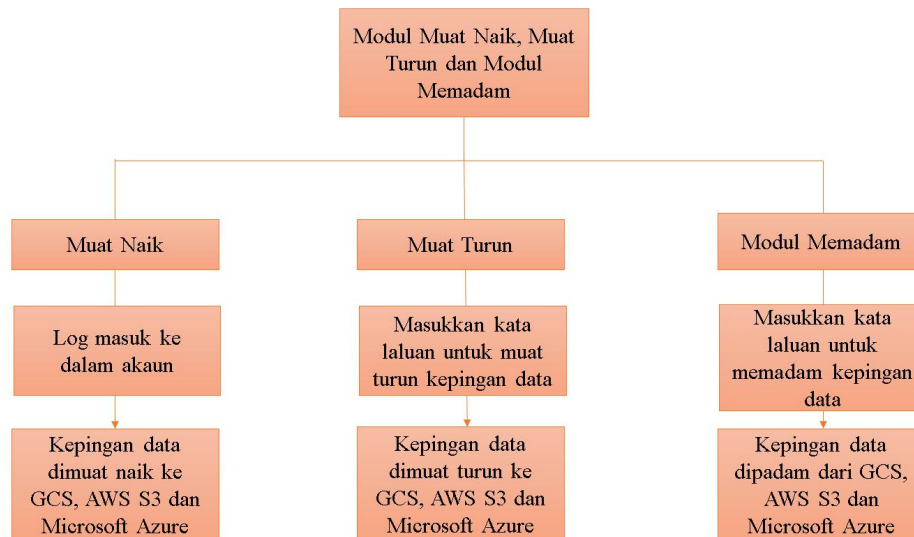
##### 4.1.1 Modul Pendaftaran dan Log Masuk Akaun



RAJAH 4.3. Carta Modul Pendaftaran dan Log Masuk Aplikasi

Modul log masuk dan pendaftaran bertanggungjawab untuk tujuan pengesahan. Fungsi log masuk dan pendaftaran permohonan dikendalikan oleh *Google Firebase Authentication*. Pengguna perlu mendaftar akaun bagi menggunakan aplikasi tersebut. Butiran pengguna berdaftar dan pengesahan pengguna dikendalikan oleh *Google Firebase Authentication*. Aplikasi ini boleh digunakan oleh pengguna yang disahkan berdasarkan kelayakan mereka di bahagian log masuk.

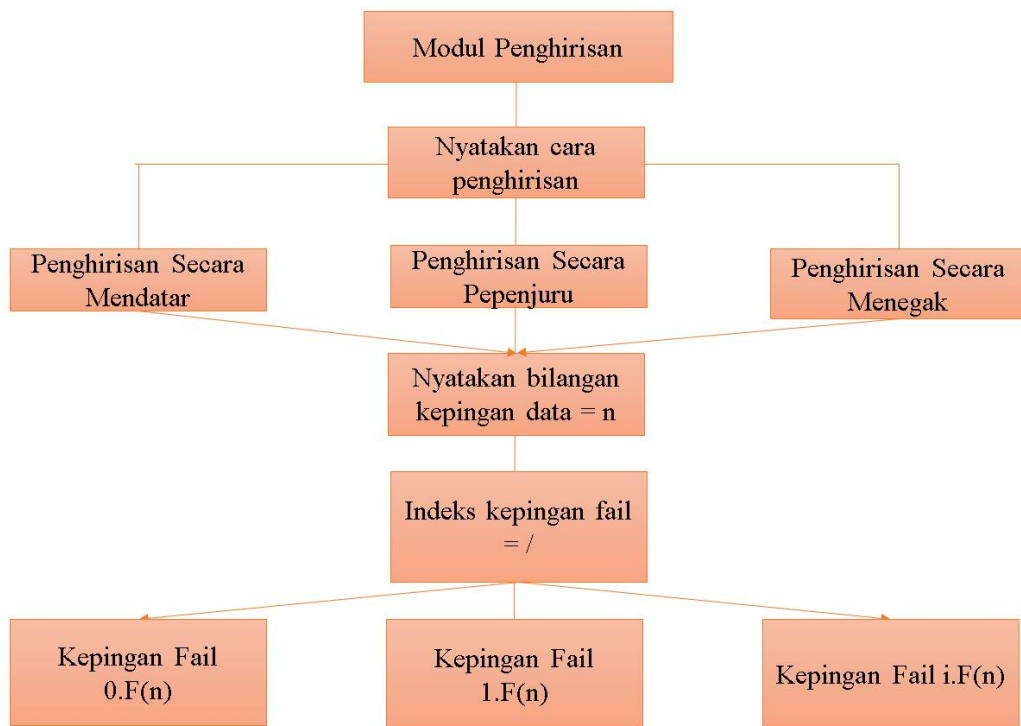
#### 4.1.2 Modul Muat Naik, Muat Turun dan Modul Memadam



RAJAH 4.4. Carta Modul Muat Naik, Muat Turun dan Modul Memadam Aplikasi

Modul muat naik, muat turun dan memadam bertanggungjawab untuk memuat naik kepingan data fail pengguna yang diproses ke storan awan dan memuat turun kepingan data fail pengguna dari storan awan. Modul memadam membolehkan pengguna untuk memadam fail yang tidak lagi diperlukan atau tidak mahu disimpan di dalam storan awan. Proses muat naik, muat turun dan memadam dikendalikan oleh API storan *GCS*, *AWS S3* dan *Microsoft Azure Storage*. Bagi proses memuat turun dan memadam fail, pengguna perlu memasukkan kod laluan atau biometrik terlebih dahulu.

#### 4.1.3 Modul Penghirisan

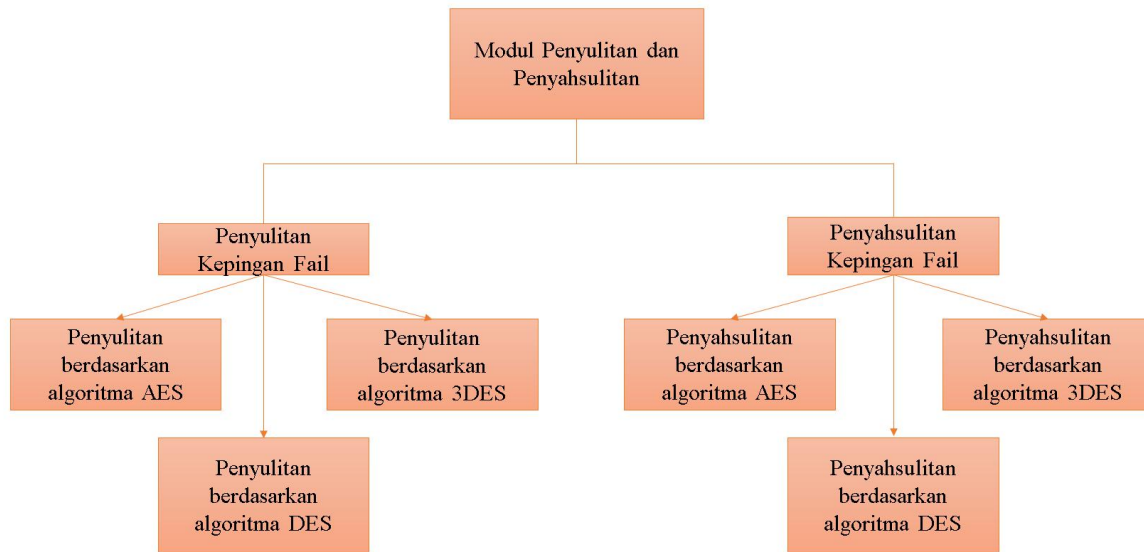


RAJAH 4.5. Carta Modul Penghirisan Aplikasi

Modul penghirisan bertanggungjawab untuk menghiris fail yang dimuat naik secara dinamik oleh pengguna. Tiga jenis penghirisan disediakan iaitu secara menegak, mendatar atau pepenjuru. Dalam proses penghirisan ini, pengguna harus menyatakan bilangan kepingan fail yang ingin dihiris. Aplikasi ini akan menggesa pengguna untuk memberi input nombor terlebih dahulu sebelum diteruskan untuk menghiris fail mengikut nilai input nombor. Fail yang dihiris kemudian akan diindeks untuk memastikan pembinaan semula fail yang mudah apabila memuat turun kepingan fail nanti.



#### 4.1.4 Modul Penyulitan dan Penyahsulitan



RAJAH 4.6. Carta Modul Penyulitan dan Penyahsulitan Aplikasi

Modul penyulitan dan penyahsulitan bertanggungjawab untuk penyulitan dan penyahsulitan kepingan data sebelum dimuat naik ke storan awan dan selepas dimuat turun dari storan awan. Hirisan data boleh disulitkan dan dinyahsulitkan menggunakan tiga algoritma yang berbeza iaitu AES, DES dan 3DES kerana masing-masing merupakan algoritma penyulitan yang dapat menyediakan tahap keselamatan yang tinggi.

#### 4.1.5 Modul Perawakkan



RAJAH 4.7. Carta Modul Perawakkan Aplikasi

Modul perawakkan bertanggungjawab untuk merawakkan susunan kepingan data dalam storan awan. Proses ini memastikan bahawa kepingan data tidak berada dalam susunan berurutan berdasarkan indeks mereka apabila dimuat naik ke storan awan. Tujuan modul perawakkan adalah untuk memastikan keselamatan kepingan data dalam penyimpanan awan sekiranya berlaku apa-apa pelanggaran keselamatan.

#### 4.1.6 Modul Pembinaan Semula Fail

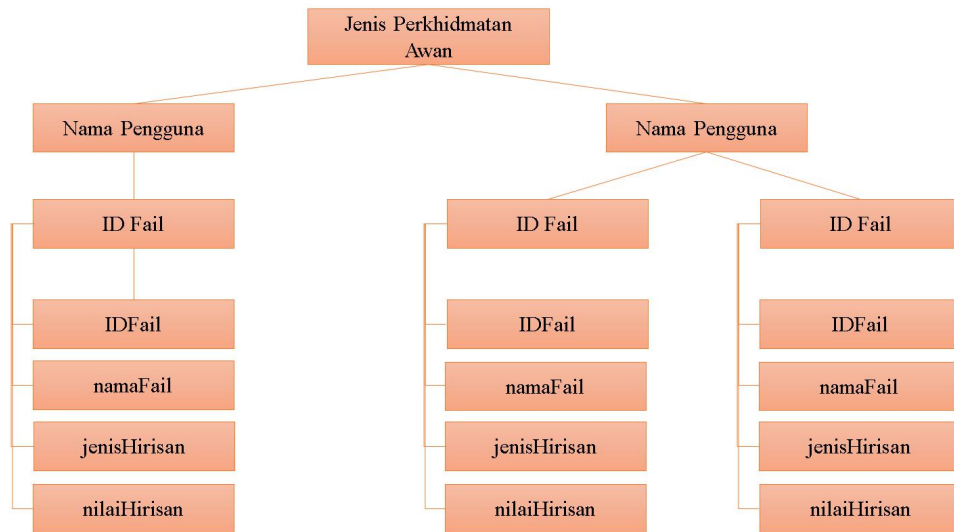


RAJAH 4.8. Carta Modul Pembinaan Semula Masuk Aplikasi

Modul pembinaan semula bertanggungjawab untuk proses penggabungan fail apabila kepingan data dimuat turun dari tiga storan awan yang berbeza. Hirisan data dinyahsulitan terlebih dahulu sebelum dibina semula. Proses pembinaan semula melibatkan penggabungan fail berdasarkan indeks untuk mendapatkan fail yang asal.

#### 4.2 Reka Bentuk Pangkalan Data

Pangkalan data akan digunakan untuk menyimpan maklumat fail yang dimuat naik bagi melancarkan proses muat turun dan memadam fail. Jenis dan nilai hirisan fail, serta nama fail dimuat naik ke pangkalan data semasa proses muat naik fail. Pangkalan data yang digunakan adalah *Google Firebase Realtime Database* yang merupakan pangkalan data *NoSQL* dan oleh itu mempunyai pengoptimuman dan fungsi yang berbeza berbanding dengan pangkalan data hubungan. *Firebase Realtime Database* menyimpan data sebagai satu pokok *JSON* yang besar dan data ringkas yang sangat mudah untuk disimpan.



RAJAH 4.9. Reka bentuk Pangkalan Data Aplikasi

### 4.3 Reka Bentuk Algoritma

Reka bentuk algoritma aplikasi membincangkan butiran dan langkah setiap fungsi melalui spesifikasi pseudokod.

#### 4.3.1 Proses Muat Naik Fail

##### MULA

Baca fail yang dimuat naik ( $F$ )

Baca jenis penghirisan yang dikehendaki daripada input pengguna ( $F$ )  
 Baca bilangan hirisan fail yang dikehendaki daripada input pengguna ( $n$ )  
 Baca jenis penyulitan yang dikehendaki daripada input pengguna ( $E$ )  
 Menghiris fail berdasarkan input pengguna ( $F(n)$ )

Indekskan hirisan fail ( $0.F(n), 1.F(n), 2.F(n), \dots, i.F(n)$ )

Sulitkan hirisan fail ( $E(0.F(n)), E(1.F(n)), E(2.F(n)) \dots E(i.F(n)) \dots$ )

Perawakkan hirisan fail

Muat naik hirisan fail secara rawak ke storan awan

##### AKHIR

#### 4.3.2 Proses Muat Turun Fail

##### MULA

Baca nama fail untuk dimuat turun ( $F$ )

Baca kod laluan/pin dari input pengguna ( $P$ )

**JIKA** kod laluan betul

Dapatkan semula hirisan fail dari storan awan ( $E(0.F(n)), E(1.F(n))... E(i.F(n))$ )

Nyahsulis hirisan fail ( $0.F(n), 1.F(n)... i.F(n)$ )

Gabungkan hirisan fail dan bina semula fail ( $F$ )

**JIKA TIDAK** kod laluan salah

Papar mesej muat turun fail ditolak

**AKHIR**

*4.3.3 Pemadaman Fail*

**MULA**

Baca fail untuk dipadam ( $F$ )

Baca kod laluan/pin dari input pengguna ( $P$ )

**JIKA** kod laluan betul

Padamkan hirisan fail dalam storan awan ( $E(0.F(n)), E(1.F(n))... E(i.F(n))$ )

**JIKA TIDAK** kod laluan salah

Papar mesej pemadaman fail dinafikan

**AKHIR**

*4.4 Reka Bentuk Antara Muka*

Reka bentuk antara muka aplikasi memberi tumpuan kepada reka bentuk fungsi yang akan digunakan oleh pengguna. Antara muka direka dengan cara yang mesra pengguna dan membolehkan pengguna berinteraksi dengan aplikasi dengan baik dan lancar. Aplikasi ini terdiri daripada beberapa antara muka yang termasuk Log Masuk, Daftar Akaun, Halaman Utama, Muat Naik Fail, Muat Turun Fail dan Memadam Fail.

*4.4.1 Log Masuk, Daftar, Halaman Utama dan Pengurusan Akaun*

Aplikasi memberikan pilihan kepada pengguna untuk storan perkhidmatan awan berdasarkan keperluan. Pengguna boleh mendaftar masuk ke aplikasi menggunakan butiran akaun mereka jika sudah mempunyai akaun. Butiran yang diperlukan adalah e-mel dan kata laluan berdaftar. Jika butiran yang salah dimasukkan, pengguna akan ditolak daripada akses aplikasi dan mempunyai pilihan untuk menekan butang “terlupa kata laluan” untuk mendapatkan semula akaun mereka. Pengguna yang tidak mempunyai akaun boleh mendaftar untuk akaun dengan memasukkan butiran mereka dan klik pada butang “Pendaftaran”. Pengguna kemudian boleh mendaftar masuk ke dalam akaun mereka dan halaman utama aplikasi dapat dilihat.



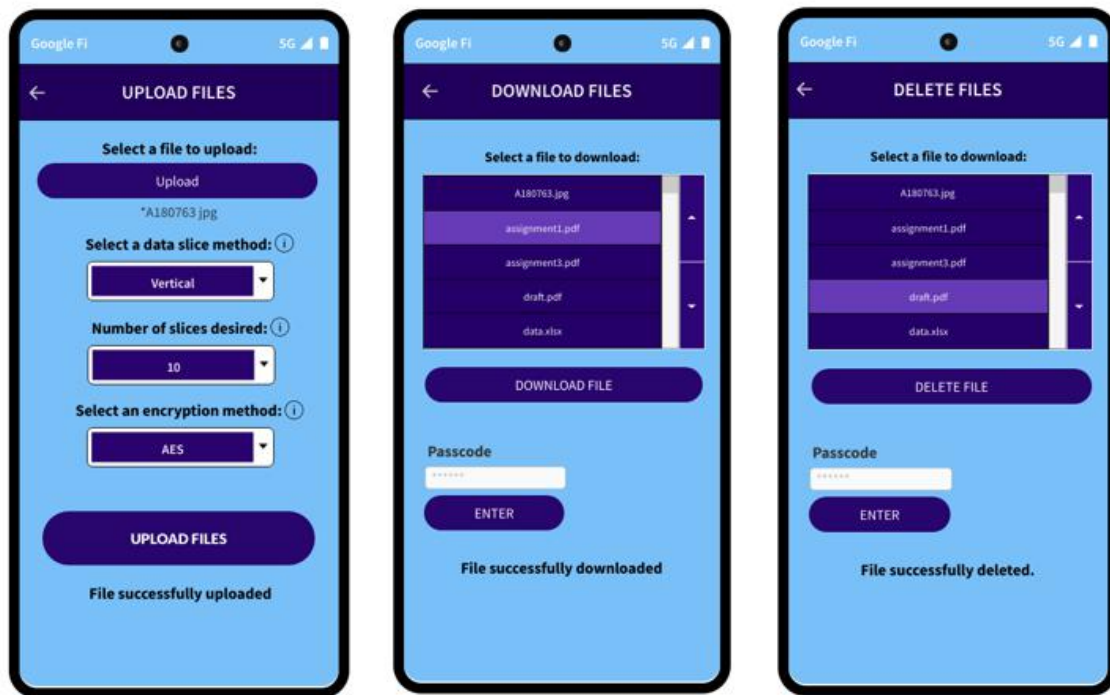
RAJAH 4.10. Reka Bentuk Antara Muka Log Masuk, Daftar Masuk dan Halaman Utama

#### 4.4.2 Muat Naik, Muat Turun dan Pemadaman Fail

Apabila pilihan muat naik fail dipilih, pengguna dihalakan ke antara muka memuat naik fail. Pengguna boleh memilih fail daripada peranti mereka dengan memilih butang Pilih Fail. Pengguna kemudiannya mesti memasukkan jenis penghirisan dan bilangan hirisan fail yang dikehendaki untuk fail dimuat naik. Pengguna juga perlu memilih algoritma penyulitan dan boleh merujuk kepada info yang disediakan jika keliru dan kurang faham. Untuk memuat naik fail, pengguna mesti memilih butang Muat Naik Fail. Sebaik sahaja fail berjaya dimuat naik mesej yang menyatakan “Fail berjaya dimuat naik” akan dipaparkan.

Apabila pilihan muat turun fail dipilih, pengguna dihalakan ke antara muka memuat turun fail. Pengguna boleh memilih fail dari senarai fail yang tersedia dan klik pada butang Muat Turun Fail. Pengguna akan digesa untuk memasukkan kod laluan atau biometrik untuk memuat turun fail. Jika kod laluan adalah betul, fail berjaya dimuat turun dan mesej yang menyatakan, “Fail berjaya dimuat turun” dipaparkan untuk memastikan integriti fail.

Apabila pilihan padam fail dipilih, pengguna dihalakan ke antara muka ini dan mereka boleh menghapuskan fail tersebut. Pengguna boleh memilih fail dari senarai fail yang tersedia dan klik pada butang Padam Fail. Pengguna akan digesa untuk memasukkan kod laluan atau biometrik sebagai pengesahan sebelum menghapuskan fail. Jika kod laluan betul, fail berjaya dipadamkan dan mesej yang menyatakan, “Fail berjaya dipadamkan” dipaparkan.



RAJAH 4.11. Reka Bentuk Antara Muka Muat Naik, Muat Turun dan Pepadaman Fail

## 5. Rumusan dan Cadangan

Kesimpulannya, terdapat pelbagai aspek keselamatan yang boleh diaplikasikan bagi memastikan data-data sulit pengguna boleh disimpan dengan selamat di dalam storan awan. 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. Aplikasi ini memberi tumpuan kepada menyediakan aspek keselamatan dalam peranti mudah alih dan awan. Pelbagai jenis masalah dan kelemahan telah dikenal pasti dan penyelesaian keselamatan yang betul telah dicadangkan untuk aplikasi untuk mengatasi kelemahan. Aspek keselamatan privasi, kerahsiaan dan integriti fail dalam peranti mudah alih dan awan boleh dicapai dengan melaksanakan langkah-langkah keselamatan seperti menggunakan teknik penghirisan dan penyulitan.

Antara cadangan yang dikemukakan untuk menambahbaik fungsi aplikasi tersebut adalah menggunakan *Flutter* atau *Amplify Studio* agar aplikasi tersebut boleh digunakan di mana-mana platform seperti peranti mudah alih *Android*, *IOS* dan juga laman sesawang.

## Rujukan

- 7 Kegunaan Umum Pengkomputeran awan. AXO Technologies. (2021). Retrieved November 30, 2022, from <https://axotechnologies.com/7-kegunaan-umum-pengkomputeran-awan/>
- Alatalo, P., Järvenoja, J., Karvonen, J., Keronen, A., & Kuvaja, P. (2002). 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.
- Bhattacharya, S. (2019). *Cryptography - data encryption standard (DES)*. C# Corner. Retrieved November 30, 2022, from <https://www.c-sharpcorner.com/article/cryptography-data-encryption-standard-des/>
- Google. (2017). *Get started with cloud storage on Android | cloud storage for firebase*. Google. Retrieved November 28, 2022, from <https://firebase.google.com/docs/storage/android/start>
- Hardik, & Santhosh K. (2022). AWS vs azure vs google cloud - detailed cloud comparison. Intellipaat Blog. Retrieved December 5, 2022, from <https://intellipaat.com/blog/aws-vs-azure-vs-google-cloud/>
- IBM Education, What is Three-Tier Architecture.(2019). Retrieved 6 December 2022, from <https://www.ibm.com/cloud/learn/three-tier-architecture>
- K. Subramanian & F. Leo John. (2017). Dynamic and secure unstructured data sharing in multicloud storage using the hybrid crypto-system. International Journal of Advanced and Applied Sciences ,5(1): 15-23. DOI: 10.21833/ijaas.2018.01.00346
- K. Subramanian & F.Leo John. (2017). Enhanced Security for Data Sharing in Multi Cloud Storage (SDSMC). (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 8, No. 3: 176 - 185. (DOI): 10.14569/IJACSA.2017.080326
- Kareesma A/P P.Nageswaran. (2021). Penyimpanan Data Sulit Dalam Persekitaran Berbilang Awan. FTSM. Universiti Kebangsaan Malaysia.
- Larson, M. (2020). What are the Differences Between DES and AES Encryption? Retrieved December 5, 2022, from <https://info.townsendsecurity.com/bid/72450/what-are-the-differences-between-des-and-aes-encryption>
- 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 (2019). Retrieved December 18, 2022, from <https://edge.siriuscom.com/security/mobile-device-security-in-the-workplace-5-key-risks-and-a-surprising-challenge/>
- Noh, M. bte M. (2021). Teknologi cloud computing. Retrieved November 12, 2022, from <http://catatantugasan.blogspot.com/2013/02/teknologi-cloud-computing.html>
- 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).
- Sandeep Nehe & M.B. Vaidya. (2015). Data Security using Data slicing over storage clouds. International Conference on Information Processing (ICIP): 322 – 325. Vishwakarma Institute of Technology. 16-19 December. DOI: 10.1109/INFOP.2015.7489401.
- Save data in a local database using Room | Android Developers(2021), Retrieved 9 December 2022, from <https://developer.android.com/training/data-storage/room>
- Singh, V. (2022). 10 benefits of cloud storage. Cloud Academy. Retrieved December 5, 2022, from <https://cloudacademy.com/blog/10-benefits-of-using-cloud-storage/>
- Uses SDK, Android Developers, Retrieved 17 December 2022, from <https://developer.android.com/guide/topics/manifest/uses-sdk-element#ApiLevels>
- What is Activity Diagram?(2019). Retrieved 16 Disember 2022, from <https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-activity-diagram/>
- What is Data Encryption? Forcepoint. (2022). Retrieved 12 November 2022, from <https://www.forcepoint.com/cyber-edu/data-encryption>
- What is Use Case Diagram? (2020). Retrieved 20 December 2022, from <https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-use-case-diagram>