

PENYIMPANAN DATA SULIT MELALUI PENYULITAN DALAM PERSEKITARAN MULTI-AWAN

SNEHA A/P MURUGAN

ELANKOVAN A/L A.SUNDARARAJAN

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

ABSTRAK

Dengan perkembangan teknologi, jumlah pengguna peranti mudah alih telah meningkat secara drastik selama bertahun-tahun. Pelbagai aplikasi dan perkhidmatan kini tersedia pada peranti mudah alih, membolehkan pengguna menjalankan tugas dan rutin harian mereka tanpa mengira masa dan lokasi. Kekangan storan peranti mudah alih telah mendorong pengguna untuk beralih kepada penyelesaian storan awan. Selama bertahun-tahun, pengkomputeran awan telah berkembang untuk menangani kekangan pengkomputeran dan storan peranti mudah alih. Kekangan storan ini dapat diatasi dengan menggunakan storan awan, dengan adanya sambungan Internet berkelajuan tinggi. Walaupun pengkomputeran awan mempunyai manfaatnya, kebimbangan mengenai keselamatan data pengguna masih wujud. Data yang disimpan di awan dihantar melalui Internet, di mana pengguna mempunyai kawalan terhad, mendedahkan data kepada risiko yang mungkin berlaku. Serangan perisian hasad yang menasaskan peranti mudah alih boleh mengakibatkan kehilangan maklumat sensitif. Selain itu, storan awan juga terdedah kepada pencerobohan data akibat ancaman dari dalam, termasuk rampasan akaun dan serangan daya kasar. Objektif kajian ini adalah untuk memastikan keselamatan data dalam persekitaran awan awam. Kajian ini mencadangkan aplikasi mudah alih yang dibangunkan menggunakan *Flutter* dan *Dart* yang membolehkan pengguna memuat naik fail mereka secara selamat ke pelbagai penyedia storan awan. Aplikasi ini menawarkan pilihan untuk sama ada memotong data terlebih dahulu dan kemudian menyulitkannya, atau menyulitkan data terlebih dahulu sebelum memotongnya kepada segmen. Segmen data ini akan dibahagikan secara dinamik, disulitkan menggunakan pelbagai jenis algoritma penyulitan, dan kemudian dimuat naik ke pelbagai penyedia storan awan. Pelaksanaan langkah-langkah keselamatan ini, yang akan dibincangkan dalam laporan ini, berdasarkan analisis pelbagai teknik. Dengan menggunakan langkah-langkah ini, aplikasi ini bertujuan untuk menghalang pencerobohan data dalam storan awan, walaupun dalam keadaan akaun storan awan pengguna digodam.

Kata Kunci: Storan awan, Penyulitan, Flutter dan Dart.

ABSTRACT

With the advancement of technology, the number of mobile device users has drastically increased over the years. Various applications and services are now available on mobile devices, allowing users to carry out their daily tasks and routines regardless of time and location. The storage limitations of mobile devices have prompted users to turn to cloud storage solutions. Over the years, cloud computing has evolved to address the computational and storage constraints of mobile devices. These storage limitations can be overcome by utilizing cloud storage, provided there is a high-speed Internet connection. Although cloud computing has its benefits, concerns about the security of user data still exist. Data stored in the cloud is transmitted over the Internet, where users have limited control, exposing the data to potential risks. Malware attacks targeting mobile devices can result in the loss of sensitive information. Furthermore, cloud storage is also susceptible to data breaches due to insider threats, including account takeovers and brute-force attacks. The objective of this study is to ensure data security in public cloud environments. This study proposes a mobile application developed using Flutter and Dart that allows users to securely upload their files to various cloud storage providers. The application offers the option to either slice the data first and then encrypt it or to encrypt the data first before slicing it into segments. These data segments will be dynamically divided, encrypted using various types of encryption algorithms, and then uploaded to multiple cloud storage providers. The implementation of these security measures, which will be discussed in this report, is based on an analysis of multiple techniques. By employing these measures, the application aims to prevent data breaches in cloud storage, even in the event of a user's cloud storage account being compromised.

Keywords: Cloud computing, Encryption algorithms, Data slicing / segmentation.

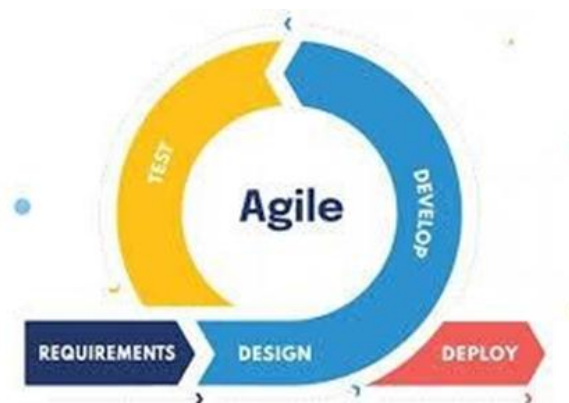
PENGENALAN

Seiring dengan kemajuan teknologi, penggunaan data dan perkongsian maklumat telah mengalami peningkatan yang ketara dari semasa ke semasa, khususnya dengan kemunculan peranti mudah alih. Peranti seperti telefon pintar membolehkan pengguna berkomunikasi dan berkongsi data tanpa mengira masa dan lokasi dengan bantuan Internet. Dengan pertumbuhan penggunaan data, pengkomputeran awan muncul sebagai penyelesaian yang membolehkan individu dan organisasi perniagaan mengakses sumber mereka tanpa batasan storan pada peranti mudah alih. Pengkomputeran awan membolehkan pengguna menyimpan data, aplikasi, dan perkhidmatan dalam talian, di mana pelbagai jenis data seperti fail, imej, dan video dapat disimpan di awan dan diakses melalui aplikasi mudah alih atau desktop. Organisasi perniagaan telah mengamalkan konsep *Bawa Peranti Anda Sendiri (BYOD)*, yang menggalakkan pekerja untuk menggunakan telefon pintar, komputer riba, dan tablet mereka sendiri di tempat kerja. Amalan ini membolehkan pekerja menggunakan peranti peribadi mereka dalam persekitaran profesional. Terdapat tiga jenis pengkomputeran awan: awan awam, persendirian, dan hibrid. Awan awam menyediakan perkhidmatan penyimpanan

melalui Internet dan dimiliki oleh pembekal perkhidmatan awan pihak ketiga, manakala awan persendirian dimiliki oleh satu organisasi dalam rangkaian tertutup untuk menyimpan sumber mereka. Awan hibrid adalah gabungan antara awan awam dan persendirian. Pengguna dapat memberi tumpuan kepada aktiviti perniagaan mereka tanpa perlu risau tentang pengkonfigurasi dan penyelenggaraan sumber storan mereka. Perkhidmatan yang disediakan berasaskan model bayar mengikut penggunaan, membolehkan pengguna menjimatkan kos dengan menyewa infrastruktur daripada membangunkannya sendiri. Kapasiti storan boleh ditingkatkan dan disesuaikan mengikut keperluan, mengurangkan kebimbangan tentang kehilangan data akibat kerosakan storan fizikal. Yang paling penting, data boleh diakses pada bila-bila masa dan di mana sahaja melalui Internet dengan menggunakan perkhidmatan awan. Selain itu, pengkomputeran awan juga menyediakan perkhidmatan seperti Infrastruktur sebagai Perkhidmatan (*IaaS*), Platform sebagai Perkhidmatan (*PaaS*), pengkomputeran tanpa pelayan, dan Perisian sebagai Perkhidmatan (*SaaS*), membolehkan pengguna memilih platform yang sesuai dengan keperluan perniagaan mereka.

METODOLOGI KAJIAN

Metodologi yang digunakan dalam pembangunan projek ini ialah Agile yang menggunakan lelaran pembangunan dan pengujian berterusan sepanjang kitaran hayat pembangunan perisian projek. Kitaran hayat pembangunan perisian merupakan satu model konseptual yang digunakan untuk memandu setiap peringkat dalam pembangunan aplikasi. Pemilihan model ini adalah kerana ia mudah difahami dan mampu menyesuaikan diri dengan perubahan yang berlaku. Model ini mempunyai aliran berulang yang sepadan dengan fasa pembangunan projek ini.



Rajah 1: Model Kitaran Hayat Agil

Empat fasa utama model agil adalah seperti berikut:

Fasa analisis

Fasa ini memberi tumpuan kepada pengumpulan maklumat yang diperlukan untuk membangunkan aplikasi. Keperluan seperti objektif, skop, masalah, dan kekangan kajian dikumpulkan untuk menganalisis keperluan kajian. Kajian dari sumber lain termasuk kajian lain, jurnal dan Internet dilakukan untuk memahami lebih lanjut keperluan kajian. Berdasarkan analisis dan perbandingan yang dilakukan dari sumber kajian yang lain, pendekatan keselamatan yang terbaik dapat disesuaikan untuk pembangunan aplikasi.

Fasa reka bentuk

Fasa ini memberi tumpuan kepada mereka bentuk aplikasi berdasarkan keperluan yang dikumpulkan. Reka bentuk ini memberi tumpuan kepada fungsi aplikasi dan reka bentuk antara muka pengguna aplikasi. Aplikasi yang dibangunkan sesuai untuk individu yang sering menyimpan dokumen kerja, fail sulit, dan imej dan video peribadi mereka pada peranti mudah alih mereka dan bimbang tentang isu keselamatan.

Keperluan fungsian pengguna adalah seperti dalam Jadual 1 berikut:

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 1: Keperluan Fungsian Pengguna 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 dalam Jadual 2 berikut:

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> . Aplikasi ini juga harus membenarkan pengguna log masuk menggunakan akaun <i>Google Drive</i> untuk pilihan storan yang lain.
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 (<i>API</i>) perkhidmatan storan awan digunakan untuk memuat naik data ke <i>AWS</i> , <i>Microsoft Azure Storage</i> dan <i>Google Drive</i> .
Cincangan Fail (Muat Naik)	Sistem harus mengira nilai cincangan untuk fail yang dimuat naik.
Penghirisan Fail	Aplikasi ini harus menghiris fail secara dinamik berdasarkan bilangan kepingan yang ditentukan oleh pengguna. Fail dihiris hendaklah diindeks.
Penyulitan Fail	Aplikasi ini patut menyulitkan setiap hirisan fail.
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 (<i>API</i>) perkhidmatan penyimpanan awan digunakan untuk memuat turun data dari <i>AWS</i> , <i>Microsoft Azure Storage</i> dan <i>Google Drive</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.

Cincangan Fail (Muat Turun)	Sistem harus mengira nilai cincangan untuk fail yang dimuat naik dan membandingkannya dengan nilai cincangan fail yang dimuat turun. Aplikasi ini harus menjana mesej tulen jika nilai cincangan adalah sama dan menjana mesej amaran jika nilai cincangan adalah berbeza.
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 (<i>API</i>) perkhidmatan penyimpanan awan digunakan untuk memadam data dari <i>AWS</i> , <i>Microsoft Azure Storage</i> dan <i>Google Drive</i> .
Log Keluar Akaun	Sistem ini harus membenarkan pengguna log keluar dari akaun.

Jadual 2: Keperluan Fungsian Sistem Aplikasi

Keperluan bukan fungsian mentakrifkan sifat dan kekangan aplikasi dan menerangkan tingkah laku aplikasi. Keperluan tidak berfungsi ditakrifkan seperti dalam Jadual 3 berikut:

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 memastikan memudahkan penggunaan.
Ketersediaan	Aplikasi ini harus sentiasa tersedia di hampir semua peranti mudah alih dan aplikasi itu harus diakses di mana sahaja dengan 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 kesilapan.
Kecekapan	Aplikasi ini harus berfungsi tanpa sebarang kelewatan dengan sambungan Internet yang baik.

Jadual 3: Keperluan Bukan Fungsian Aplikasi

Aplikasi yang akan dibangunkan memberi tumpuan kepada aspek keselamatan data, oleh itu prinsip keselamatan data dibincangkan seperti dalam Jadual 4 berikut:

Prinsip	Keterangan
Integriti	Aplikasi ini hendaklah memastikan bahawa data yang disimpan di awan tidak diusik. Pencincangan 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 hanya pengguna yang diberi kuasa boleh mengakses aplikasi dan melakukan muat turun fail dengan pengesahan kod laluan atau biometrik.

Jadual 4: Keperluan Keselamatan Siber Aplikasi

Fasa pengkodan

Fasa ini memberi tumpuan kepada pembangunan aplikasi menggunakan alat dan sumber yang diperlukan. Pelaksanaan aplikasi ini dibangunkan menggunakan *Flutter* dan *Android Studio*, iaitu persekitaran pembangunan bersepadu (*IDE*) yang sesuai untuk pembangunan aplikasi mudah alih. Walaupun *Flutter* biasanya menggunakan bahasa *Dart*, dalam projek ini, Java turut digunakan untuk menguruskan logik backend dan fungsi khusus yang memerlukan integrasi asli *Android*. Dokumentasi yang digunakan untuk persekitaran berbilang awan termasuk dokumentasi *AWS Amplify* untuk *Android*, *Firebase*, *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***, ***amplifyframework:aws-auth-cognito***, ***com.google.cloud:google-cloud-storage***, ***firebase-database***, ***firebase-auth***, ***azure-storage-android***, ***com.google.cloud:libraries-bom***, ***com.android.tools:desugar_jdk_libs***, ***drive-api-v3***, ***org.slf4j:slf4j-api***, dan ***org.slf4j:slf4j-log4j12***. Semua *dependencies* dan *libraries* ini digunakan dalam aplikasi untuk pengesahan pengguna, storan awan untuk muat naik, muat turun dan memadam fail pengguna.

Fasa pengujian

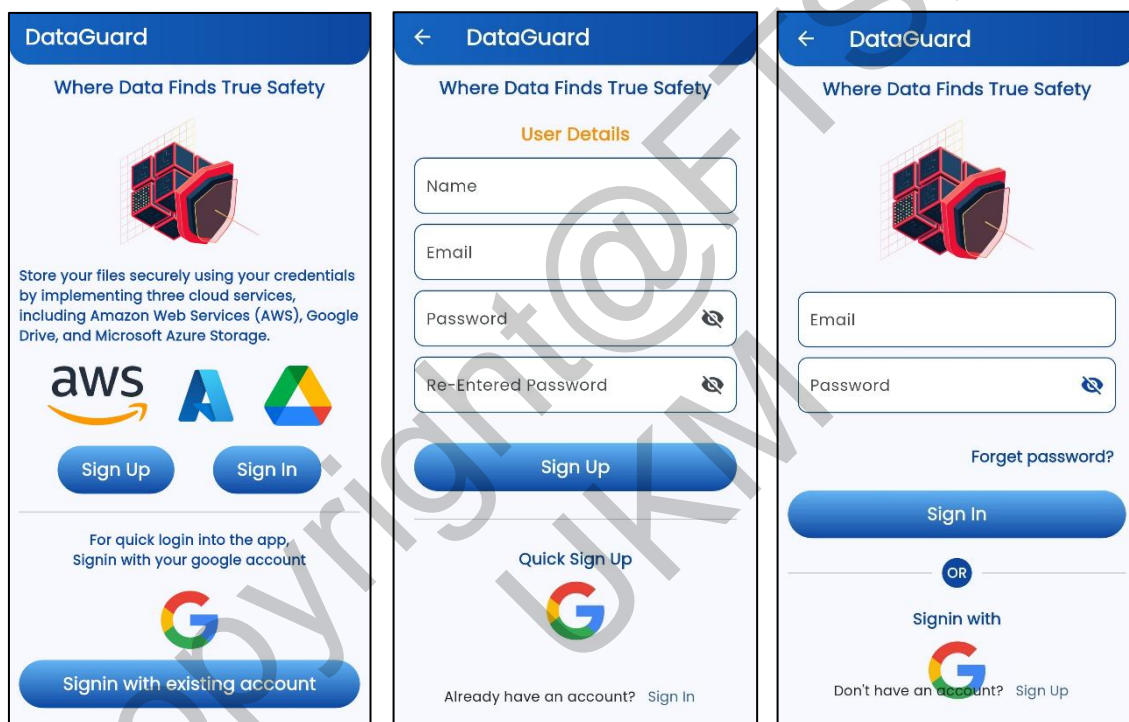
Fasa ini memberi tumpuan kepada menguji aplikasi berdasarkan keperluan dan menyelesaikan masalah aplikasi untuk ralat. Objektif ujian untuk aplikasi *Penyimpanan Data Sulit Melalui Penyulitan Dalam Persekitaran Multi-Awan* adalah untuk menguji komponen aplikasi yang penting untuk fungsi utama yang melindungi data pengguna menggunakan teknik seperti pencincangan, penghirisan, dan penyulitan. Ujian tahap sistem juga dilakukan berdasarkan aspek fungsi dan tidak berfungsi aplikasi. Jenis ujian yang 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 seperti dalam Jadual 5.

Jenis Fail	Saiz 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)	✓	✓	✓	✓
Fail Audio (.mp3)			✓	

Jadual 5: Jenis Fail dan Saiz Fail Diuji Aplikasi

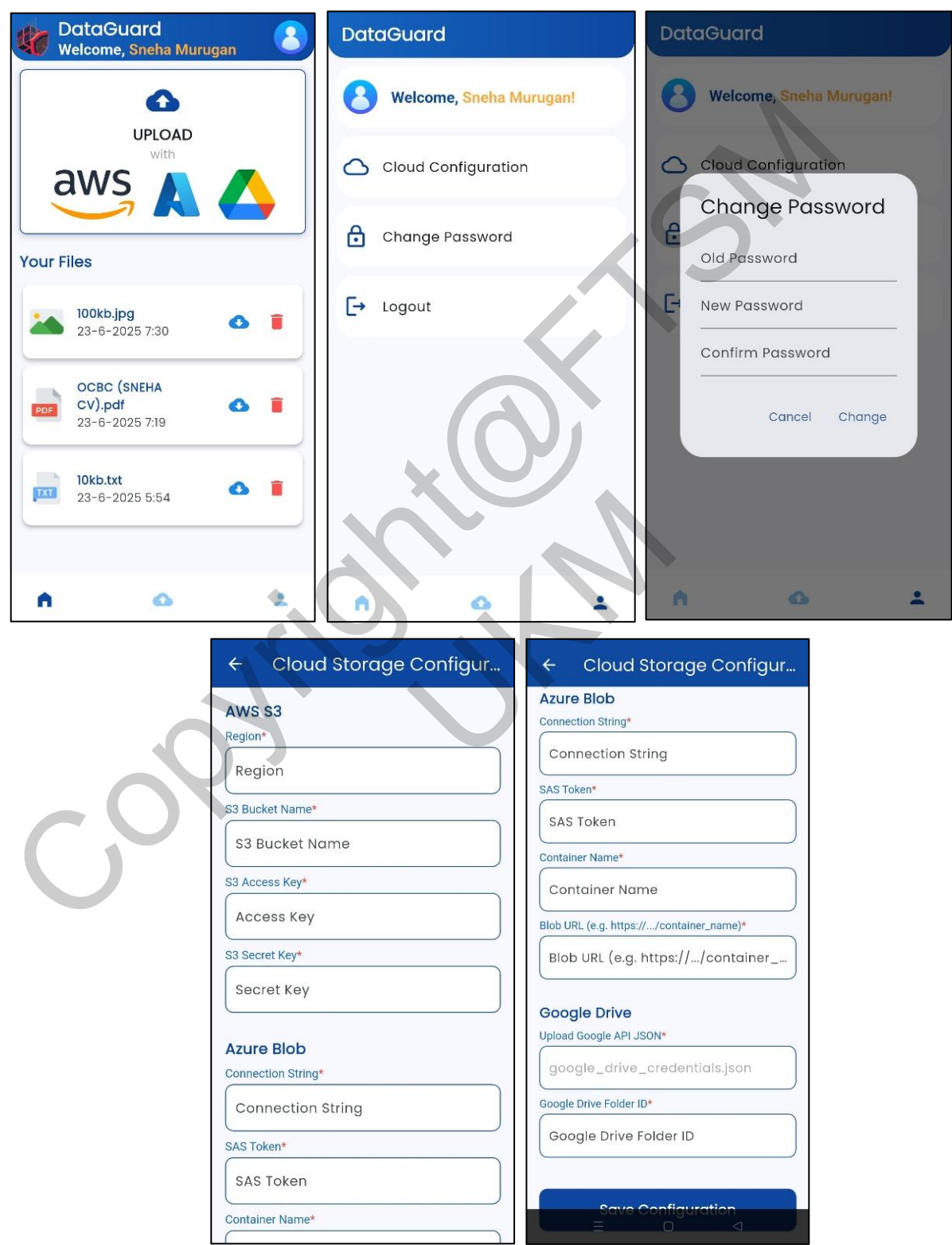
KEPUTUSAN DAN PERBINCANGAN

Aplikasi ini terdiri daripada antara muka Selamat Datang di mana pengguna boleh memilih jenis storan awan yang dikehendaki. Jika pengguna memilih untuk menggunakan perkhidmatan *AWS* dan *Azure Storage*, terdapat antara muka Daftar Masuk di mana pengguna boleh log masuk ke akaun sedia ada mereka. Mereka boleh mendaftar sebagai pengguna baharu dalam antara muka Daftar dengan butiran yang diminta. Bagi pengguna yang memilih untuk menggunakan akaun *Google*, pengesahan akaun *Google Drive* diperlukan seperti yang ditunjukkan dalam Rajah 2.



Rajah 2: Rajah Antara Muka Halaman Selamat Datang, Log Masuk, Daftar, dan 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 dan menguruskan butiran akaun mereka di halaman utama seperti dalam Rajah 3.



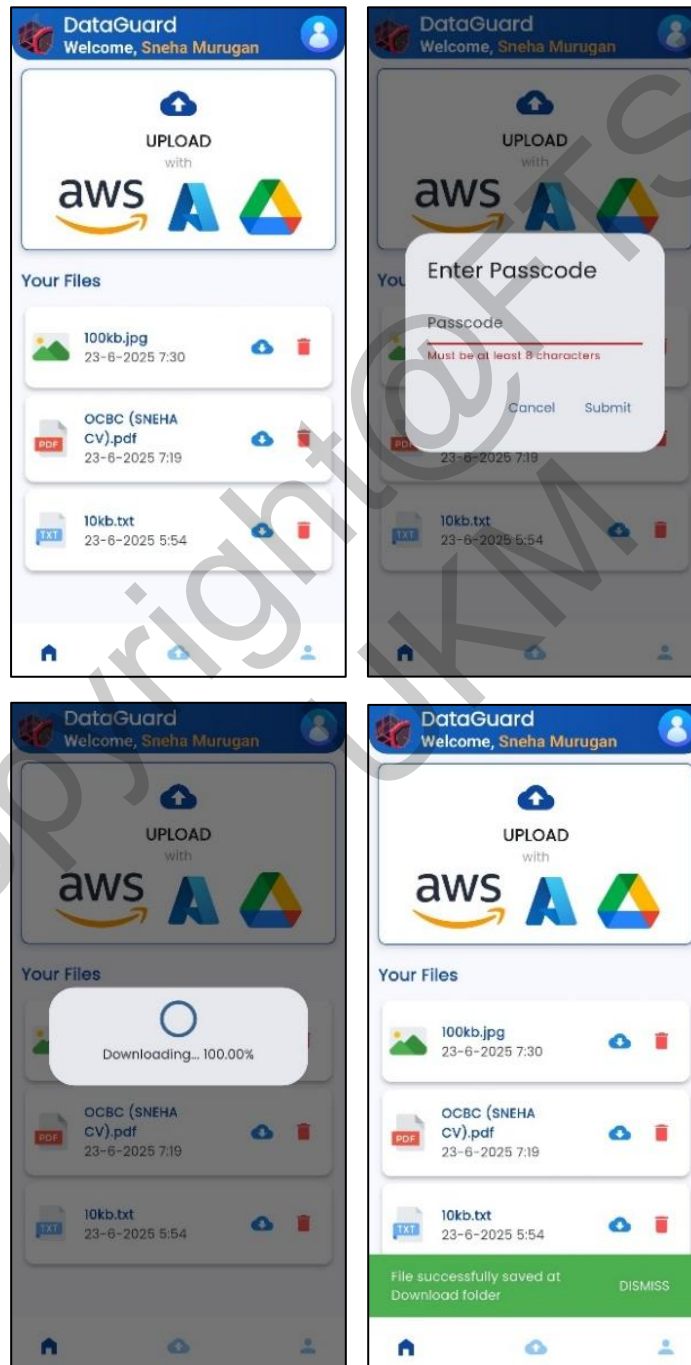
Rajah 3: Rajah Antara Muka Halaman Utama dan Pengurusan Akaun

Dalam antara muka muat naik fail, pengguna boleh memilih fail yang ingin mereka muat naik dari peranti mudah alih mereka. Mereka kemudian boleh memilih jenis hirisan (*Horizontal* atau *Vertical*), bilangan kepingan yang dikehendaki untuk menghiris fail mereka dari senarai *dropdown* dan jenis penyulitan (*AES* atau *SEA*). Mereka kemudian boleh klik butang muat naik untuk menyelesaikan proses muat naik seperti dalam Rajah 4.

The image displays three sequential screenshots of the DataGuard mobile application's file upload interface. Each screen features a blue header with the 'DataGuard' logo. The first screenshot shows the initial state with a 'Choose File' button, 'Horizontal' slicing type selected, '50' bit slicing size, 'Select Encryption Algorithm' dropdown, and a 'Passcode' field. The second screenshot shows the 'Bit slicing size' dropdown menu expanded, listing options from 50 to 100. The third screenshot shows the 'Encryption Algorithm' dropdown menu expanded, listing 'AES' and 'SEA'. All three screenshots include an 'Upload Now' button at the bottom and a standard mobile navigation bar with home, upload, and user icons.

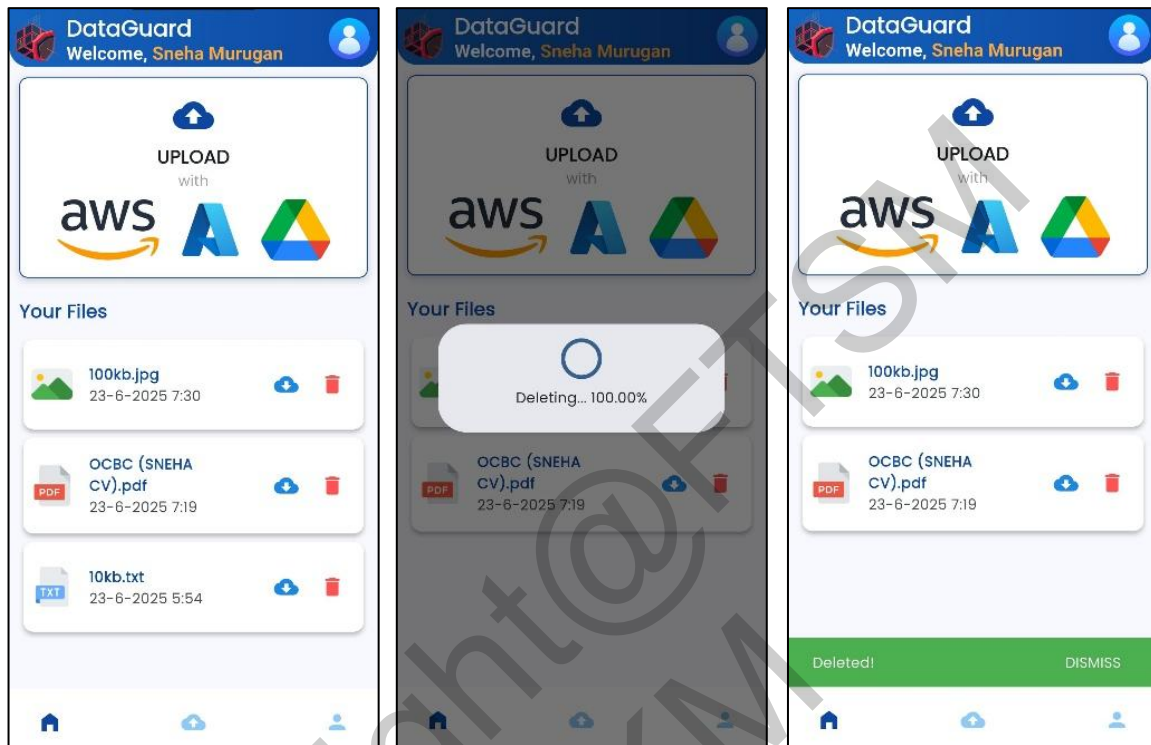
Rajah 4: Rajah Antara Muka Muat Naik Fail

Dalam antara muka muat turun fail, pengguna boleh memilih fail untuk dimuat turun daripada senarai 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. Mereka akan digesa dengan *dialog pop-up* kod laluan atau biometrik untuk memuat turun fail. Setelah kod laluan yang betul dimasukkan, fail akan berjaya dimuat turun. Mesej akan dipaparkan menyatakan fail telah dimuat turun ke direktori bernama *Downloads* seperti dalam Rajah 5.



Rajah 5: Rajah Antara Muka Muat Turun Fail

Dalam antara muka memadam fail, pengguna boleh memilih fail yang ingin mereka padamkan dan klik butang padam. Mereka akan digesa dengan *dialog pop-up* kod laluan atau biometrik untuk memadam fail. Setelah kod laluan yang betul dimasukkan, fail akan berjaya dipadamkan seperti yang ditunjukkan dalam Rajah 6.



Rajah 6: Rajah Antara Muka Memadam Fail

Cadangan Penambahbaikan

Selepas menjalankan kajian yang menyeluruh, cadangan untuk penambahbaikan masa hadapan adalah menggunakan lebih daripada 3 storan awan untuk meningkatkan keselamatan. Keselamatan lebih baik apabila lebih banyak storan awan digunakan kerana kebocoran dan pelanggaran data menjadi lebih sukar. Kedua, fungsi pemulihan fail yang dipadam boleh ditambah sebagai ciri “*Recycle Bin*” supaya pengguna boleh memulihkan fail yang terpadam secara tidak sengaja. Akhirnya, Tambahan pula, aplikasi boleh menambah sokongan mesra OKU, serta memberi pilihan kepada pengguna untuk menggunakan kata laluan yang dijana secara rawak dan menyimpan kunci penyulitan secara selamat dalam aplikasi. Dengan ini, pengguna akan mempunyai fleksibiliti dalam menggunakan aplikasi.

KESIMPULAN

Penyelidikan ini dimulakan dengan mengenal pasti masalah dan kebimbangan keselamatan diikuti dengan pernyataan objektif dan skop projek. 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 fungsian dan 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 kritikan dan memastikan aplikasi berfungsi dengan baik tanpa kesilapan. Bahagian ini akan membincangkan kekangan aplikasi dan cadangan untuk penambahbaikan masa hadapan.

Terdapat beberapa batasan aplikasi dan salah satunya termasuk penggunaan minimum penyedia penyimpanan awan. Aplikasi ini akan menggunakan pilihan 3 storan awan kerana kerumitan. Kedua, 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. Proses keselamatan yang merangkumi cincangan, penyulitan dan penghirisan yang dilakukan pada fail yang lebih besar akan menggunakan lebih banyak kuasa. Akhirnya, algoritma penghirisan yang khusus tidak dibincangkan untuk implementasi aplikasi disebabkan kekangan masa.

PENGHARGAAN

Penulis kajian ini ingin ucapkan setinggi-tinggi penghargaan dan jutaan terima kasih kepada Prof. Madya Dr. Elankovan a/l A. Sundararajan, penyelia penulis kajian ini yang telah memberi tunjuk ajar serta bimbingan untuk menyiapkan projek ini dengan jayanya.

Penulis kajian ini juga ingin mengucapkan terima kasih kepada semua pihak yang membantu secara langsung mahupun tidak langsung dalam menyempurnakan projek ini. Segala bantuan yang telah dihulurkan amatlah dihargai kerana tanpa bantuan mereka, projek ini tidak dapat dilaksanakan dengan baik. Semoga tuhan merahmati dan memberikan balasan yang terbaik.

RUJUKAN

- Bhagat, S. A. 2022. Review on mobile application development based on flutter platform. International Journal for Research in Applied Science and Engineering Technology 10(1): 803-809.
- Brenner, R. & Wunder, S. 2015. Scaled Agile Framework: Presentation and real world example. 2015 IEEE Eighth International Conference on Software Testing, Verification and Validation Workshops (ICSTW), pp.1-2.
- Çakıroğlu, M., Cüneyt, B., Ahmet, T. & Özdemir, Ç. 2010. Performance evaluation of scalable encryption algorithm for wireless sensor networks. Scientific Research and Essays 5(9): 856-861.
- Chougale, P., Yadav, V., Gaikwad, A. & Vidyapeeth, B. 2021. Firebase-overview and usage. International Research Journal of Modernization in Engineering Technology and Science 3(12): 1178-1183.
- Dagne, L. 2019. Flutter for cross-platform App and SDK development.
- Fauzan, R., Siahaan, D., Rochimah, S. & Triandini, E. 2019. Use case diagram similarity measurement: A new approach. 2019 12th International Conference on Information & Communication Technology and System (ICTS), pp.3-7.
- Foluwaseyi. n.d. AES Encryption in Flutter Applications. <https://medium.com/@foluwaseyi.dev/aes-encryption-in-flutter-applications-6f6cfc320521> [3 JULY 2025]
- Dart Dev. n.d. *SecretBox* class | *cryptography* package. <https://pub.dev/documentation/cryptography/latest/cryptography/SecretBox-class.html> [3 JULY 2025]
- Dart Dev. n.d. *block* | *Dart Package*. <https://pub.dev/packages/block> [3 JULY 2025]
- Dart Dev. n.d. *encrypt* | *Dart Package*. <https://pub.dev/packages/encrypt> [3 JULY 2025]
- Stack Overflow. 2013. String - Get Real Path For Uri Android – Stack Overflow. <https://stackoverflow.com/questions/17546101/get-real-path-for-uri-android> [28 MAC 2025]
- Gupta, L., 2015. HowToDoInJava. Java File Checksum - MD5 and SHA-256 Hash Example. <https://howtodoinjava.com/java/java-security/sha-md5-file-checksum-hash/> [29 MAC 2025]
- QRA. n.d. Home – QRA. <https://qracorp.com/functional-vs-non-functional-requirements/> [15 NOVEMBER 2024]
- Leffingwell, D., 2021. Scaled Agile Framework. Nonfunctional Requirements, Scaled Agile Framework. <https://www.scaledagileframework.com/nonfunctional-requirements/> [15 NOVEMBER 2024]

www.visual-paradigm.com. n.d. What is Activity Diagram?. <https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-activity-diagram/> [15 NOVEMBER 2024]

www.visual-paradigm.com. n.d. What is Use Case Diagram?. <https://www.visual-paradigm.com/guide/uml-unified-modeling-language/what-is-use-case-diagram/> [15 NOVEMBER 2024]

Zimmermann, R., 2017. Sirius Edge. Mobile Device Security in the Workplace: 5 Key Risks and a Surprising Challenge - Sirius Edge. <https://edge.siriuscom.com/security/mobile-device-security-in-the-workplace-5-key-risks-and-a-surprising-challenge> [17 NOVEMBER 2024]

Android Developers. n.d. Uses SDK, Android Developers. <https://developer.android.com/guide/topics/manifest/uses-sdk-element#ApiLevels> [17 NOVEMBER 2024]

Sneha A/P Murugan (A193005)
Prof. Madya Dr. Elankovan A/L A.Sundararajan
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia