TCRYPT: ALAT PENYULITAN DATA DILINDUNGI KATA LALUAN DENGAN PENGURUSAN KUNCI

SYUKRINA BINTI JAMALUDIN[1]

AZANA HAFIZAH BINTI MOHD AMAN[2]

[1,2]*Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor Darul Ehsan, Malaysia*

ABSTRAK

Dalam era globalisasi moden, perkembangan teknologi berlaku dengan sangat pesat dan menjadi kehidupan seharian bergantung sepenuhnya kepada kemajuan teknologi ini. Teknologi memudahkan pelbagai aktiviti seperti berhubung dengan rakan, membuat pembelian dalam talian dan semuanya hanya di hujung jari. Namun begitu, maklumat dan data peribadi seseorang banyak disimpan di peranti seperti telefon pintar dan juga komputer riba yang terdedah kepada pelbagai ancaman keselamatan seperti akses tanpa kebenaran, kecurian data serta aktiviti penggodaman. Ancaman ini sering berlaku apabila pengguna menggunakan kata laluan yang lemah seperti berkaitan nama, tarikh lahir atau gabungan mudah seperti "123456". Lebih membimbangkan, ada juga pengguna yang menulis kata laluan di tempat terbuka seperti *post-it* pada skrin komputer demi kemudahan mengingati tetapi tindakan ini mendedahkan mereka kepada risiko serangan siber. Akibatnya, penggodam mampu mendapatkan akses kepada data peribadi pengguna dengan mudah. Sehubungan itu, pembangunan alat penyulitan data dapat membantu pengguna menyulitkan dan menyahsulitkan fail atau data peribadi mereka. Penyulitan merupakan teknik penting untuk menjamin keselamatan dan privasi data. Sistem ini menggunakan algoritma *Advanced Encryption Standard* (AES) bagi menjamin kerahsiaan fail. Selain itu, *Password-Based Key Derivation Function 2* (PBKDF2) digunakan untuk menjana kunci penyulitan yang kukuh daripada kata laluan pengguna, dengan penambahan *salt* dan bilangan iterasi tertentu untuk mengurangkan risiko serangan *brute-force*. Ciri tambahan seperti *salting*, semakan kekuatan kata laluan, dan *Two-Factor Authentication* (2FA) turut disertakan untuk memperkukuh keselamatan sistem. Dalam pelaksanaan sistem ini, teknologi seperti *Firebase Authentication, Firebase Firestore*, dan *Firebase Storage* turut digunakan untuk menyokong proses pengesahan pengguna, penyimpanan metadata, dan pengurusan fail yang tersulit secara dalam talian. Dengan ini, pengguna dapat menikmati sistem penyulitan data yang bersifat universal, selamat dan mudah digunakan untuk melindungi maklumat peribadi daripada ancaman digital.

Kata kunci: *post-it,* AES, PBKDF2, *salt,* 2FA, *Firebase Authentication, Firebase Firestore*, *Firebase Storage*.

PENGENALAN

Dalam era digital yang pesat membangun, keselamatan data peribadi dan maklumat sensitif menjadi semakin penting bagi individu dan organisasi. Ancaman seperti pencerobohan data, akses tanpa kebenaran, dan penggodaman telah menunjukkan peningkatan, termasuk insiden besar seperti kebocoran lebih 46 juta data pengguna mudah alih di Malaysia pada tahun 2017 (BBC News, 2017). Situasi ini mendorong kepada keperluan mendesak untuk sistem penyulitan data yang kukuh dan pengurusan kunci yang selamat bagi melindungi maklumat peribadi dalam peranti digital. Sehubungan itu, projek ini membangunkan TCrypt, iaitu sebuah alat penyulitan data dilindungi kata laluan dengan pengurusan kunci, yang bertujuan menyediakan penyelesaian menyeluruh dan mesra pengguna untuk keselamatan digital.

Tujuan utama projek ini adalah untuk membangunkan sistem penyulitan fail yang menggunakan algoritma moden seperti *Advanced Encryption Standard* (AES) bagi menjamin keselamatan maklumat, serta mengintegrasikan pengurusan kunci yang selamat melalui kaedah kriptografi hibrid dan penggunaan perkhidmatan *Key Management Service* (KMS). Projek ini turut menyediakan ciri tambahan seperti pemulihan kata laluan secara selamat menggunakan *two-factor authentication* (2FA) bagi meningkatkan keselamatan keseluruhan sistem. Skop projek ini fokus kepada pembangunan aplikasi mudah alih Android yang digunakan oleh pelajar atau individu yang menyimpan data sensitif. Aplikasi ini juga membenarkan pengguna untuk menyulitkan dan menyahsulitkan fail, namun tidak merangkumi sokongan untuk sistem berskala besar atau perkongsian awan secara langsung.

Projek ini penting kerana penyelesaian sedia ada seperti AxCrypt dan VeraCrypt masih mempunyai kekurangan dari aspek kemudahan penggunaan dan kekangan ciri keselamatan seperti pemulihan kata laluan yang efektif. TCrypt dihasilkan bagi mengatasi kekurangan tersebut dengan menggabungkan pendekatan kriptografi simetri dan asimetri, serta penyelesaian keselamatan yang lebih fleksibel dan intuitif. Kajian ini menyumbang kepada bidang keselamatan siber dengan menawarkan sistem yang praktikal. Ini boleh digunakan dalam kehidupan seharian, dan sesuai untuk individu mahupun organisasi yang prihatin terhadap perlindungan data.

Dari sudut metodologi, projek ini menggunakan model pembangunan *Waterfall*, iaitu pendekatan linear yang melibatkan fasa analisis keperluan, reka bentuk sistem, pembangunan modul, pengujian, pelaksanaan, serta penyelenggaraan. Kaedah ini dipilih kerana kesesuaian alirannya yang jelas dan tersusun, sejajar dengan keperluan pembangunan aplikasi keselamatan. Selain itu, data awal diperoleh melalui soal selidik atas talian untuk mengenal pasti keperluan pengguna terhadap fungsi dan ciri-ciri keselamatan dalam aplikasi penyulitan. Reka bentuk sistem pula dibina berasaskan seni bina *Model-View-Controller* (MVC) yang menyusun komponen secara modul dan memudahkan pengurusan sistem.

Akhir sekali, sistem ini dinilai dari segi keberkesanannya dalam mencapai objektif, mengenal pasti kekangan seperti pengetahuan teknikal dan kos, serta mencadangkan penambahbaikan masa hadapan seperti integrasi awan, sokongan pelbagai platform, dan

pemantauan keselamatan masa nyata. Sistem TCrypt diharap menjadi penyelesaian praktikal dan efektif dalam melindungi data pengguna secara menyeluruh dalam era digital yang semakin mencabar.

METODOLOGI KAJIAN

Metodologi yang digunakan dalam pembangunan projek ini ialah *Waterfall*. Model ini salah satu model pembangunan yang menggunakan pendekatan linear dan berurutan. Setiap fasa perlu diselesaikan sepenuhnya sebelum bergerak ke fasa seterusnya. Dengan ini membolehkan dokumentasi yang lengkap di setiap fasa, memudahkan semakan dan laporan bagi tujuan penilaian. Oleh kerana projek ini melibatkan pembangunan aplikasi mudah alih dengan fungsi penyulitan, penyahsulitan, pengurusan kunci dan lain-lain, ini memastikan setiap modul dapat dibina, diuji dan disahkan secara berperingkat.

Fasa analisis

Fasa ini memberi pemberatan dalam menganalisis keperluan sistem. Dalam fasa ini, keperluan fungsian dan bukan fungsian ditentukan daripada pihak berkepentingan projek ini. Fasa ini juga dijalankan untuk memastikan projek yang dibangunkan mencapai objektif yang telah ditetapkan. Semua maklumat telah dikumpul daripada pengguna melalui soal selidik dan kajian literatur.

Fasa reka bentuk

Fasa reka bentuk merupakan fasa yang menentukan seni bina sistem yang digunakan. Dalam fasa ini, reka bentuk seni bina, pangkalan data, algoritma dan antara muka telah dihasilkan untuk memudahkan proses pembangunan dan memastikan objektif kajian dapat dicapai. Fasa ini melibatkan perancangan struktur *Model-View-Controller* (MVC).

Fasa pembangunan

Fasa ini adalah membangunkan sistem modul-modul menggunakan *Android Studio* dengan bahasa pengaturcaraan *Kotlin* dan *Java*. Tambahan pula, ia integrasi dengan *Firebase Authentication, Firestore* dan *SQLite* untuk penyimpanan data dan kawalan peranan pengguna.

Fasa pengujian

Fasa pengujian merupakan salah satu fasa yang penting dalam pembangunan sebuah aplikasi mudah alih. Hal ini kerana pengujian dijalankan untuk mencari kecacatan, ralat dan kelemahan dalam aplikasi ini. Ujian fungsian dan bukan fungsian dilaksanakan untuk memastikan semua modul berfungsi seperti yang dirancang.

Fasa pelaksanaan

Dalam fasa pelaksanaan, sistem aplikasi TCrypt ini diuji bersama pengguna sebenar dalam bentuk aplikasi prototaip. Penyesuaian dan penambahbaikan dilakukan berdasarkan maklum balas pengguna.

Fasa penyelenggaraan

Apabila ralat dapat dikenal pasti, pembaikan dan pembetulan dapat dilakukan untuk memastikan aplikasi TCrypt yang lancar dengan jayanya dan memastikan pengalaman yang terbaik bagi pengguna. Penambahbaikan akan diteruskan sekiranya sistem ingin dikembangkan ke tahap yang lebih tinggi selepas projek ini selesai.

Kaedah Pengumpulan Data

Terdapat dua kaedah utama digunakan dalam pengumpulan data bagi menyokong pembangunan sistem ini:

1. **Kajian Literatur**
   Kajian di atas artikel jurnal, dan dokumentasi teknikal telah dijalankan untuk memahami konsep penyulitan data, kriptografi hibrid, pengurusan kunci dan kelemahan sistem sedia ada seperti AxCrypt dan VeraCrypt. Kajian ini juga merangkumi algoritma AES serta aplikasi *Firebase* sebagai *backend.*

2. **Soal Selidik Pengguna**
   Soal selidik atas talian diagihkan kepada responden. Soalan tersebut disusun untuk mengenal pasti keperluan pengguna terhadap keselamatan data, pengalaman dalam mengguna aplikasi TCrypt, tahap kesedaran tentang ancaman keselamatan dan keperluan sistem yang mesra pengguna.

Soal selidik ini membolehkan pengumpulan maklumat dengan pantas dan dari kumpulan sasaran yang pelbagai, di samping menjimatkan kos dan masa. Kajian literatur pula penting untuk memastikan pembangunan sistem berdasarkan kepada amalan terbaik dan penyelidikan terdahulu.

Kaedah Analisis Data

1. Analisis Deskriptif Kuantitatif
   Data soal selidik yang berbentuk skala Likert dan pilihan berganda dianalisis menggunakan kaedah taburan kekerapan dan peratusan. Maklumat ini digunakan untuk mengenal pasti keutamaan pengguna terhadap ciri keselamatan dan fungsi sistem yang diperlukan.

2. Analisis Kualitatif
   Maklumat dari kajian literatur dianalisis secara bertema untuk mengenal pasti keperluan teknikal, cabaran keselamatan dan ciri sistem sedia ada. Hasil ini digunakan untuk merancang modul dan algoritma dalam sistem TCrypt.

Majoriti responden menyatakan bahawa mereka tidak menggunakan aplikasi penyulitan secara aktif, tetapi percaya penyulitan adalah penting. Ini menunjukkan keperluan kepada sistem yang lebih mudah digunakan tetapi masih selamat.

Pengukuran dan Alat Ukur

Untuk menilai keberkesanan dan kefungsian sistem TCrypt:

a) Ujian Fungsian
Menguji setiap fungsi sistem seperti log masuk, pendaftaran, penyulitan fail, dan penyahsulitan. Ujian ini memastikan setiap komponen bekerja mengikut keperluan yang ditetapkan.

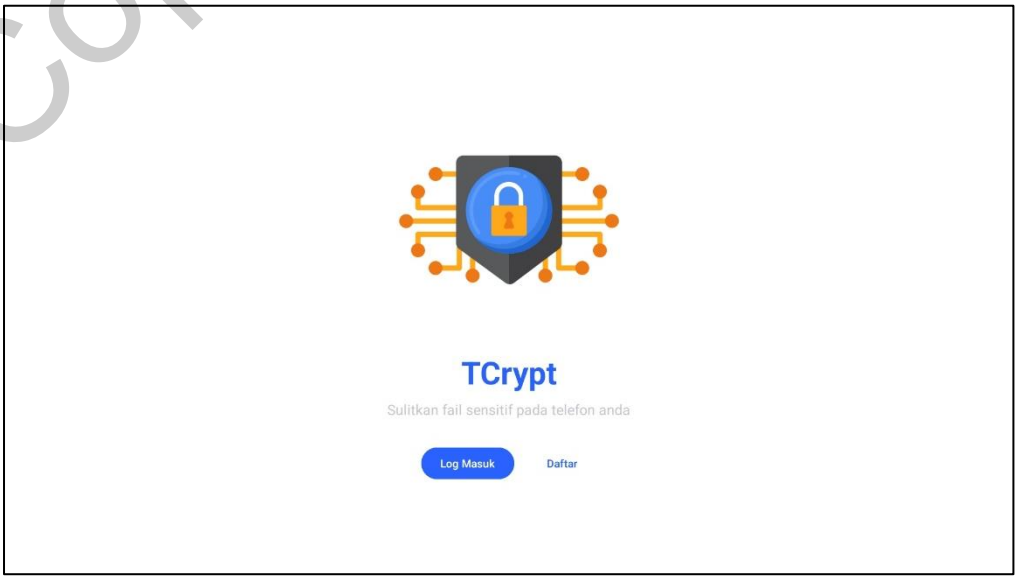
b) Ujian Kebolehgunaan *(Usability Testing)*
Responden mencuba sistem dan memberikan maklum balas melalui borang penilaian. Aspek yang diuji termasuk antara muka, kesenangan penggunaan, kelajuan proses dan kefahaman pengguna.

c) Instrumen Penilaian Pengguna
Borang soal selidik selepas penggunaan sistem mengandungi item-item penilaian seperti tahap kepuasan, persepsi keselamatan, dan kemudahan navigasi. Hasilnya digunakan untuk cadangan penambahbaikan sistem.

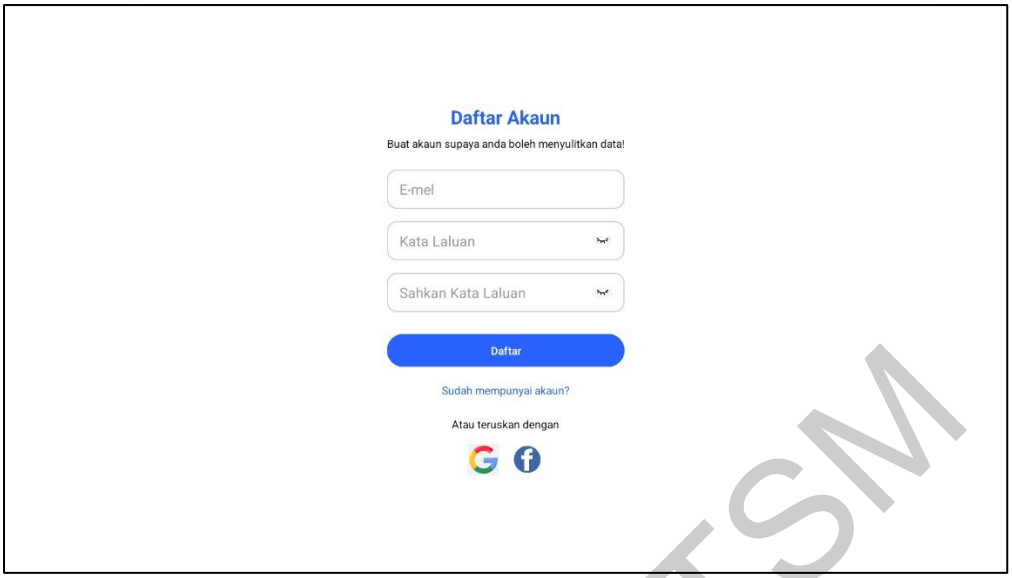
Dengan pendekatan metodologi yang terperinci ini, projek TCrypt dapat dibangunkan secara sistematik dan berasaskan keperluan sebenar pengguna serta prinsip keselamatan maklumat yang kukuh. Ini juga memastikan hasil akhir projek bukan sahaja dapat memenuhi objektif yang ditetapkan, tetapi juga menawarkan penyelesaian praktikal terhadap isu keselamatan digital masa kini.

KEPUTUSAN DAN PERBINCANGAN

Sistem TCrypt telah berjaya dibangunkan dalam bentuk aplikasi mudah alih berasaskan platform *Android*. Aplikasi ini merangkumi beberapa fungsi utama yang telah dilaksanakan dan diuji secara menyeluruh. Antara fungsi utama yang telah berjaya dibangunkan termasuk ciri pendaftaran dan log masuk pengguna yang menggunakan *Firebase Authentication* untuk keselamatan dan kemudahan pengesahan identiti.



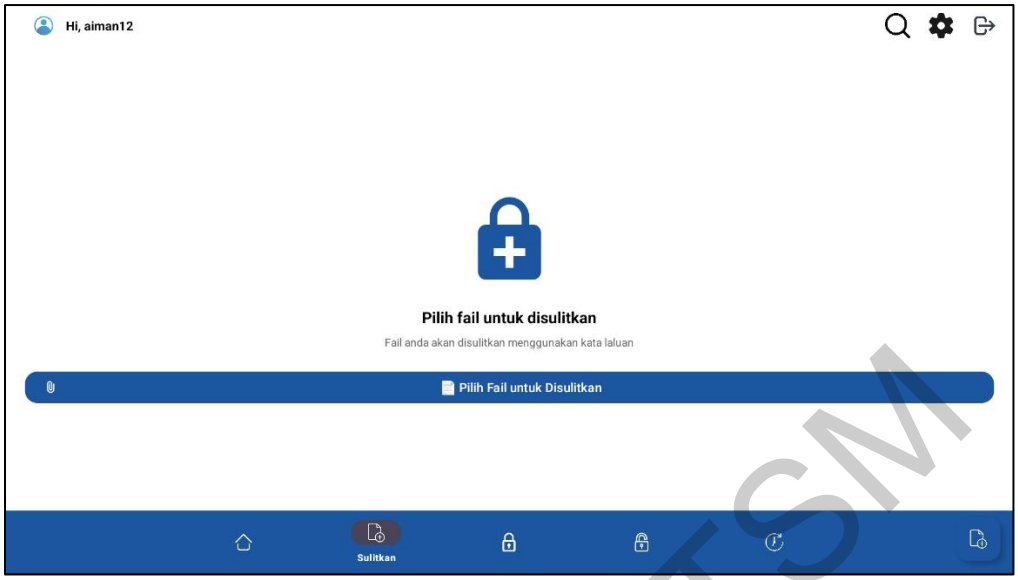
Rajah 1 Antara muka hadapan TCrypt



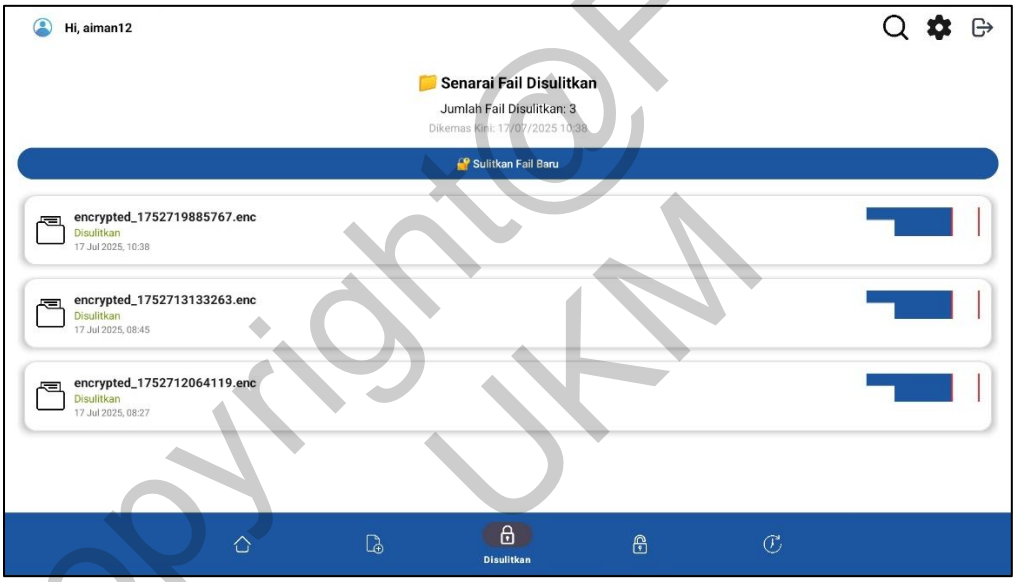
Rajah 2 Antara muka Pendaftaran Akaun

Rajah 3 Antara Muka Log Masuk

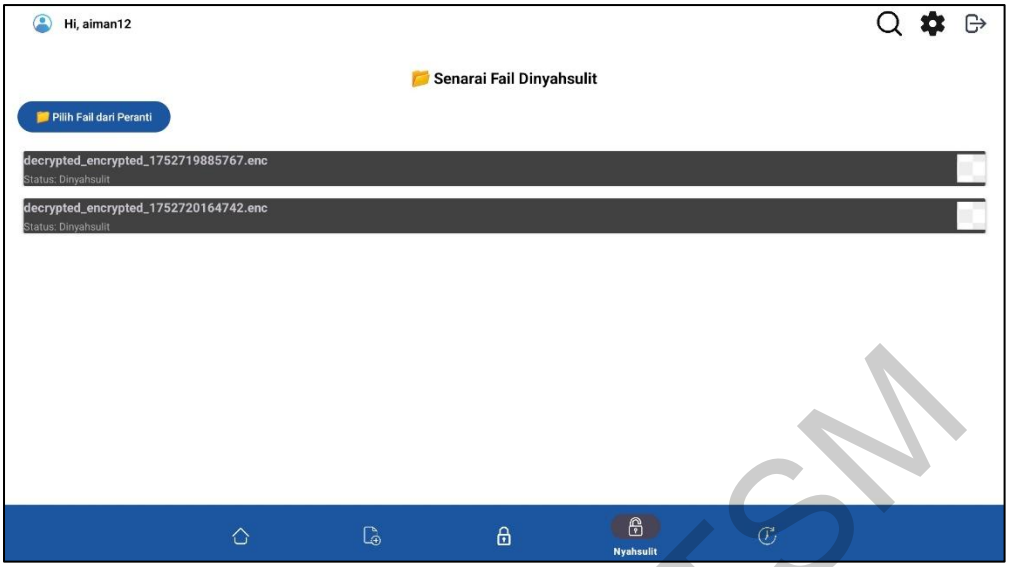
Selain itu, sistem ini menyokong proses penyulitan dan penyahsulitan fail menggunakan algoritma *Advanced Encryption Standard* (AES) yang terbukti kukuh dan efisien dalam melindungi maklumat. Untuk menjamin keselamatan tambahan, kata laluan yang dimasukkan oleh pengguna tidak digunakan secara langsung sebagai kunci penyulitan. Sebaliknya, sistem menggunakan algoritma *Password-Based Key Derivation Function 2* (PBKDF2) untuk menukar kata laluan tersebut menjadi kunci AES yang kuat melalui proses derivasi yang melibatkan penggunaan *salt* dan iterasi berulang. Pendekatan ini dapat mengurangkan risiko serangan *brute-force* dan meningkatkan keselamatan kunci yang dijana.



Rajah 4 Antara Muka Penyulitan



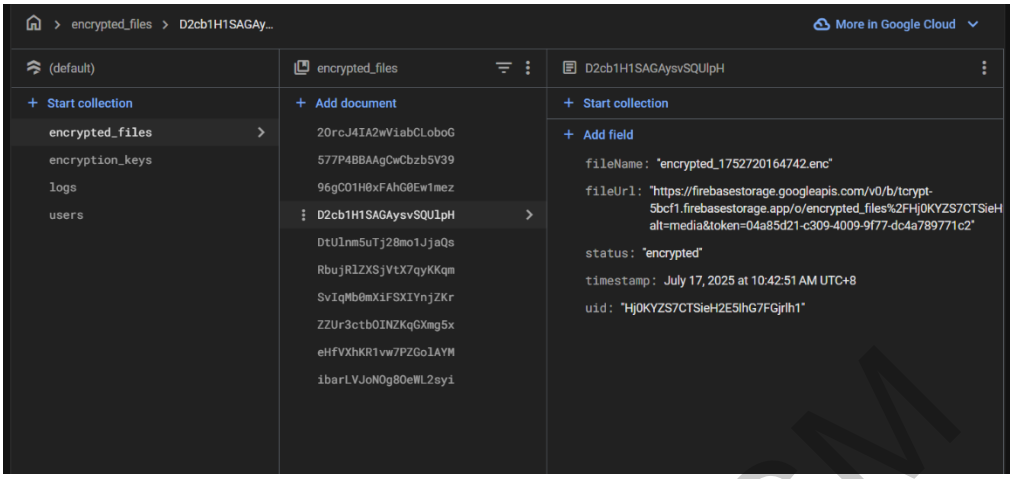
Rajah 5 Antara Muka Senarai Penyulitan



Rajah 6 Antara Muka Penyahsulitan

TCrypt juga mengintegrasikan pengurusan kunci secara selamat melalui pendekatan algoritma AES, membolehkan kunci disimpan dan diurus dengan lebih sistematik. Di samping itu, aplikasi ini menyediakan ciri pemulihan kata laluan yang dilindungi melalui kaedah *two-factor authentication* (2FA) yang meningkatkan tahap keselamatan ketika pengguna ingin mengakses semula akaun mereka. Fail yang telah disulitkan disimpan dengan selamat di *Firebase Storage* manakala metadata berkaitan disimpan dalam *Firestore* bagi memastikan pengurusan fail yang teratur.

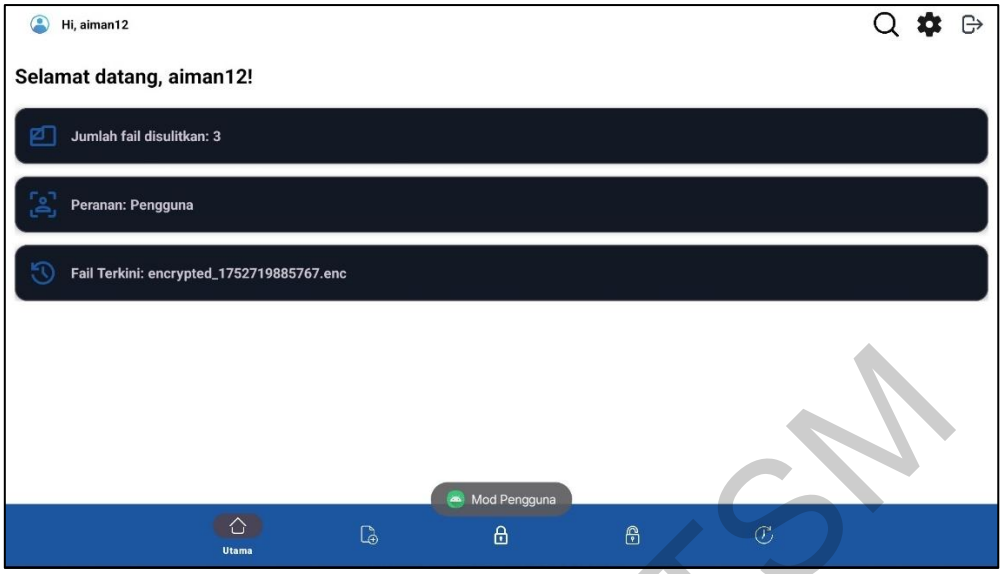
Rajah 7 Antara Muka Pengurusan Kunci



Rajah 8 menunjukkan Firebase Storage

Sistem ini turut menyokong pengasingan peranan pengguna, iaitu antara pengguna biasa (*User*) dan pentadbir (*Admin*), yang diuruskan menggunakan pangkalan data tempatan *SQLite*. Setiap fungsi yang dibangunkan telah diuji dan didapati berfungsi sepenuhnya mengikut spesifikasi sistem.

Rajah 9 Antara Muka terhadap *Admin*



Rajah 10 Antara Muka terhadap *User*

Keputusan ujian fungsian menunjukkan bahawa semua modul utama termasuk pendaftaran, log masuk, penyulitan, penyahsulitan, pengurusan kunci, pemulihan kata laluan dan pengurusan peranan pengguna berjaya dilaksanakan tanpa sebarang ralat yang kritikal. Ini membuktikan bahawa sistem TCrypt berfungsi dengan baik dari segi teknikal dan bersedia untuk digunakan dalam skala yang lebih luas.

Fungsi	**Status Ujian**
Pendaftaran & Log Masuk	Berfungsi
Penyulitan	Berfungsi
Penyahsulitan	Berfungsi
Pengurusan Kunci	Berfungsi
Pemulihan Kata Laluan	Berfungsi
Kawalan Peranan Pengguna	Berfungsi

Analisis Keputusan

Hasil ujian menunjukkan bahawa sistem TCrypt berfungsi sepenuhnya dan memenuhi objektif kajian yang telah ditetapkan. Fungsi penyulitan dan penyahsulitan fail menunjukkan kecekapan masa dan keselamatan yang baik, dengan fail yang dilindungi tidak boleh dibuka tanpa kata laluan yang sah. Modul pengurusan kunci berjaya menyimpan dan mengurus kunci dengan selamat, serta menyokong pemulihan kata laluan dengan tahap keselamatan tambahan melalui 2FA.

Maklum balas daripada pengguna menunjukkan bahawa antara muka aplikasi

dianggap mudah digunakan dan difahami. Majoriti responden juga menyatakan bahawa mereka berasa lebih yakin terhadap keselamatan data peribadi apabila menggunakan sistem ini. Ini menunjukkan bahawa TCrypt bukan sahaja berfungsi secara teknikal, tetapi juga diterima dari segi kebolehgunaan.

Perbandingan dengan Kajian Terdahulu

Sistem TCrypt ini dibandingkan dengan aplikasi penyulitan sedia ada seperti VeraCrypt dan AxCrypt.

Ciri	**VeraCrypt**	**AxCrypt**	**TCrypt**
Penyulitan	Ya	Ya	Ya
Pemulihan kata laluan	Tiada	Tiada	Ada
Two-Factor Authentication (2FA)	Tiada	Tiada	Ada
Mesra pengguna	Sederhana	Mesra	Mesra
Platform sokongan	Windows, macOS and Linux	Windows, macOS, Android, IOS	Android, IOS

TCrypt mengatasi kekangan aplikasi lain dengan menambahkan ciri keselamatan tambahan iaitu 2FA, kebolehan pemulihan kata laluan dan antara muka mudah alih yang mesra pengguna. Kekuatan ini menjadikan TCrypt lebih fleksibel dan sesuai digunakan oleh pengguna moden, terutamanya pengguna telefon pintar.

Penjelasan Terhadap Keputusan

Keputusan yang diperoleh menunjukkan bahawa pendekatan kriptografi hibrid (AES untuk penyulitan fail dan RSA untuk pengurusan kunci) merupakan kaedah yang efektif dalam menjamin kerahsiaan data. Selain itu, penggunaan *Firebase Storage* dan *Firestore* membolehkan penyimpanan data secara selamat di awan, manakala integrasi *SQLite* membolehkan pengurusan peranan pengguna secara tempatan.

Penggunaan metodologi *Waterfall* juga menyumbang kepada pembangunan sistem yang teratur dan terancang. Setiap modul dibangunkan secara berperingkat dan diuji secara sistematik. Penggunaan alat pengujian fungsian dan borang soal selidik pasca-penggunaan turut memberi sokongan kepada penilaian objektif keberkesanan sistem.

Implikasi dan Kesimpulan

Hasil kajian ini menunjukkan bahawa sistem penyulitan fail yang dilengkapi dengan pengurusan kunci, pemulihan kata laluan, dan pengesahan dua faktor dapat meningkatkan

keselamatan data peribadi secara signifikan. Sistem seperti TCrypt boleh dimanfaatkan dalam pelbagai konteks seperti perlindungan maklumat pengguna, keselamatan fail organisasi, atau pelaksanaan standard keselamatan dalam aplikasi mudah alih.

Implikasi terhadap industri keselamatan maklumat adalah positif kerana pendekatan ini selaras dengan amalan terbaik siber semasa. Bagi bidang akademik pula, projek ini menyumbang kepada pemahaman terhadap reka bentuk sistem keselamatan yang terjamin antara keselamatan dan kebolehgunaan.

Cadangan untuk Kajian Masa Hadapan

Walaupun sistem TCrypt telah berjaya dibangunkan dan diuji, masih terdapat beberapa kekangan serta ruang penambahbaikan yang boleh diselidik dalam kajian masa hadapan. Antaranya ialah pengembangan sistem ke platform lain seperti versi web bagi membolehkan akses merentas peranti dan sistem operasi. Selain itu, fungsi penyulitan berkelompok boleh ditambah bagi membolehkan pengguna menyulitkan beberapa fail secara serentak, sekali gus menjimatkan masa dan meningkatkan kecekapan. Ciri pemantauan keselamatan masa nyata juga boleh diterapkan, seperti integrasi log audit atau sistem pengesanan pencerobohan, bagi membolehkan pentadbir memantau aktiviti mencurigakan secara langsung. Tambahan pula, sistem boleh dikembangkan dengan ciri awan selamat yang menyokong kerjasama antara pengguna, di mana fail disulitkan secara automatik sebelum dikongsi. Kajian akan datang juga boleh memberi tumpuan kepada mengoptimumkan prestasi dari segi saiz fail, kelajuan proses penyulitan, serta penggunaan memori dan bateri peranti, agar aplikasi lebih ringan, pantas dan sesuai digunakan dalam pelbagai keadaan.

Kajian masa hadapan juga boleh menumpukan kepada meningkatkan prestasi dan penggunaan sumber, terutamanya dari segi saiz fail, kelajuan penyulitan, dan penggunaan memori.

KESIMPULAN

Secara keseluruhannya, projek pembangunan sistem TCrypt telah berjaya dilaksanakan dan mencapai objektif yang ditetapkan. Sistem ini direka bentuk untuk menyulitkan data secara selamat dengan menggunakan kombinasi teknologi penyulitan moden seperti algoritma AES dan pengurusan kunci. Keputusan daripada ujian menunjukkan bahawa semua fungsi utama sistem termasuk pendaftaran, log masuk, penyulitan, penyahsulitan, dan pengurusan kunci telah berfungsi dengan baik tanpa ralat, serta diterima baik dari sudut kebolehgunaan oleh pengguna.

Objektif utama projek ini, iaitu membangunkan aplikasi penyulitan data mudah alih yang dilindungi kata laluan dan menyokong pemulihan kata laluan serta pengasingan peranan pengguna, telah berjaya dicapai. Tambahan pula, ciri tambahan seperti *Two-Factor Authentication* (2FA) dan antara muka yang mesra pengguna telah memberikan nilai tambah kepada sistem yang dibangunkan. Hal ini menunjukkan bahawa pendekatan yang diambil adalah berkesan dari segi teknikal dan praktikal.

Hasil kajian ini memberikan implikasi positif kepada bidang keselamatan maklumat, terutamanya dalam konteks perlindungan data peribadi pengguna peranti mudah alih. Sistem TCrypt boleh dijadikan sebagai model penyelesaian keselamatan digital yang seimbang antara keselamatan, fungsi dan kemudahan penggunaan. Dalam konteks industri, ia membuka peluang kepada pembangunan aplikasi keselamatan berasaskan pengguna biasa yang tidak memerlukan pengetahuan teknikal mendalam.

Namun begitu, terdapat beberapa kekangan yang dikenal pasti sepanjang pembangunan, antaranya ialah kekangan platform terhad kepada *Android* dan *IOS* sahaja, serta kekangan dari segi masa dan sumber bagi menjalankan ujian dalam skala yang lebih besar. Oleh itu, cadangan untuk kajian masa hadapan termasuk memperluaskan aplikasi ke platform lain seperti web, menambah ciri pemantauan keselamatan masa nyata, dan meningkatkan prestasi sistem dari segi kelajuan serta penggunaan sumber. Secara ringkasnya, TCrypt berjaya dibangunkan sebagai sistem penyulitan fail yang selamat, fleksibel dan sesuai digunakan oleh pengguna harian. Ia bukan sahaja mencapai objektif kajian, malah berpotensi untuk dikembangkan lebih jauh sebagai penyelesaian keselamatan digital yang kukuh dan mesra pengguna dalam era digital yang semakin mencabar.

PENGHARGAAN

Penulis kajian ini ingin ucapkan setinggi-tinggi penghargaan dan jutaan terima kasih kepada Dr. Azana Hafizah Binti Mohd Aman, 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

Authentication | React Native Firebase. (n.d.). https://rnfirebase.io/auth/usage

BBC News. (2017, October 31). *Malaysian data breach sees 46 million phone numbers leaked*. https://www.bbc.com/news/technology-41816953

Block, S. (2024, November 10). *Kerckhoff principle - Kerckhoff & Cryptography - Maxime von Kerckhoff*. Rock the Prototype - Softwareentwicklung & Prototyping. https://rock-the-prototype.com/en/cryptography/kerckhoff-principle/

Ciernikova. T. 2022. Selected open tools supporting security and privacy protection for regular end-users (Bachelor's thesis). Masaryk University, Faculty of informatics.

Firebase. (n.d.). *Firebase*. https://firebase.google.com/

GeeksforGeeks. (2025, January 3). *MVC Design pattern*. GeeksforGeeks. https://www.geeksforgeeks.org/system-design/mvc-design-pattern/

Kirvan, P., Lutkevich, B., & Lewis, S. (2024, November 15). *What is a Waterfall model? Definition and guide*. Search Software Quality. https://www.techtarget.com/searchsoftwarequality/definition/waterfall-model

What is VeraCrypt? (n.d.). https://cyberpedia.reasonlabs.com/EN/veracrypt.html

Welekwe, A., & Welekwe, A. (2025, February 17). *AxCrypt review and Alternatives*. Comparitech. https://www.comparitech.com/net-admin/axcrypt-review/

Petras, B. (2023). What is password encryption, and how does it work?. https://nordvpn.com/blog/what-is-password-encryption/

Rae PullRequest. (2024, January 19). *Understanding the Benefits of Key Derivation Functions: A Deep Dive into PBKDF2*. *PullRequest*. https://www.pullrequest.com/blog/understanding-the-benefits-of-key-derivation-functions-a-deep-dive-into-pbkdf2/

Syukrina Binti Jamaludin (A193647)
Dr. Azana Hafizah Binti Mohd Aman
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia