AUTOMASI KESELAMATAN E-MEL DALAM BENTUK SAMBUNGAN GOOGLE

AIMI AYUNI BINTI SHAMSUDIN

TS. DR. WAN FARIZA BINTI PAIZI@FAUZI

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

ABSTRAK

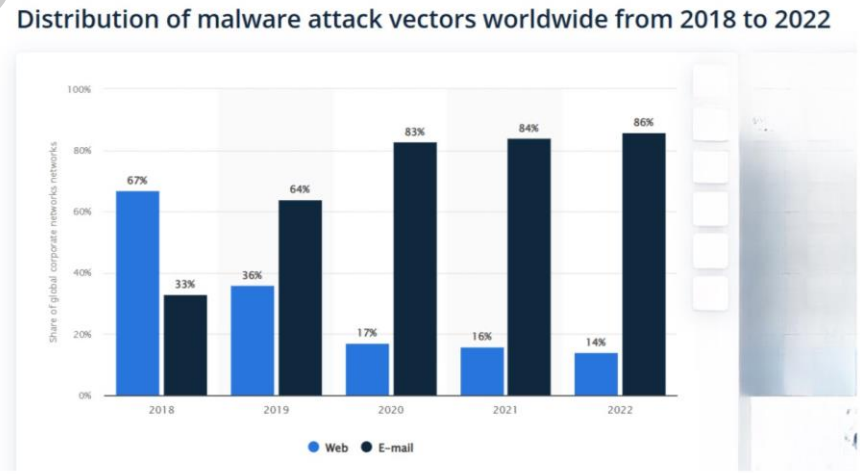
Tidak dapat dinafikan Gmail adalah sebahagian daripada sistem perisian Google (Google extension) sehingga ia disepadukan dengan pelbagai produk dan perkhidmatan lain. Akibatnya, pautan e-mel mereka terdedah secara meluas kepada perkhidmatan yang membuka ruang kepada penggodam beretika dan pakar IT untuk cuba menggodam maklumat peribadi mereka. Penggodam akan mencuba pelbagai cara untuk memasuki ke e-mel pengguna, seperti menghantar perisian hasad melalui kegagalan lampiran, menghantar janji ganjaran yang membolehkan pengguna menghantar e-mel maklumat bank peribadi mereka dan menyamar sebagai pengguna untuk mendapatkan maklumat mereka dengan mudah. Artikel oleh Drake Bennett (2022), mengatakan bahawa seorang pengintip dari China telah menggunakan Gmail dan iCloud untuk menggodam rahsia perdagangan korporat. Pengintipan dari China ini datang pada masa AS dan Eropah membincangkan risiko keselamatan perkakasan China daripada Huawei Technologies Co., dan platform teknologi China Tiktok melihat betapa banyak pengintip China ini bergantung kepada Apple Inc. dan Alphabet Inc. Google. Untuk mengukuhkan keselamatan e-mel dalam Gmail, projek ini bercadang untuk melindungi akaun e-mel pengguna dengan membina keselamatan automatik melalui sambungan Google (Google extension). Ia boleh menjadi mimpi ngeri keselamatan apabila perisian hasad, perisian pengintip dan penjejak berasaskan penyemak imbas yang cuba menceroboh privasi dan keselamatan pengguna. Dengan menggunakan sambungan Google (Google extension), pengguna boleh menambahkannya terus ke penyemak imbas mereka dari penjuru kanan sebelah atas Chrome, membolehkan mereka mengakses tetapan mereka dengan mudah. Automasi keselamatan e-mel akan menyekat iklan dan penjejak, perisian hasad dan tapak penipuan untuk menghalang sebarang kandungan dan aktiviti yang berniat jahat atau tidak diingini daripada memberi kesan kepada Gmail anda. Ia menggunakan gabungan alat pembangunan web, seperti Persekitaran Pembangunan Bersepadu (IDE), iaitu Visual Studio Code dan Sublime Text, yang akan menjadi penyunting teks untuk menulis dan mengedit kod. Seterusnya, untuk menguji keselamatan sambungan Google, alatan seperti Google API Explorer akan digunakan untuk menentukan keberkesanannya dan memastikan sambungan Google (Google extension) bersambung dalam persekitaran Gmail. Oleh itu, tujuan projek ini adalah untuk meningkatkan keselamatan pengguna dan membantu pengguna menjimatkan

masa dengan mengoptimumkan prestasi e-mel, kebolehhantaran dan penglibatan mereka di Gmail. Selain itu, ia memastikan komunikasi yang lebih berkesan antara pengguna tidak mudah dipintas atau diubah oleh penggodam.

PENGENALAN

Perkembangan teknologi informasi membuat layanan berkirim pesan dapat dilakukan dengan pantas dan efisien melalui e-mel. Kebanyakan aplikasi yang digunakan untuk memudahkan seseorang berkirim pesan adalah Yahoo Mail, Outlook, Gmail dan lain-lain. Gmail telah berevolusi membantu pengguna dalam berkomunikasi, mendapatkan notifikasi serta mendapatkan informasi. Melalui artikel (20+ Gmail Statistics to Know, 2021), pengguna yang menggunakan Gmail secara aktif adalah sebanyak 1.5 billion sekitar tahun 2018 pada rajah 1 Hal ini juga, menyebabkan lebih daripada 10 juta pengguna telah menerima mesej spam dan e-mel berniat jahat secara berterusan tetapi dapat disekat secara automatik melalui Google's anti-abuse machine pada setiap hari.

Walaupun *Gmail* telah menyediakan pelbagai fitur keselamatan untuk melindungi maklumat pengguna, masih terdapat kebimbangan mengenai keselamatan yang ditawarkan memandangkan *Gmail* mempunyai popularity dalam kalangan pengguna. Daripada artikel (Sudeep, 2022), *ThreatLabz* telah menganalisis mengenai serangan pancingan data *adversary-in-the-middle* (AitM) yang mensasarkan pengguna perusahaan *Gmail*. Serangan itu mampu memintas perlindungan pengesahan berbilang factor (*MFA*) *Gmail* dengan menghantar e-mel kepada eksekutif *CEO* untuk melakukan serangan pancingan data oleh aktor ancaman. Antara kebimbangan yang ditemui dalam *Gmail* adalah serangan pancingan data, perisian hasad, rampasan akaun, penipuan e-mel dan akses tanpa kebenaran. Kebimbangan ini akan memberi kemudaratan kepada pengguna yang menggunakan *Gmail* ini sebagai alat komunikasi utama mereka. Bukan itu sahaja, prestasi kerja pengguna juga terjejas serta maklumat peribadi yang telah diceroboh menyebabkan pengguna mengalami kerugian kewangan serta mendatangkan tekanan emosi pengguna.



Rajah 1 Menunjukkan perbandingan perisian hasad melalui email dan web

Sumber: Petrosyan, A. 2023

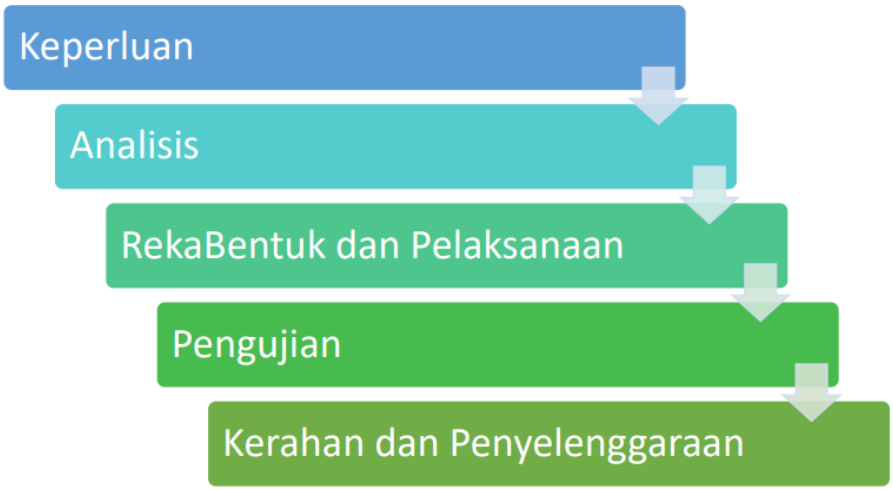
Bagi meningkatkan lagi keselamatan dalam persekitaran email, pembinaan automasi keselamatan melalui sambungan *Google* (*Google extension*) telah dibangunkan dalam projek ini. Sambungan *Google* ini dapat membantu dalam melindungi data pengguna dan bebas daripada serangan pepijat dan perisian hasad. Seterusnya, untuk mendapatkan perlindungan yang lebih lanjut sambungan *Google* akan menyediakan beberapa fitur seperti pengimbasan pautan serta lampiran muat turun dan muat naik fail, pengesanan unsur pancingan data dan keselamatan e-mel yang tertumpu kepada produktiviti. Oleh itu, sambungan *Google* ini meningkatkan tahap keselamatan pengguna *Gmail* sebagai alat utama komunikasi secara atas talian.

METODOLOGI KAJIAN

Untuk menjayakan sebuah projek yang kompleks adalah penting untuk menggunakan rangka kerja pengurusan projek seperti kaedah Air Terjun, kaedah Tangkas, Pengaturcaraan Ekstrem dan Pembangunan Aplikasi Pantas (RAD) bagi menyelaraskan keseluruhan proses mencipta sesebuah projek yang berkesan.

Bagi membangunkan automasi keselamatan email dalam bentuk sambungan *Google*, rangka pengurusan projek yang digunakan adalah kaedah Air Terjun. Kaedah Air Terjun merupakan pendekatan yang mengutamakan fleksibiliti dalam mengerjakan sebuah perisian yang akan berfungsi dengan kerap dan bukannya hanya memfokuskan pada dokumentasi komprehensif sahaja.

Berdasarkan artikel (Ben, 2023), penggunaan metodologi Air Terjun bukan sahaja membantu dalam kecekapan operasi namun ia memberikan satu transformasi yang menyelaraskan setaip kepentingan bagi memastikan perjalanan operasi berjalan dengan sempurna. Malah, mengamalkan konsep Air Terjun menyebabkan syarikat mengalami pertumbuhan sebanyak 60 peratus dalam menghasilkan keuntunga



Rajah 2 Merupakan sebuah rajah metodologi bagi kaedah Air Terjun

Fasa 1: Keperluan

Fasa ini amat penting bagi mengetahui dan mengenalpasti objektif kajian dan menitikberatkan ciri-ciri yang diperlukan melalui perbincangan bersama penyelia. Antaranya adalah dengan mengumpulkan maklumat ancaman-ancaman yang telah dihadapi oleh pengguna apabila menggunakan e-mel melalui pembacaan. Pelbagai artikel, jurnal dan kajian lepasan telah dikumpulkan bagi mengetahui dengan lebih mendalam berkenaan keselamatan di e-mel melalui sambungan Google. Pembacaan yang dilakukan di Google Scholar membantu dalam mengumpulkan data-data yang kukuh berkenaan perisian hasad dan kebocoran maklumat pengguna melalui e-mel. Selain itu, 5 sambungan Google akan dipilih secara manual untuk menganalisa kelemahan dalam setiap sambungan. Pengumpulan maklumat ini akan membantu dalam meneliti pembinaan fungsi yang berkesan untuk pengguna seperti melihat perbezaan API dalam setiap sambungan.

Fasa 2: Analisis

Fasa ini dijalankan setelah analisa dikenalpasti bagi memenuhi keperluan objektif kajian. Setelah mengumpulkan data untuk keperluan pengguna, kajian ini akan memfokuskan dalam membina keselamatan automasi melalui sambungan Google untuk mengatasi serangan siber iaitu perisian hasad, penipuan dan pancingan data. Pembangun akan meneliti cara yang terbaik bagi mementingkan keselamatan seperti membina pengimbasan lampiran dan menyekat ancaman seperti pancingan data. Aplikasi HTML, JavaScript telah dicadangkan melalui beberapa kajian untuk digunakan bagi memasukkan data yang dikumpul dan dipercayai bagi membina skrip kandungan keselamatan yang optimum. Oleh itu, perancangan ini akan memutuskan ciri-ciri yang perlu diutamakan dan menganggarkan proses yang diperlukan untuk menyelesaikan masalah serta mencapai setiap objektif dengan berkesan.

Fasa 3: Reka Bentuk dan Pelaksanaan

Dalam fasa ini, penyelesaian ancaman-ancaman yang dikenal pasti akan dibentuk bagi memenuhi keperluan pengguna. Dengan mereka bentuk sambungan Google ini, ia akan mengesan sebarang pancingan data atau perisian hasad yang diterima melalui fail lampiran dengan menyekat ancaman tersebut melalui mekanisme antara muka pengaturcaraan aplikasi (API). Seterusnya, pembangun akan menerapkan had kebenaran dalam mencapai pautan sah apabila fail tersebut membawa pengguna kepada laman web yang tidak sah. Sebagai contoh, kod yang akan diimplementasi iaitu "permissions": ["activeTab", "storage", "https://example.com/"], penyerang hanya boleh menggunakan kebenaran yang telah ada pada sambungan sahaja kerana mereka tidak dapat mengubah suai data atau mendapat akses data pengguna Ia membantu dalam mengehadkan dan menghalang penyerang daripada mendapat akses tanpa had kepada data pengguna.

Fasa 4: Pengujian

Seterusnya melalui fasa pengujian ini, ia membantu dalam membuat penilaian sejauh mana pembangunan keselamatan sambungan Google ini berkesan kepada pengguna. Fasa ini akan melakukan pengujian setelah sebahagian kod telah dibaiki dan dikerjakan agar kelemahan kod dapat dikesan dengan pantas. Fasa ini akan menggunakan Test Driven Development (TDD) yang merupakan sebuah pendekatan pembangunan perisian yang ditulis sebelum pelaksanaan

kod yang sebenar. Proses ini mengikuti kitaran yang pendek dengan memfokuskan tiga langkah utama iaitu menulis kes ujian yang gagal, menulis jumlah minimum kod untuk lulus ujian dan memfaktorkan semula kod untuk menambah baik reka bentuk perisian. Secara ringkas, ujian ini diuji terlebih dahulu dan jika terdapat sebarang kegagalan maka kod yang baharu akan ditulis untuk melepasi ujian dan menjadikan kod bebas daripada pepijat. Ujian ini juga dijalankan bagi memastikan persekitaran projek mencapai keperluan pengguna dan tersedia untuk dimuat turun dan dipasang dalam Chrome.

Fasa 5: Kerahan dan Penyelenggaraan

Setelah pengujian diselesaikan, pengguna boleh mula menggunakan hasil yang dimuat naik oleh pembangun sebagai sebuah kajian yang lengkap. Dalam fasa ini, perkembangan sambungan Google ini telah berjaya dibangunkan mengikut keperluan objektif pengguna. Pembangun akan mengumpulkan data daripada pengguna secara berperingkat sekiranya terdapat masalah apabila mengimplementasikan hasil tersebut. Akhir sekali, pemantauan dari semasa ke semasa akan dibuat supaya pembangun juga akan sentiasa mengemas kini ciri-ciri keselamatan yang diperlukan oleh pengguna.

KEPUTUSAN DAN PERBINCANGAN

Melalui hasil kajian yang telah dilakukan, jadual perbandigan antara sambungan yang sedia ada telah dibina, Hal ini memastikan, jurang kajian telah dibuat dan memahami perbezaan setiap sambungan yang sedia ada untuk dijadikan rujukan dalam membangunkan CipherShield ini.

Dasar keselamatan secara sambungan web ini memainkan peranan penting dalam menambah lapisan keselamatan e-mel pengguna. FlowCrypt, VirusTotal, OPSWAT, Giant Sentinel dan XQ Secure Gmail merupakan sambungan yang berbeza dalam menawarkan fitur-fitur keselamatan yang memainkan peranan dalam melindungi maklumat sensitif pengguna. FlowCrypt telah menonjolkan fungsi utamanya yang menyediakan penyulitan hujung-ke-hujung untuk pengguna Gmail begitu juga dengan XQ Secure Gmail yang menawarkan fungsi penyulitan, kawalan akses dan perlindungan terhadap pancingan data, perisian hasad dan penipuan. Namun, FlowCrypt menggunakan kadar keselamatan automasi serta membenarkan penyulitan terhadap lampiran fail yang besar berbanding dengan XQ Secure Gmail yang tidak menyediakan fungsi tersebut. Kadar keberkesanan mereka yang sama mengkhususkan kepada pengguna yang ingin melakukan e-mel yang sulit berbanding mengesan ancaman seperti pancingan data.

Seterusnya, bagi sambungan VT4Browser yang mempunyai fungsi utama dalam pengimbasan fail dan URL merentasi pelbagai pelayar web. Sambungan ini juga menyediakan automasi dalam pengimbasan fail dan URL bagi meningkatkan kecekapan dalam mengesan ancaman yang sejajar dengan objektif pembinaan projek ini. Namun, sambungan ini menyediakan tahap keselamatan yang sederhana apabila mengenal pasti unsur berniat jahat dalam lampiran e-mel kerana VT4Browser ini tidak hanya tertumpu dalam menyumbang

pengimbasan lampiran di e-mel sahaja. Selain itu, sambungan lain iaitu OPSWAT turut mengambil pendekatan khusus dalam menyediakan keselamatan yang lanjut kepada e-mel. Ia telah melakukan keselamatan automatik dengan menganalisis kandungan dan pengimbasan berterus bagi melindungi ancaman seperti pancingan data, perisian hasad dan penipuan melalui analisi lampiran e-mel. Tetapi, OPSWAT yang mempunyai potensi keselamatan yang tinggi menyebabkan kerumitan dalam penyelesaian keselamatan yang menghalang organisasi yang kecil atau pengguna yang tidak mahir teknologi untuk menggunakannya. Malah, OPSWAT ini memerlukan sumber keselamatan yang banyak untuk mengoptimumkan penyelesaian e-mel yang mempunyai lampiran fail.

Paling ketara antara 5 buah sambungan ini adalah terhadap jurang automasi. XQ Secure *Gmail*, Giant Sentinel dan FlowCrypt tidak mempunyai sebarang ciri automasi dalam mengendali mengesan ancaman melalui pengimbasan fail manakala VT4Browsers dan OPSWAT mempunyai automasi keselamatan namun terdapat jurang yang besar antara 2 sambungan tersebut. Automasi VT4Browsers tertumpu pada pengimbasan fail dan URL pelbagai aplikasi dan pelayar web manakala automasi bagi OPSWAT khusus untuk keselamatan e-mel. Automasi OPSWAT disepadukan secara mendalam menyediakan langkah keselamatan automatik komprehensif yang disesuaikan untuk e-mel berbanding API VirusTotal yang membolehkan penyepaduan ke dalam sistem yang membenarkan proses pengimbasan automatik.

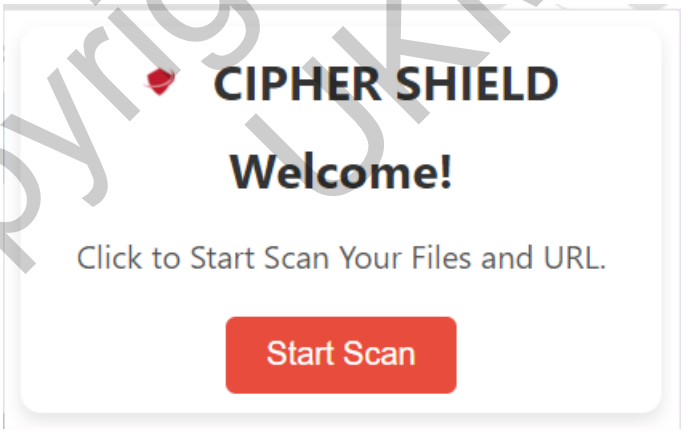
Mengikut kadar keselamatan yang ditawarkan oleh sambungan yang di atas, FlowCrypt dan XQ Secure *Gmail* menawarkan tahap keselamatan e-mel yang asas dan sederhana manakala OPSWAT, VT4Browser dan Giant Sentinel berupaya dalam mengesan ancaman lanjutan dan lebih cenderung memberikan kadar keselamatan yang lebih tinggi dalam *Gmail* kerana mereka menawarkan perlindungan yang lebih kukuh terhadap ancaman seperti pancingan data, perisian hasad dan penipuan melalui analisis kandungan lampiran e-mel serta pengimbasan yang berterusan.

Jadual 1 Perbandingan Alat Sambungan

Jenis Sambungan	**FlowCrypt**	**VT4Browser**	**OPSWAT**	**Giant Sentinel**	**XQ Secure *Gmail***
Fungsi Utama	Menyediakan penyulitan untuk e-mel dan lampiran fail serta memastikan kandungan kekal sulit dan dilindungi daripada pancingan data.	Membenarkan pengguna mengimbas fail atau URL untuk berkemungkinan perisian hasad atau ancaman menggunakan perkhidmatan VirusTotal.	Memberikan perlindungan menyeluruh terhadap ancaman seperti pancingan data, perisian hasad dan kandungan yang berniat jahat.	Menawarkan keselamatan siber yang komprehensif melalui perkhidmatan risikan, pemantauan dan tindak balas ancaman.	Meningkatkan keselamatan dalam e-mel dengan menawarkan penyulitan, kawalan akses atau lapisan tambahan.
Kaedah Konfigurasi Keselamatan	Automasi	Automasi	Automasi	Automasi	Tiada
Bahasa Pengaturcaraan	*HTML*, JavaScript dan CSS.	JavaScript, *HTML*, dan APIs	Python, C++ dan Java	Python, Java	JavaScript, *HTML* dan CSS
Jenis API yang digunakan	*Gmail* API	VirusTotal Public API	MetascanApiKey, API keys	*Gmail* API	*Gmail* API
Pengesanan melalui lampiran fail	Tiada	Ada	Ada	Ada	Tiada
Kadar Keberkesanan	Berkesan untuk pengguna yang ingin menyulitkan mesej dan lampiran fail mereka dengan lancar	Berkesan untuk pengguna yang bimbang akan keselamatan fail atau pautan yang diterima di dalam talian.	Berkesan untuk pengguna atau organisasi yang menyediakan keselamatan e-mel yang komprehensif untuk melindungi ancaman di e-mel.	Berkesan dalam menyediakan ancaman lanjutan dan keupayaan tindak balas yang pantas.	Berkesan memberi perlindungan tambahan dalam e-mel namun tidak menyediakan keselamatan secara automasi.
Tahap Keselamatan	Sederhana	Tinggi	Tinggi	Sederhana	Rendah

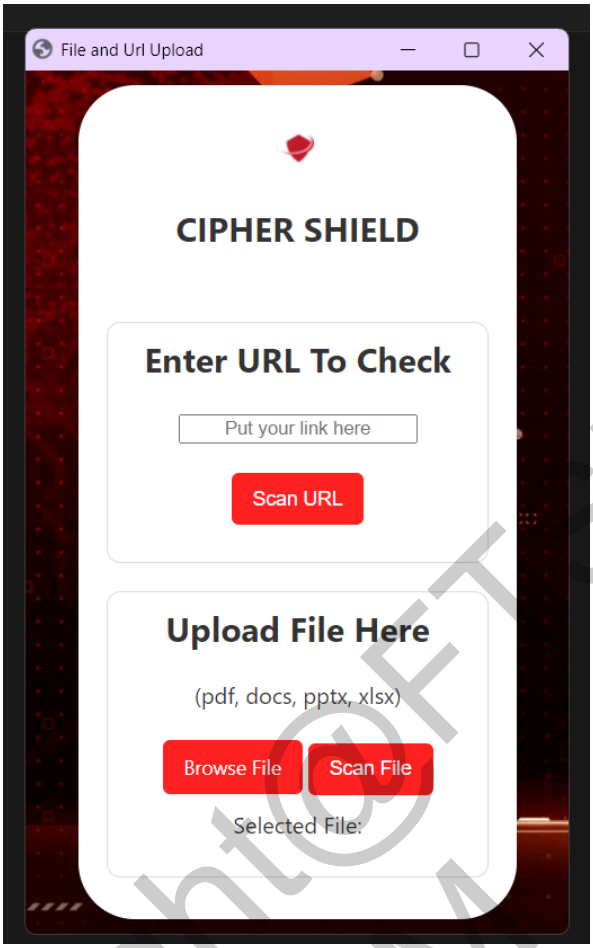
Oleh itu, cadangan penyelesaian yang dapat dibuat berdasarkan kajian kesusasteraan dibuat bagi meningkatkan tahap keselamatan pengguna di e-mel. Antara pembinaan yang dibuat oleh pembangun adalah pembinaan sistem sambungan CipherShield.

Pelaksanaan sistem sambungan CipherShield menyatupadukan fungsi dalam menguatkan infrakstruktur e-mel dalam menghadapi serangan siber. Intergasi dalam sambungan ini dapat mengesan serangan pancingan data, perisian hasad dengan membuat analisis kandungan e-mel dan pengimbasan lampiran yang di muat turun dan pautan oleh pengguna. Bukan itu sahaja, sekiranya pengimbasan fail dan pautan yang dibuat berjaya mengesan sebarang perisian hasad, sambungan menyekat akses tersebut bagi memastikan pautan atau fail yang berniat jahat tidak dibuka oleh pengguna. Pengesanan pancingan data oleh API akan menggunakan pangkalan data sedia ada untuk menganalisis kandungan e-mel bagi memberi kesedaran kepada pengguna potensi ancaman yang bakal dihadapi. Pengimbasan melalui lampiran atau pautan pula akan mengimplementasikan aplikasi Flask menghantar ke API bagi mengesan perisian hasad serta mengesahkan ketulenan penghantar secara VirusTotal API. Selain itu, mekanisme API membantu dalam pengesanan ancaman automatik secara lampiran dan e-mel tanpa campur tangan manual. Automasi ini akan digunakan untuk menguatkuasakan dasar keselamatan dalam komunikasi e-mel dan memberi kesederan mengenai fail dan pautan yang mencurigakan secara automatik berdasarkan peraturan yang ditetapkan. Pelaksanaan yang komprehensif ini memberi jamian yang kukuh untuk pengguna dalam memperkukuhkan keselamatan dalam e-mel mereka.



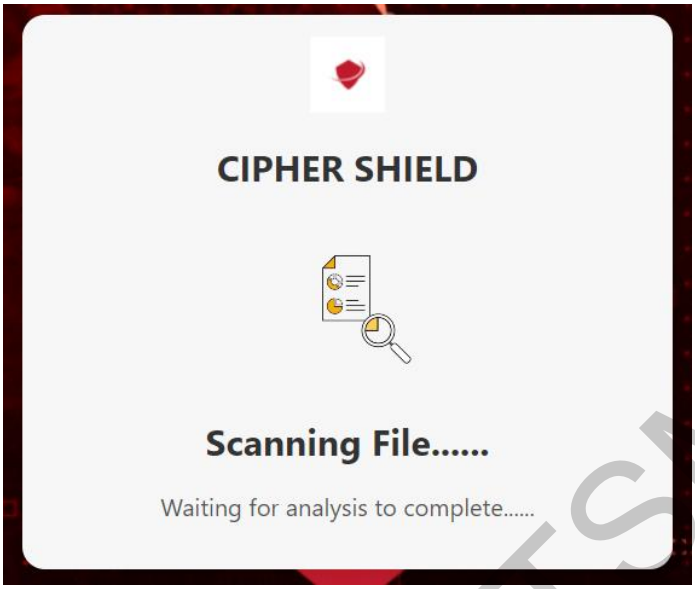
Rajah 1 Antara Muka Untuk Memaparkan Halaman Muat Naik Pautan dan Fail

Rajah 1 menunjukkan antara muka untuk mengeluarkan paparan utama pengimbasan lampiran fail (CipherShield). Pengguna akan dapat melihat paparan utama ini apabila telah memasang sambungan di web pelayar iaitu Chrome. Melalui paparan ini, pengguna dapat melihat paparan muat naik fail dan pautan untuk pengimbasan yang ingin dilakukan sama ada pautan atau fail.



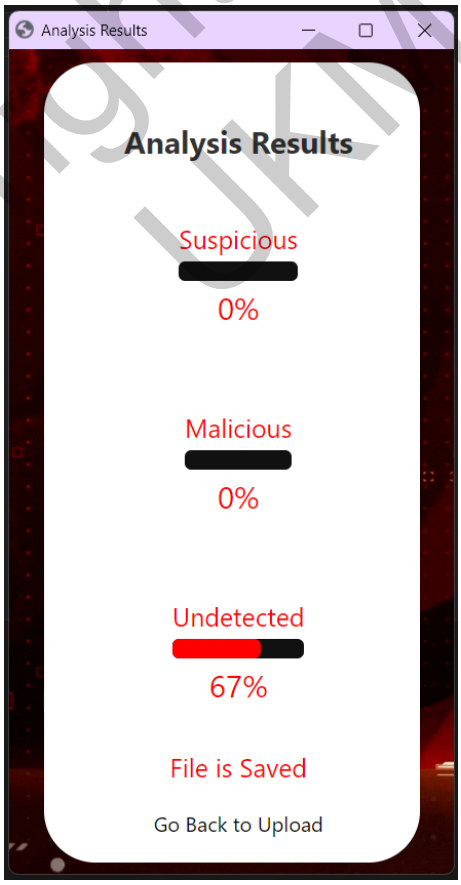
Rajah 2 Antara Muka Tetapan Pengimbasan

Rajah 2 menunjukkan antara muka bagi paparan utama pengimbasan lampiran fail (CipherShield). Pengguna akan dapat melihat paparan utama ini apabila telah memasang sambungan di web pelayar iaitu *Chrome*. Melalui paparan ini, pengguna dapat memuat naik pautan atau fail seperti pdf, docs, pptx dan xslx untuk melakukan pengimbasan dan mengesan ancaman perisian hasad atau pancingan data.



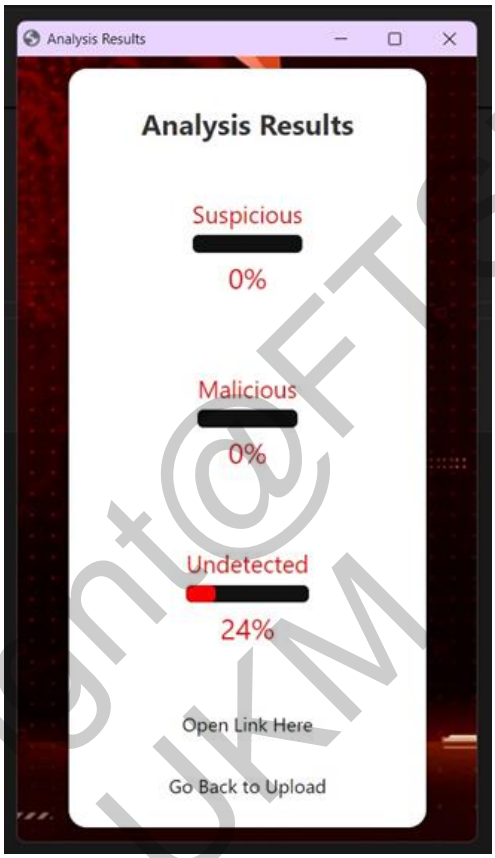
Rajah 3 Antara Muka Pengimbasan Lampiran

Rajah 3 menunjukkan antara muka bagi pengimbasan lampiran yang merupakan salah satu fungsi utama iaitu mengetahui proses sambungan dalam mengesan lampiran fail yang di muat turun oleh pengguna dalam emel. Pengguna perlu menunggu sehingga paparan analisis imbasan berjaya dipaparkan.



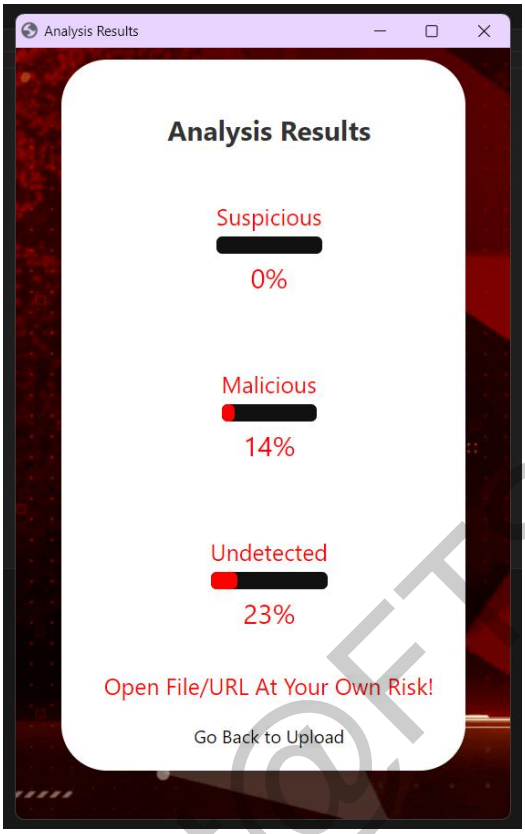
Rajah 4 Antara Muka Hasil Analisis Imbasan Muat Turun dan Naik Fail

Rajah 4 menunjukkan antara muka halaman keputusan analisis setelah melakukan pengimbasan fail yang bebas daripada ancaman. Halaman keputusan ini dikeluarkan secara automatik pada tab baharu setelah proses pengimbasan fail berjaya. CipherShield menyediakan butang ‘Go To Upload’ bagi memaparkan semula tetapan pengimbasan.



Rajah 5 Antara Muka Hasil Analisis Imbasan Pautan

Rajah 5 menunjukkan antara muka bagi hasil analisis pautan yang tidak mempunyai sebarang perisian hasad dan pancingan data. Sambungan menyediakan dua butang iaitu ‘Open Link Here’ bagi mengakses ke pautan yang diimbas atau ‘Go To Upload’ untuk kembali ke antara muka utama pengimbasan.



Rajah 6 Antara Muka Hasil Analisis Perisian Hasad/Pancingan Data Pada Pautan Atau Fail

Rajah 6 menunjukkan antara muka bagi hasil analisis pautan atau fail yang mempunyai perisian hasad atau pancingan data. Sambungan menyediakan butang‘Go To Upload’ untuk kembali ke antara muka utama pengimbasan dan mesej amaran kepada pengguna sekiranya ingin juga membuka pautan atau fail tersebut.

Hasil Pengujian Kebolehgunaan

Pada bahagian ini, ujian kebolehgunaan telah dibuat melibatkan beberapa aspek kritikal merangkumi kemudahan pengguna, kepuasan antara muka, kebolehgunaan dan kepuasan keseluruhan sistem. Melalui gabungan semua aspek ini, ia dapat memberikan gambaran keseluruhan mengenai sejauh mana sistem CipherShield ini membentuk dan memenuhi jangkaan pengguna. Responden yang digunakan membantu dalam menaik taraf sambungan dan membaiki sistem untuk memberikan pengalaman yang lebih baik kepada pengguna.

Selain itu, keputusan ujian kebolehgunaan sistem sambungan CipherShield dipengaruhi oleh faktor umur dan tahap pendidikan responden. Keputusan yang dibuat akan menjelaskan responden yang menghadapi kesukaran dan pendedahan teknologi bergantung kepada umur responden sama ad atua atau muda. Tahap pendidikan juga penting, di mana mereka dengan pendidikan lebih tinggi menunjukkan pemahaman dan kecekapan yang lebih baik dalam menggunakan sistem, yang seterusnya mempengaruhi kepuasan keseluruhan mereka.

Mengikut tinjauan yang dilakukan, keputusan maklum balas yang berjaya dikumpulkan mengikut faktor umur responden dan tahap pendidikan responden. Terdapat 3 jenis pengguna yang dikenal pasti dalam membantu membina analisis berkenaan sistem sambungan CipherShield.

Berikut merupakan sebuah jadual demografi pengguna iaitu jadual 2 menunjukkan kekerapan penggunaan sambungan mengikut peringkat umur responden manakala jadual 3 menunjukkan tahap pendidikan responden dalam menggunakan sistem sambungan ini. Merujuk kepada jadual2, kebanyakkan responden berumur daripada 21 hingga 30 tahun iaitu sebanyak 3 jumlah keseluruhannya, Bagi responden yang berumur 20 tahun ke bawah mencatatkan hanya sebanyak 2 dan tiada responden bagi umur 30 tahun ke atas yang menggunakan sambungan ini.

Jadual 2 Peratus Umur Responden

Umur	Kekerapan	Peratus (%)
20 tahun ke bawah	2	40
21 – 30 tahun	3	60
30 tahun ke atas	0	0

Bagi jadual 3, pula menunjukkan majoriti daripada responden mempunyai 60% daripada tahap pendidikan pengajian tinggi. Bagi tahap pendidikan menengah pula hanya mencatatkan sebanyak 40% daripada keseluruhan responden dan tiada responden bagi tahap pendidikan menengah. Oleh itu, setiap soalan tinjauan kebolehgunaan telah meletakkan skala 1 hingga 5 bagi mendapatkan nilai purata dalam mengesan kelemahan sistem sambungan. Mulai pada skala 1 iaitu **'Sangat Tidak Setuju', 'Tidak Setuju', 'Agak Setuju', 'Setuju'** dan yang terakhir iaitu skala 5 adalah **'Sangat Setuju'.**

Jadual 3 Tahap Pendidikan

Tahap Pendidikan	Kekerapan	Peratus (%)
Pendidikan Menengah	0	0
Pendidikan Pra-Universiti	2	40
Pengajian Tinggi	3	60

a. Kemudahan Kegunaan

Berdasarkan jadual 4, aspek pertama yang diuji adalah tahap kemudahan kegunaan sistem kepada pengguna. Pemberian soalan mengenai pendapat pengguna terhadap tahap kemudahan

semasa penggunaan sistem sambungan CipherShield. Nilai purata paling tiggi pada bahagian ini adalah 1 dimana pengumpulan data telah menunjukkan kebanyakkan pengguna bersetuju bahawa sistem ini adalah mudah digunakan. Nilai purata keseluruhan yang didapati jelas bahawa sistem sambungan ini menepati dalam kemudahan kegunaan.

Jadual 4 Purata Kemudahan Kegunaan

Soalan	Purata
Saya dapat menggunakan sistem tanpa panduan yang diberikan.	1
Saya dapat memahami apa yang berlaku sepanjang menggunakan sistem.	1
Saya dapat memuat naik fail dan pautan yang ingin dimbas dengan mudah dan cepat.	1
Saya dapat mengimbas dan mengesan pautan yang berunsur pancingan data dengan cepat.	0.8
Saya dapat mengimbas dan mengesan muat naik fail yang berunsur pancingan data dengan cepat.	1
Saya dapat mengimbas dan mengesan muat turun fail di Gmail dengan cepat	0.8

b. Kepuasan Antara Muka

Berdasarkan jadual 5, aspek kedua memfokuskan tahap kepuasan antara muka bagi keseluruhan sistem oleh pengguna. Nilai purata paling tinggi yang dikumpulkan iaitu sebanyak 1 menunjukkan bahawa pengguna bersetuju bahawa antara muka sistem sambungan amat sesuai digunakan dan berpuas hati dengan antara muka tersebut.

Jadual 5 Purata Kepuasan Antara Muka

Soalan	Purata
Skema warna sistem yang digunakan adalah sesuai dan menarik	1
Jenis huruf dan ukuran perkataan yang digunakan adalah sesuai	1
Reka bentuk sistem adalah menarik	0.8
Penggunaan antara muka pengguna sistem ini amat konsisten	0.8

c. Kebolehgunaan

Berdasarkan jadual 6, aspek ketiga memfokuskan tahap kebolehgunaan sistem oleh pengguna dalam menilai fungsi yang penting setelah membangunkan sambungan CipherShield. Menurut nilai purata yang diberikan, pengguna menunjukkan bahawa mereka berpuas hati dengan sistem sambungan ini.

Jadual 6 Purata Kebolehgunaan

Soalan	Purata
Sistem ini dapat mengeluarkan antara muka utama sambungan	1
Sistem ini mengeluarkan pemberitahuan proses pengimbasan fail secara automatik	1
Sistem ini mengeluarkan paparan analisis keputusan secara automatik	1
Sistem ini menyatakan bahawa pautan dan fail tidak selamat secara automatik	1
Pemaparan maklumat dalam sistem adalah tepat dan benar	1

d. Kepuasan Sistem

Berdasarkan jadual 7, aspek ketiga memfokuskan tahap kepuasan sistem oleh pengguna dalam menilai keseluruhan kepuasan setelah menggunakan sambungan CipherShield. Menurut nilai purata yang diberikan iaitu paling tinggi adalah 1, pengguna menunjukkan bahawa mereka berpuas hati dengan sistem sambungan ini.

Jadual 7 Purata Kepuasan Sistem

Soalan	Purata
Saya berpuas hati dengan sistem ini.	1
Saya berpuas hati dengan antara muka sistem ini	1
Sistem ini mudah difahami dan berkesan	1
Sistem ini berfungsi dengan pantas	0.8
Saya akan cadangkan sistem ini kepada rakan saya	1

Cadangan Penambahbaikan

Antara cadangan untuk meningkatkan sistem yang boleh dilaksanakan pada masa hadapan adalah:

i. Membina aplikasi mudah alih supaya memudahkan pengguna dalam memuat naik aplikasi serta menggunakan aplikasi secara offline untuk melakukan pengesanan perisian hasad dalam fail dan pautan.

ii. Menggunakan teknologi pembelajaran mesin dan algoritma untuk meningkatkan kelajuan fail.

iii. Membina model API yang sendiri yang menyediakan pengimbasan tahap tinggi daripada berbilang enjin antivirus bagi menentukan risiko fail dan pautan kepada pengguna.

iv. Menerbitkan sambungan yang di bina pada laman web Chrome Store bagi memudahkan dan mempercepatkan pemasangan sambungan di laman web Chrome pengguna.

KESIMPULAN

Secara kesimpulannya, bab ini memberikan gambaran keseluruhan kajian yang telah dilakukan. Tujuan utama kajian ini adalah untuk membangunkan automasi keselamatan emel dalam bentuk sambungan Google yang dinamakan CipherShield agar pengguna dapat mengesan fail yang berbahaya yang telah dimuat turun serta pautan fail yang berada di peranti pengguna. Objektif utama ini dapat dicapai dengan berjaya menghasilkan sistem sambungan yang berfungsi dengan baik dan boleh diakses oleh pengguna pada laman web Chrome mereka.

Kajian ini turut merangkumi pembangunan senarai fungsi CipherShield yang dihasilkan berdasarkan analisis terhadap keperluan keselamatan dokumen dalam pelbagai format. Ini termasuk dokumen-dokumen seperti docs, xlsx, dan pptx. CipherShield berjaya menunjukkan keupayaannya dalam mengimbas dan melindungi fail-fail tersebut, walaupun masih terdapat kekangan dalam menyokong format fail lain seperti fail gambar yang sering digunakan dalam pertukaran emel.

Selain itu, kajian ini juga mendapati bahawa keberkesanan CipherShield dalam melakukan imbasan dan memberikan laporan keselamatan adalah memuaskan. Namun, terdapat beberapa cabaran yang dihadapi, antaranya ialah keperluan untuk penyambungan internet yang kukuh dan masa yang agak lama diperlukan untuk memproses imbasan dokumen. Ini sedikit sebanyak mengurangkan efisiensi pengguna dalam menjalankan tugas-tugas harian yang memerlukan semakan fail dengan cepat. Walaupun begitu, kajian ini memberikan pemahaman yang lebih mendalam mengenai konsep dan fungsi CipherShield serta menyediakan panduan untuk meningkatkan keupayaannya pada masa hadapan. Ini termasuk mengembangkan sokongan untuk lebih banyak jenis fail, memperbaiki kecepatan proses imbasan, dan mengurangkan kebergantungan kepada sambungan internet. Kajian ini juga mencadangkan penggunaan teknologi pembelajaran mesin dan pengkomputeran awan untuk meningkatkan prestasi dan keberkesanan CipherShield.

Secara keseluruhan, kajian ini menunjukkan bahawa CipherShield adalah alat yang berpotensi besar dalam meningkatkan keselamatan dokumen digital dan melindungi pengguna dari ancaman siber yang semakin berkembang. Dengan peningkatan dan penambahbaikan yang dicadangkan, diharapkan CipherShield dapat terus digunakan sebagai alat yang berkesan dan dipercayai dalam menjaga keselamatan emel dan dokumen digital pengguna.

Kekuatan Sistem

Kekuatan bagi sambungan CipherShield adalah sebagai lanjutan keselamatan yang teguh dengan menyediakan perlindungan terhadap ancaman pada pautan dan fail melalui penyepaduan VirusTotal API. Antara kekuatan yang terdapat dalam sambungan ini adalah keupayaan pengimbasan masa nyata yang membolehkan pengguna menerima makluman segera mengenai potensi risiko terhadap pautan dan fail bagi menghalangkan pembukaan fail dan pautan yang berniat jahat. Antara muka yang mesra pengguna juga turut memastikan pengguna dapat menavigasi menggunakan fungsi sambungan dengan mudah tanpa perlu penambahan kepakaran teknikal. Secara keseluruhannya, sambungan CipherShield menggabungkan pengimbasan dan pengesanan yang kukuh dalam meningkatkan keselamatan persekitaran emel pengguna pada laman web Chrome mereka.

Kelemahan Sistem

Antara kekurangan dan had yang dihadapi oleh sistem sambungan CipherShield adalah:

i. Internet

Penggunaan sistem ini memerlukan penyambungan internet yang kukuh. Sekiranya pengguna tidak mempunyai internet, pengguna tidak dapat menggunakan serta mengakses kepada sambungan CipherShield.

ii. Masa

Sistem ini memakan masa yang panjang untuk menerima hasil imbasan bagi muat naik dan muat turun fail. Penggunaan masa yang panjang mengurangkan efisien pengguna dalam melakukan tugasan atau kerja yang memerlukan semakan fail yang pantas.

iii. Akses Terhad

Sistem ini mempunyai akses yang terhad terhadap VirusTotal API dimana untuk melihat hasil pengimbasan yang lebih teliti dengan menggunakan berbilang enjin antivirus perlu menjadi pelanggan yang premium dan menyediakan akses yang tiada terhad untuk melakukan pengimbasan fail dan pautan.

PENGHARGAAN

Terlebih dahulu, bersyukur saya ke hadrat ilahi ke atas kurniaan rahmatNya serta limpah kurniaNya sehingga saya berjaya menyiapkan projek tahun akhir ini dengan baik. Setinggi-tinggi ucapan penghargaan dan terima kasih kepada penyelia projek saya iaitu Ts. Dr. Wan

Fariza binti Paizi@Fauzi yang sudi meluangkan masa tidak mengira pagi, petang mahupun malam membantu saya menyatukan projek akhir ini. Beliau juga banyak memberi bimbingan dan tunjuk ajar dan meneliti setiap perkara yang dilakukan oleh saya sepanjang tempoh menyiapkan projek ini. Beliau juga banyak membantu saya dalam memberi pendapat yang berguna berkenaan projek dan memperbetulkan kesilapan saya dalam membangunkan projek ini.

Di kesempatan ini, jutaan terima kasih yang tidak terhingga saya ungkapkan kepada semua pensyarah di Fakulti Teknologi dan Sains Maklumat yang berusaha dan bertungkus-lumus membantu pelajar-pelajar tahun akhir dalam menjayakan projek tahun akhir yang ingin dibangunkan oleh pelajar. Usaha yang diberikan dalam memastikan setiap pelajar menghantar laporan mengikut masa yang ditetapkan dengan membuat taklimat dan penerangan secara mendalam mengenai setiap topik usulan projek ini. Taklimat yang diberikan turut membantu pelajar dalam proses membuat dokumentasi dengan berkesan.

Akhir sekali, saya ingin mengucapkan ribuan terima kasih terhadap rakan-rakan saya yang bertungkus-lumus dengan memberikan idea, tenaga dan masa membimbing saya menyiapkan projek ini mengikut tempoh pelaksanaan projek. Mereka yang sentiasa saling ingat mengingati dan berkongsi maklumat antara satu sama lain agar saya tidak ketinggalan dalam menyiapkan projek ini. Malah, jutaan terima kasih kepada keluarga saya terutama ibu bapa saya yang banyak memberikan sokongan dan dorongan agar kesihatan mental dan fizikal saya terjaga sepanjang menyiapkan projek ini. Kata-kata serta doa yang dilimpahkan menjadi ukuran kepada saya untuk terus gigih dalam menyempurnakan projek saya sehingga berjaya.

RUJUKAN

Akhawe, D., Saxena, P. & Song, D. (t.th.). Privilege Separation in HTML5 Applications.

Abby. 2023. Gmail Guide: History, origin, and more. History-Compute: https://history-computer.com/gmail-guide/

Bapat, D., Butler, K. & Mcdaniel, P. (t.th.). Towards Automated Privilege Separation.

Barth, A., Felt, A.P., Saxena, P. & Boodman, A. (t.th.). Protecting Browsers from Extension Vulnerabilities. https://attacker.com/,.

Barua, A., Zulkernine, M. & Weldemariam, K. 2013. Protecting web browser extensions from JavaScript injection attacks. *Proceedings of the IEEE International Conference on Engineering of Complex Computer Systems, ICECCS* hlm. 188–197. Institute of Electrical and Electronics Engineers Inc.

Barua, Anton. 2014. *Protecting Browser Extensions from JavaScript Injection Attacks with Runtime Protection and Static Analysis.* Library and Archives Canada = Bibliothèque et Archives Canada.

Bennett, D. 2022. Chinese spy uses Gmail, iCloud, showing tech privacy is harder than it looks. Bloomberg.com.: https://www.bloomberg.com/news/newsletters/2022-09-16/chinese-spy-uses-gmail-icloud-showing-tech-privacy-is-harder-than-it-looks

Carlini, N., Felt, A.P. & Wagner, D. (t.th.). An Evaluation of the *Google Chrome* Extension Security Architecture.

Chen, H. & Hossain, M. (t.th.). Developing a *Google Chrome* Extension for Detecting Phishing Emails.

Cure, A. 2019. C#/.NET/Core training in Denver: https://cypressdatadefense.com/blog/impact-of-security-misconfiguration/

Cook, A. J.2020. Power Automate integrated with Virus Total to scan files and links. Flow Alt Delete - Josh Cook [Microsoft MVP]. https://flowaltdelete.ca/2020/08/10/power-automate-integrated-with-virus-total-to-scan-files-and-links/

Dilipbhai, J. 2019. A browser extension to detect malicious PDFs.

Fig, B. 1. The system components diagram for detecting phishing URLs in. . . (n.d.). ResearchGate. https://www.researchgate.net/figure/The-system-components-diagram-for-detecting-phishing-URLs-in-a-real-time-environment_fig1_357289431

Garfinkel, S.L., Margrave, D., Schiller, J.I., Nordlander, E. & Miller, R.C. 2005. How to Make Secure Email Easier To Use.

Grren, O. 2023. *Google Email Checker Tool: Unleashing the Power of Verification*. Retrieved from Emailsvalidation: https://emaillistvalidation.com/blog/*Google*-email-checker-tool-unleashing-the-power-of-verification/

Goud, N. 2018. *Media Prima Berhad Malaysia servers hit by Ransomware Attack - Cybersecurity Insiders*. Cybersecurity Insiders. https://www.cybersecurity-insiders.com/media-prima-berhad-malaysia-servers-hit-by-ransomware-attack/

Han'guk Chŏngbo Kwahakhoe, IEEE Computer Society & Institute of Electrical and Electronics Engineers. (t.th.). *The 32nd International Conference on Information Networking (ICOIN 2018) : January 10 (Wed.)-12 (Fri.), 2018, Holiday Inn Chiang Mai, Chiang Mai, Thailand*.

Institute of Electrical and Electronics Engineers. (t.th.). *2016 IEEE Conference on Communications and Network Security (CNS).*

Liu, L., Yan, G. & Chen, S. (t.th.). *Chrome* Extensions: Threat Analysis and Countermeasures. http://www.*Google*.com.

Lutkevich, B., & Lewis, S. 2022. waterfall model. Software Quality: https://www.techtarget.com/searchsoftwarequality/definition/waterfall-model

Manekar, A., Bhambore, D., Kalbande, J., Meshram, R. & Khan, A. (t.th.). ACE EMAIL COMPOSER EXTENSION (BROWSER EXTENSION). *www.irjmets.com @International Research Journal of Modernization in Engineering 122* https://www.doi.org/10.56726/IRJMETS37834.

Masri, R. & Aldwairi, M. 2017. Automated malicious advertisement detection using VirusTotal, URLVoid, and TrendMicro. *2017 8th International Conference on*

Information and Communication Systems, ICICS 2017 hlm. 336–341. Institute of Electrical and Electronics Engineers Inc.

Mehta, P. 2016. *Creating Google Chrome Extensions*. *Creating Google Chrome Extensions*. Apress.

Mohsienuddin Mohammad, S. & Lakshmisri, S. 2018. Security automation in Information technology. *International Journal of Creative Research Thoughts* Vol. 6 www.ijcrt.org.

Morgan, S. 2017. *Google* prevents 10 million malicious emails every 60 seconds: Gmail users beware. CSO Online: https://www.csoonline.com/article/560269/*Google*-prevents-10-million-malicious-emails-every-60-seconds-gmail-users-beware.html

PricillaWhite. 2020. Are there security vulnerabilities in Gmail even in 2020 – GBHackers on Security | #1 globally trusted cyber security news platform. GBHackers on Security | #1 Globally Trusted Cyber Security News Platform: https://gbhackers.com/are-there-security-vulnerabilities-in-gmail-even-in-2020/

Phishing Activity Trends Report. (2023). APWG. Retrieved December 10, 2023, from https://apwg.org/trendsreports/

Aimi Ayuni Binti Shamsudin (A187865)
Ts. Dr. Wan Fariza Binti Paizi@Fauzi
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia