Vol. 10, Issue 2, pp. 157-166 | DECEMBER 2025
DOI: https://doi.org/10.53840/myjict10-2-237

FAKTOR KEJAYAAN KESELAMATAN PLATFORM ANTARA MUKA APLIKASI PENGATURCARAAN DALAM SEKTOR AWAM MALAYSIA

[i*]Siti Norul Huda Sheikh Abdullah, [i]Azril Hanafi Abdullah Sharwani, [i]Monaliza Sahri, [ii]Juzlinda Mohd Ghazali, [iii]Azlina binti Ali, & [iv]Nik Rafizal Nik Ab. Rahim,

[i]Pusat Keselamatan Siber, Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia, Bangi, Selangor

[ii]Fakulti Multimedia Kreatif dan Komputeran (FMKK), Universiti Islam Selangor, Bandar Seri Putra, Selangor

[iii]Jabatan Digital Negara, Kementerian Digital, Cyberjaya, Selangor

[iv]HLAi Sdn Bhd, Cyberjaya, Selangor

*e-mail: snhsabdullah@ukm.edu.my

Article history:
Submission date: 6 November 2025
Received in revised form: 29 December 2025
Acceptance date: 30 December 2025
Available online: 31 December 2025

Keywords:
Keselamatan Data, Platform Perkongsian Data, Application Programming Interface (API), Faktor Kejayaan, PLS-SEM

Funding:
Projek ini telah dibiayai oleh dua geran penyelidikan: TT-2023-016 "Rangka Kerja Perkongsian Data Malaysia" dan TT-2023-019 bertajuk "Pembangunan Dasar Perkongsian Data Negeri Selangor".

Competing interest:
The author(s) have declared that no competing interests exist.

Cite as:
Sahri, M., Sheikh Abdullah, S. N. H. ., Abdullah Sharwani, A. H. ., Ali, A. ., Mohd Ghazali, J. ., & Nik Ab. Rahim, N. R. . (2025). Faktor Kejayaan Keselamatan Platform Antara Muka Aplikasi Pengaturcaraan Dalam Sektor Awam Malaysia: Application Programming Interface Platform Security Success Factors. Malaysian Journal of Information and Communication Technology (MyJICT), 10(2), 157-166. https://doi.org/10.53840/myjict10-2-237

ABSTRAK

Perkembangan teknologi digital telah memperluas penggunaan Antara Muka Aplikasi Pengaturcaraan atau *Application Programming Interface* (API) sebagai medium utama dalam proses perkongsian data antara sistem dan agensi. Namun, peningkatan insiden kebocoran data yang kritikal, khususnya dalam sektor kerajaan, menimbulkan kebimbangan terhadap tahap keselamatan platform perkongsian data. Kelemahan tersebut berpunca daripada kekurangan faktor kejayaan yang berkaitan dengan (i) keperluan keselamatan khusus bagi pelbagai jenis data, (ii) ketidakpatuhan terhadap peraturan dan undang-undang, serta (iii) kegagalan dalam melindungi privasi pengguna. Oleh itu, kajian ini dijalankan bagi mengenal pasti faktor kejayaan keselamatan platform API dalam ekosistem perkongsian data sektor awam. Kaedah kajian melibatkan analisis literatur untuk memahami ekosistem perkongsian data dan mengenal pasti faktor-faktor utama yang membentuk instrumen kajian. Seramai 81 orang pakar daripada pelbagai agensi telah terlibat bagi menilai dan mengesahkan faktor yang dikenal pasti. Analisis model menggunakan *Partial Least Squares-Structural Equation Modeling* (PLS-SEM) menunjukkan bahawa semua hipotesis hubungan faktor diterima, dengan nilai signifikan p=0.002 (H1: Berskala dan Daya Tahan Tinggi → Reka Bentuk), p=0.000 (H2: Pemantauan Aktiviti → Berskala dan Daya Tahan Tinggi), p=0.040 (H3: Perlindungan Data dan Privasi → Berskala dan Daya Tahan Tinggi), dan p=0.000 (H4: Standard Keselamatan → Perlindungan Data dan Privasi). Hasil kajian ini membentuk lima faktor kejayaan utama keselamatan platform perkongsian data melalui API, iaitu: (i) reka bentuk, (ii) berskala dan daya tahan tinggi, (iii) standard keselamatan, (iv) pemantauan aktiviti, serta (v) perlindungan data dan privasi. Kajian ini dapat menyumbang kepada pembangunan kerangka keselamatan API bagi Platform API sektor awam yang lebih kukuh dan berdaya tahan terhadap ancaman siber masa kini.

APPLICATION PROGRAMMING INTERFACE PLATFORM SECURITY SUCCESS FACTORS IN THE MALAYSIAN PUBLIC SECTOR

ABSTRACT

The development of digital technology has expanded the use of Application Programming Interface (API) as the primary medium in the data sharing process between systems and agencies. However, the increase in critical data leak incidents, especially in the government sector, has raised concerns about the security level of data sharing platforms. These weaknesses stem from the lack of success factors related to (i) specific security requirements for various types of data, (ii) non-compliance with regulations and laws, and (iii) failure to protect user privacy. The study identifies the security success factors of API platforms within the public sector data sharing ecosystem. The study method involved a literature analysis to understand the data sharing ecosystem and identify the main factors that formed the study instrument. Eighty-one experts from various agencies were involved in assessing and validating the identified factors. Model analysis using Partial Least Squares-Structural Equation Modeling (PLS-SEM) showed that all factor relationship hypotheses were accepted, with significant values of p=0.002 (H1: Scalability and High Resilience → Design), p=0.000 (H2: Activity Monitoring → Scalability and High Resilience), p=0.040 (H3: Data Protection and Privacy → Scalability and High Resilience), and p=0.000 (H4: Security Standards → Data Protection and Privacy). The results of this study formed five key success factors for the security of API platforms, namely: (i) design, (ii) scalability and high resilience, (iii) security standards, (iv) activity monitoring, and (v) data and privacy protection. This study contributes to the development of an API security framework for public sector API Platforms that are stronger and more resilient to today's cyber threats.

Keywords: *Security Data, Platform Sharing Data, Application Programming Interface (API), Success Factors, PLS-SEM*

Pengenalan

Perkembangan teknologi digital telah mengubah landskap ekonomi dan sosial global dengan kemunculan ekonomi digital berasaskan interaksi antara manusia, perniagaan, peranti digital dan data. Infrastruktur utama ekonomi digital ialah hyper-connectivity yang menghubungkan pelbagai sistem dan peranti pintar. Data kini menjadi sumber ekonomi terpenting menggantikan bahan bakar tradisional, dengan nilai ekonomi digital Asia Tenggara dianggarkan mencecah RM930 bilion pada tahun 2022 (Google & Temasek & Bain Company, 2022).

Dalam konteks ini, Application Programming Interface (API) memainkan peranan penting sebagai jambatan komunikasi antara pelbagai aplikasi dan sistem. API membolehkan perkongsian data rentas platform bagi meningkatkan kecekapan operasi, integrasi sistem, serta inovasi perkhidmatan digital. Nilai pasaran global API dijangka berkembang daripada RM17.97 bilion pada tahun 2022 kepada RM156.33 bilion menjelang tahun 2030 (Data Bridge Market Research, 2023).

Peningkatan penggunaan API turut meningkatkan risiko dan isu dalam keselamatan data negara. Pada tahun 2022, Malaysia menyaksikan beberapa insiden kebocoran data besar melibatkan pendedahan berjuta-juta rekod peribadi rakyat termasuk MyKad, maklumat identiti, dan butiran peribadi sensitif. Insiden-insiden ini bukan sahaja menunjukkan kelemahan serius dalam keselamatan sistem sektor awam, malah menggariskan risiko penyalahgunaan data apabila maklumat tersebut diakses secara tidak sah dan diperdagangkan di dark web (Leng & Doris Liew, 2024).

Kelemahan Kajian dan Amalan Sedia Ada

Kelemahan ini berpunca dari pelbagai faktor. Kajian lepas (Jin et al., 2019; Naz et al., 2019; Tsohou et al., 2020) juga mengenal pasti tiga kelemahan utama lain dalam pelaksanaan keselamatan perkongsian data:

1. Kekurangan keperluan keselamatan spesifik bagi pelbagai jenis data,
2. Ketidakpatuhan terhadap undang-undang dan peraturan, serta
   Ketidakupayaan melindungi privasi pengguna

Dalam konteks Malaysia, ketiadaan standard keselamatan yang seragam untuk platform perkongsian data melalui API di sektor awam Malaysia, mengakibatkan variasi tahap perlindungan data antara agensi serta meningkatkan risiko kebocoran maklumat sensitif dan menjejaskan keyakinan pengguna terhadap penggunaan perkhidmatan digital Kerajaan (Leng & Doris Liew, 2024). Penyimpanan dan perkongsian data rentas sempadan menghadapi cabaran pematuhan terhadap peraturan tempatan seperti Akta Perlindungan Data Peribadi 2010 (PDPA) dan standard antarabangsa termasuk General Data Protection Regulation (GDPR)(Solove & Schwartz, 2020). Kekurangan garis panduan standardisasi keselamatan data yang diterima pakai secara universal menyukarkan agensi kerajaan untuk memastikan konsistensi dan kepatuhan dalam pelaksanaan API.

Laporan CyberSecurity Malaysia turut menunjukkan sektor awam merupakan sektor yang paling terdedah terhadap risiko keselamatan data di mana sektor awam mencatat 22% daripada keseluruhan insiden pelanggaran data di Malaysia (Yeoh, 2023). Kelemahan tadbir urus data seperti kebocoran data ini yang berpunca daripada kelemahan dalam mekanisme penyulitan, pengesahan identiti yang tidak konsisten, dan kawalan capaian yang tidak terstandardisasi (Gawande et al., 2021; Habibzadeh et al., 2019).

Kelemahan ini menjejaskan keyakinan pengguna dan meningkatkan risiko kebocoran maklumat sensitif. Oleh itu, penyelidikan ini menumpukan kepada pengenalpastian faktor kejayaan keselamatan platform perkongsian data melalui API, pembangunan model keselamatan berasaskan faktor tersebut, Hasil dapatan kajian ini dapat membantu dalam penyediaan Prosedur Operasi Standard (SOP) bagi memastikan pelaksanaan keselamatan data yang menyeluruh dan konsisten di seluruh agensi kerajaan.

Analisis Jurang

Walaupun kajian terdahulu telah membincangkan isu keselamatan maklumat dan perkongsian data secara umum, terdapat kekurangan kajian yang memfokuskan secara khusus kepada keselamatan platform perkongsian data berasaskan API dalam konteks sektor awam Malaysia. Selain itu, kebanyakan kajian sedia ada menilai faktor keselamatan secara terasing, tanpa mengintegrasikan aspek teknikal, tadbir urus, dan pematuhan perundangan dalam satu model keselamatan yang menyeluruh. Terdapat juga kekurangan bukti empirikal yang menguji hubungan antara faktor kejayaan keselamatan API menggunakan pendekatan statistik seperti Partial Least Squares Structural Equation Modeling (PLS-SEM).

Objektif Kajian

Kajian ini dijalankan untuk mencapai objektif berikut dalam konteks keselamatan platform perkongsian data melalui API di sektor awam:

1. Mengenal pasti faktor kejayaan keselamatan platform API yang kritikal dalam ekosistem perkongsian data sektor awam.
2. Membangunkan model keselamatan platform API berdasarkan hubungan antara faktor-faktor kejayaan yang dikenal pasti.
3. Menguji hubungan antara faktor kejayaan menggunakan PLS-SEM, untuk menilai kesan faktor terhadap keselamatan dan kebolehpercayaan platform.

Sorotan Literatur

Perkongsian data melalui Application Programming Interface (API) menjadi tunjang kepada transformasi digital sektor awam dan swasta. Namun, isu keselamatan seperti kebocoran maklumat dan pencerobohan siber semakin meningkat akibat kelemahan reka bentuk API, ketidakpatuhan terhadap undang-undang, serta kekurangan standard keselamatan menyeluruh (Hussain, Salah, et al., 2020). Kajian literatur ini membincangkan empat dimensi utama yang menyumbang kepada kejayaan keselamatan platform perkongsian data melalui API: (i) undang-undang dan dasar, (ii) piawaian keselamatan maklumat, (iii) teknologi dan privasi, serta (iv) amalan pemantauan dan tadbir urus.

Undang-undang dan Dasar Perlindungan Data

Perlindungan data peribadi merupakan asas kepada keselamatan digital sesebuah negara. General Data Protection Regulation (GDPR) di Kesatuan Eropah menetapkan hak pemilik data dan prinsip ketelusan

sebagai piawaian global (Krishnamurthy, 2020). Di Amerika Syarikat, pendekatan perlindungan data bersifat sektoral seperti Health Insurance Portability and Accountability Act (HIPAA) dan Children's Online Privacy Protection Act (COPPA).

Malaysia pula memperkenalkan Personal Data Protection Act (PDPA) 2010, namun ia hanya terpakai kepada entiti komersial dan tidak meliputi sektor kerajaan. Beberapa kajian mendapati keperluan mengemaskini PDPA bagi menambah klausa pelanggaran data serta memperluas skop perlindungan kepada entiti awam (Ahmed & Zulhuda, 2019; Ghani et al., 2020). Dalam konteks pentadbiran awam, sektor awam merupakan peneraju dalam proses digitalisasi dan seterusnya membangunkan keupayaan hab data kerajaan serta menetapkan keperluan kerjasama rentas agensi secara selamat dan berintegriti berpandukan dasar semasa seperti Dasar Perkongsian Data Sektor Awam (DPSA) dan Pelan Strategik Pendigitalan Sektor Awam 2021–2025 (Jalil et al., 2023).

Piawaian dan Tadbir Urus Keselamatan Maklumat

Keselamatan maklumat menuntut pendekatan berasaskan piawaian antarabangsa. ISO/IEC 27001 menekankan pembangunan Information Security Management System (ISMS) melalui kitaran Plan-Do-Check-Act bagi menjamin kawalan berterusan terhadap risiko keselamatan. BS 7799 pula menjadi asas kepada penubuhan piawaian ISMS global, manakala Control Objectives for Information and Related Technologies (COBIT) serta Information Technology Infrastructure Library (ITIL) menyediakan kerangka tadbir urus dan pengurusan infrastruktur IT (Susanto et al., 2011). Pematuhan kepada piawaian ini menjamin integriti, ketersediaan dan kerahsiaan data — tiga prinsip utama dalam model Confidentiality, Integrity, and Availability (Chai & Zolkipli, 2021).

Teknologi API dan Perlindungan Privasi

API merupakan komponen penting dalam membolehkan sistem berbeza berkomunikasi dan bertukar data. Namun, reka bentuk API yang lemah boleh menjadi punca utama kebocoran data (Bloch, 2007). Ciri prestasi seperti kebolehskalaan, keseimbangan beban (load balancing), dan kawalan akses menentukan tahap daya tahan platform (Borgogno & Colangelo, 2019; Pawan & Rakesh, 2019).

Aspek keselamatan API perlu menekankan kawalan akses, penyulitan data, pengesahan identiti (authentication), serta kebenaran (authorization) yang kukuh (Hussain, Noye, et al., 2020; Sun et al., 2022). Teknologi seperti OAuth 2.0 dan OpenID Connect memperkukuh keselamatan pengguna, manakala pendekatan privacy-by-design memastikan privasi dipertimbangkan sejak fasa reka bentuk (Amalia et al., 2020).

Pemantauan dan Ekosistem Perkongsian Data

Pemantauan trafik API secara masa nyata penting bagi mengesan aktiviti mencurigakan serta menilai kadar ralat dan prestasi sistem (D'Elia et al., 2021; Stiefel & Ananthanarayanan, 2023). Negara maju seperti Estonia memperkenalkan platform X-Road, yang menggunakan seni bina teragih dan Public Key Infrastructure (PKI) untuk menjamin keselamatan transaksi data antara agensi (Mändar, 2017). Malaysia pula mengembangkan MyGDX (Malaysia Government Data Exchange) sebagai tulang belakang integrasi data sektor awam, berasaskan prinsip keselamatan, pertanggungjawaban dan pematuhan (Hasliza et al., 2020; Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), 2023).

Inisiatif negeri seperti Selangor Government Data Exchange (SelGDX) juga memperlihatkan bagaimana perkongsian data boleh dipacu melalui tadbir urus dan piawaian keselamatan yang konsisten di peringkat negeri (The Star, 2023). Pendekatan bersepadu antara dasar, piawaian, dan teknologi membentuk asas kepada keberkesanan ekosistem perkongsian data yang selamat dan boleh dipercayai (Amelia Natasya et al., 2023; Monaliza et al., 2023).

Rumusan Kajian Literatur

Kajian literatur menunjukkan bahawa kejayaan keselamatan platform perkongsian data melalui API dipengaruhi oleh gabungan faktor dasar, piawaian, teknologi dan tadbir urus. Persekitaran yang mengintegrasikan kerangka undang-undang yang jelas, pematuhan terhadap piawaian keselamatan antarabangsa, serta pelaksanaan kawalan teknologi yang proaktif akan memastikan perkongsian data awam berjalan dengan selamat, berintegriti dan mampan. Oleh itu, pemahaman mendalam terhadap

faktor-faktor ini menjadi asas kepada pembangunan model faktor kejayaan keselamatan platform perkongsian data melalui API yang akan diuji dalam kajian ini.

Metodologi Kajian

Kajian ini menggunakan pendekatan campuran yang menggabungkan kaedah kuantitatif bagi mengenal pasti serta mengesahkan faktor-faktor kejayaan keselamatan platform perkongsian data melalui API. Menurut (Bairagi & Munot, 2019), pendekatan tersusun penting bagi memastikan objektif kajian dapat dicapai dengan berkesan. Pendekatan kuantitatif digunakan bagi mengukur hubungan antara konstruk melalui soal selidik.

Kajian ini dilaksanakan dalam dua fasa utama. Fasa pertama melibatkan analisis literatur dan pembangunan instrument. Analisis dokumen dan kajian terdahulu dilakukan untuk mengenal pasti faktor-faktor berkaitan keselamatan API dan membangunkan instrumen soal selidik. Fasa kedua pula melibatkan pembangunan dan Pengesahan Model: Data daripada soal selidik dianalisis menggunakan kaedah Partial Least Squares–Structural Equation Modeling (PLS-SEM) bagi membina model faktor kejayaan keselamatan API.

Kaedah Pengumpulan Data

Kaedah pengumpulan data utama digunakan iaitu soal selidik. Soal selidik ini bertujuan mengumpul maklum balas responden yang terlibat secara langsung dalam ekosistem perkongsian data sektor awam. Ia merangkumi 44 item dibahagikan kepada tujuh (7) bahagian iaitu: Demografi, Latar Belakang Perkongsian Data, Reka Bentuk API, Pemantauan Aktiviti API, Berskala dan Daya Tahan Tinggi, Perlindungan Data dan Privasi, serta Standard Keselamatan. Soalan diukur menggunakan Skala Likert enam mata (1 = sangat tidak setuju hingga 6 = sangat setuju) bagi menilai tahap persetujuan terhadap setiap pernyataan.

Persampelan dan Lokasi Kajian

Kajian ini menggunakan kaedah persampelan rawak berfokus (purposive random sampling) bagi memastikan responden yang dipilih benar-benar mempunyai pengetahuan dan pengalaman langsung dalam pelaksanaan perkongsian data sektor awam melalui platform Application Programming Interface (API). Sasaran kajian tertumpu kepada pegawai kerajaan yang terlibat secara langsung dalam perancangan, tadbir urus, pembangunan, keselamatan, atau operasi perkongsian data antara agensi.

Kajian dijalankan di Sepang dan Klang, Selangor, yang merupakan lokasi utama penempatan kementerian dan agensi kerajaan persekutuan serta negeri yang aktif dalam inisiatif pendigitalan dan perkongsian data. Pemilihan lokasi ini bertujuan untuk memastikan keterwakilan agensi yang terlibat secara langsung dalam pelaksanaan platform perkongsian data nasional.

Sebanyak 81 responden pakar telah dipilih dan terlibat dalam kajian ini, merangkumi pegawai daripada agensi persekutuan dan kerajaan negeri yang berperanan sebagai pembuat keputusan, pelaksana teknikal, dan pengguna sistem perkongsian data.

Kaedah Analisis Data

Analisis data dijalankan menggunakan gabungan kaedah analisis deskriptif dan analisis inferensi. Data kuantitatif dianalisis menggunakan perisian SmartPLS 4.0. Langkah analisis model PLS-SEM meliputi:

1. Kebolehpercayaan Indikator: Penilaian pemuatan faktor (>0.7) untuk memastikan kesahan setiap item (Jr. et al., 2020).
2. Kebolehpercayaan Konstruk: Diukur menggunakan Cronbach's Alpha ($\alpha \geq 0.7$) bagi menilai ketekalan dalaman konstruk (George & Mallery, 2016).
3. Kesahan Konvergen (AVE): Nilai Average Variance Extracted ($AVE \geq 0.5$) digunakan untuk mengesahkan kesahan konvergen (Purwanto & Sudargini, 2021).
4. Kesahan Diskriminan: Menentukan perbezaan yang jelas antara konstruk (Matthes & Ball, 2018).
5. Kolinearitiy: Diuji menggunakan Variance Inflation Factor ($VIF < 5$) untuk memastikan tiada masalah kolinearitiy antara pemboleh ubah (Joe F. Hair Jr et al., 2017).

6. Koefisien Lintasan (β): Menilai hubungan antara konstruk eksogenus dan endogenus berdasarkan nilai β dan signifikan ($p < 0.05$).

Kebolehpercayaan dan Kesahan Instrumen

Model pengukuran diuji untuk memastikan kesahan dan kebolehpercayaan instrumen. Nilai Alfa Cronbach ($\alpha = 0.71–0.99$) menunjukkan tahap kebolehpercayaan yang baik(Bond & Fox, 2015). Hasil ujian menunjukkan semua konstruk mencapai tahap kesahan dan kebolehpercayaan yang diterima.

Secara keseluruhan, metodologi kajian ini dirancang secara sistematik untuk membangunkan dan mengesahkan model faktor kejayaan keselamatan platform perkongsian data melalui API. Hasil analisis kuantitatif dari PLS-SEM menjadi asas kepada pembentukan SOP keselamatan API yang boleh dijadikan panduan rasmi bagi memperkukuh keselamatan data sektor awam di Malaysia.

Dapatan Kajian

Demografi

Kajian ini dijalankan untuk mengenal pasti faktor-faktor keselamatan utama dalam pembangunan dan pelaksanaan platform perkongsian data melalui Application Programming Interface (API) di sektor awam Malaysia. Sebanyak 103 borang soal selidik telah diedarkan kepada responden dalam kalangan pegawai teknologi maklumat dan pentadbir data di agensi kerajaan, dan 81 set soal selidik yang lengkap telah diterima semula dengan kadar maklum balas 78.6%. Kadar ini menunjukkan penglibatan yang baik serta kebolehpercayaan data yang tinggi bagi analisis model yang dijalankan.

Kajian ini melibatkan seramai 81 orang responden daripada pelbagai kementerian dan agensi kerajaan. Majoriti responden terdiri daripada perempuan (55.6%) dan lelaki (44.4%), dengan kumpulan umur tertinggi berusia 41–50 tahun (61.7%), diikuti 30–40 tahun (28.4%). Sebahagian besar responden berbangsa Melayu (97.5%), dan berkelulusan Ijazah Sarjana Muda (43.2%), manakala selebihnya memiliki kelulusan Sarjana, Diploma, dan Sekolah Menengah. Dari segi klasifikasi perkhidmatan, bidang Teknologi Maklumat (23.5%) merupakan yang tertinggi, diikuti oleh Sains (17.3%), Tadbir dan Diplomatik (12.3%), serta Kewangan (11.1%).

Bagi kategori perkhidmatan, majoriti responden terdiri daripada Kumpulan Pengurusan dan Profesional (55.6%), diikuti Pelaksana (40.7%), manakala Pengurusan Tertinggi (3.7%) merupakan kumpulan terkecil. Sebahagian besar responden telah berkhidmat lebih 10 tahun (76.3%), menunjukkan pengalaman kerja yang luas dalam sektor awam. Dari segi pelaksanaan, 80.2% agensi dilaporkan melaksanakan perkongsian data, dan 87.7% responden terlibat secara langsung dalam aktiviti tersebut. Peranan utama dalam perkongsian data didominasi oleh CIO/CDO (37.5%), diikuti Penyelaras Perkongsian Data (26.8%), dan Pengguna (19.6%). Secara keseluruhan, 75.3% agensi telah melaksanakan perkongsian data melalui platform rasmi, menggambarkan tahap kesedaran dan penglibatan yang tinggi terhadap inisiatif perkongsian data sektor awam.

Analisis Deskriptif

Analisis awal menunjukkan lima konstruk utama yang dikenal pasti sebagai faktor kejayaan keselamatan platform API, iaitu:

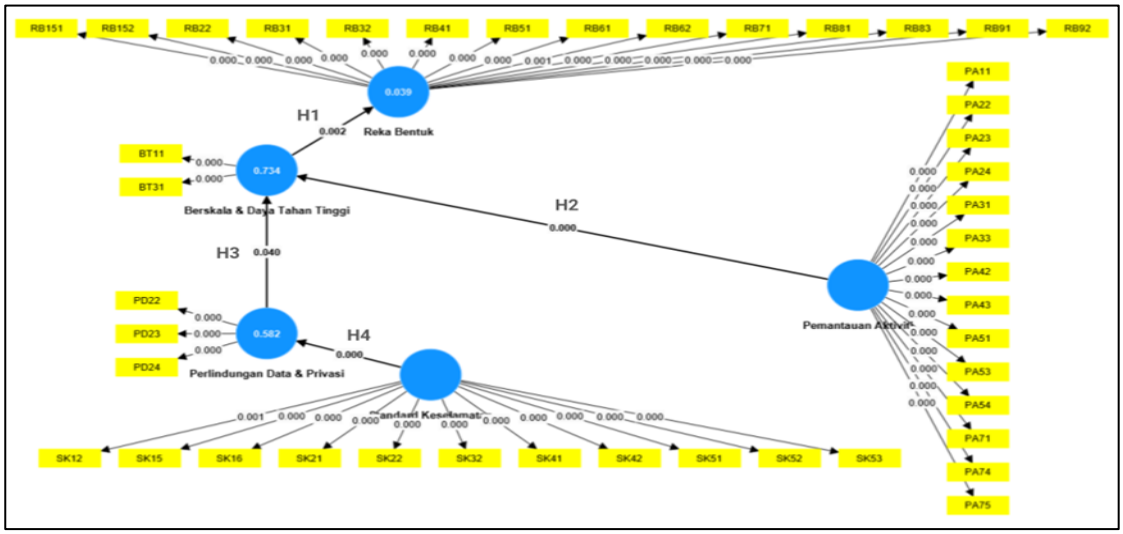
1. Reka Bentuk API (API Design)
2. Pemantauan Aktiviti API (API Monitoring)
3. Berskala dan Daya Tahan Tinggi (Scalability & Resilience)
4. Perlindungan Data dan Privasi (Data Protection & Privacy)
5. Standard Keselamatan (Security Standard)

Kesemua konstruk mencatatkan nilai min yang tinggi (antara 0.024 hingga 0.588) dan sisihan piawai yang rendah, menunjukkan tahap persetujuan yang kukuh dalam kalangan responden terhadap kepentingan faktor-faktor tersebut. Faktor Berskala dan Daya Tahan Tinggi memperoleh purata tertinggi, menggambarkan bahawa kebolehpercayaan dan kestabilan API dianggap komponen paling kritikal dalam memastikan keberkesanan dan keselamatan perkongsian data kerajaan.

Selain itu, konstruk Perlindungan Data dan Privasi serta Standard Keselamatan turut menunjukkan nilai min yang konsisten tinggi, menunjukkan kesedaran yang besar terhadap pematuhan kepada dasar keselamatan siber, undang-undang perlindungan data seperti PDPA, dan standard antarabangsa seperti ISO/IEC 27001 dalam memastikan keselamatan data terjamin.

Analisis Model PLS-SEM dan Perbincangan

Kaedah Partial Least Squares – Structural Equation Modelling (PLS-SEM) digunakan untuk mengesahkan kesahan dan kebolehpercayaan model kajian seperti Rajah 1. Kebolehpercayaan Dalaman bagi semua konstruk mencatat nilai Cronbach's Alpha (α) antara 0.787 hingga 0.974, melebihi had minimum 0.7, menunjukkan tahap kebolehpercayaan dalaman yang tinggi. Selain daripada itu, Kesahan Menumpu (Convergent Validity) menunjukkan Nilai Average Variance Extracted (AVE) berada antara 0.511 hingga 0.824, memenuhi syarat kesahan menumpu (>0.5). Kesahan Diskriminan (Discriminant Validity) berdasarkan kriteria Fornell-Larcker, menunjukkan semua konstruk tidak bertindih, membuktikan setiap konstruk adalah unik. Seterusnya, Kolineariti iaitu Nilai Variance Inflation Factor (VIF) yang rendah (<1.010) menunjukkan tiada masalah multikolineariti dalam model.



Rajah 1: Hasil analisis model pengukuran menunjukkan nilai pemuatan bagi setiap konstruk

Hasil penilaian struktur model menunjukkan kesemua hipotesis adalah signifikan pada aras $p < 0.05$, membuktikan hubungan positif antara faktor teknikal dan keselamatan API seperti ditunjukkan dalam Jadual 1 berikut:

Jadual 1: *Pengujian koefisien lintasan*

Hipotesis	Hubungan Konstruk	Koefisien (β)	Nilai p	Keputusan	Menyokong Kajian Lepas
H1	Berskala & Daya Tahan Tinggi → Reka Bentuk API	-0.197	0.002	Diterima	(Serrano & Oñate, 2021)
H2	Pemantauan Aktiviti API → Berskala & Daya Tahan Tinggi	0.860	0.000	Diterima	(Gawande et al., 2021)
H3	Perlindungan Data & Privasi → Berskala & Daya Tahan Tinggi	0.128	0.040	Diterima	(Hammouda et al., 2015)
H4	Standard Keselamatan → Perlindungan Data & Privasi	0.763	0.000	Diterima	(Hussain, Noye, et al., 2020)

Keputusan menunjukkan Standard Keselamatan mempunyai pengaruh langsung yang kuat terhadap Perlindungan Data dan Privasi, manakala kedua-dua konstruk ini menyumbang kepada peningkatan ketahanan dan kebolehskalaan API, seterusnya memperkukuh reka bentuk API yang lebih selamat dan mampan.

Dapatan ini memperkukuh penemuan kajian terdahulu (Gawande et al., 2021; Hammouda et al., 2015; Hussain et al., 2019; Serrano & Oñate, 2021) yang menegaskan bahawa faktor teknikal seperti pemantauan, kawalan capaian, serta kepatuhan kepada piawaian keselamatan merupakan tunjang utama dalam s keselamatan API. Model ini juga membuktikan bahawa pemantauan aktiviti API secara berterusan bukan sahaja meningkatkan ketahanan sistem, tetapi juga memperkukuh mekanisme kawalan ancaman seperti pencerobohan, kebocoran data, dan serangan siber (Hasan et al., 2023).

Selain itu, dapatan menunjukkan bahawa perlindungan data dan privasi memainkan peranan penting dalam membina kepercayaan pengguna terhadap ekosistem digital kerajaan. Ini seiring dengan pendekatan Dasar Perkongsian Data Sektor Awam (DPDSA) dan inisiatif PADU, yang menekankan keperluan keselamatan, ketelusan, serta kebolehkesanan dalam pengurusan data.

Kesimpulan

Secara keseluruhan, kajian ini membuktikan bahawa faktor kejayaan keselamatan platform API bergantung kepada lima faktor utama yang saling berkait iaitu Standard Keselamatan, Perlindungan Data dan Privasi, Pemantauan Aktiviti API, Berskala dan Daya Tahan Tinggi, serta Reka Bentuk API yang selamat dan modular.

Dapatan ini boleh membantu dalam membangunkan Model Keselamatan API, Prosedur Operasi Standard (SOP) bagi perkongsian data rentas agensi di Malaysia. Melalui pemantauan berterusan, pematuhan piawaian, serta kesedaran keselamatan yang tinggi, organisasi sektor awam mampu memperkukuh ekosistem perkongsian data yang selamat, dipercayai, dan berdaya tahan tinggi.

Penghargaan

Projek ini telah dibiayai oleh dua geran penyelidikan: TT-2023-016 “Rangka Kerja Perkongsian Data Malaysia” dan TT-2023-019 bertajuk “Pembangunan Dasar Perkongsian Data Negeri Selangor”.

Rujukan

Ahmed, S. M. S., & Zulhuda, S. (2019). Data Protection Challenges in The Internet of Things Era: An Assessment of Protection Offered by PDPA 2010. *International Journal of Law Government and Communication*. https://doi.org/10.35631/ijlgc.417001

Amalia, C., Poetry, E. G., Kono, M. K., Kusuma, D. A., & Kurniawan, A. (2020). Legal Issues of Personal Data Protection and Consumer Protection in Open API Payments. *Journal of Central Banking Law and Institutions*, *1*(2).

Amelia Natasya, A. W., Siti Norul Huda, S. A., Monaliza, S., Khairul Akram, Z. A., Umi Asma’, M., Salwani, A., Madihah, M. S., Shafiza, M. S., Bakar Jamili, G., & Ismail, C. A. (2023). *Laporan Teknikal Projek Industri Pembangunan: Pembangunan Dasar Perkongsian Data Bagi Kerajaan Selangor Melalui SelGDX*.

Bairagi, V., & Munot, M. V. (2019). *Research Methodology: A Practical and Scientific Approach*. Chapman and Hall/CRC.

Bond, T. G., & Fox, C. (2015). *Applying the Rasch Model; Fundamental Measurement in the Human Sciences*. Routledge.

Borgogno, O., & Colangelo, G. (2019). Data sharing and interoperability: Fostering innovation and competition through APIs. *Computer Law and Security Review*, *35*(5). https://doi.org/10.1016/j.clsr.2019.03.008

Chai, K. Y., & Zolkipli, M. F. (2021). Review on Confidentiality, Integrity and Availability in Information Security. *Journal of ICT In Education*, *8*(2), 34–42. https://doi.org/10.37134/jictie.vol8.2.4.2021

D’Elia, D. C., Nicchi, S., Mariani, M., Marini, M., & Palmaro, F. (2021). Designing Robust API

Monitoring Solutions. *IEEE Transactions on Dependable and Secure Computing*, *20*(1), 392–406. https://doi.org/10.1109/TDSC.2021.3133729

Data Bridge Market Research. (2023). *Global Application Programming Interfaces (API) Management Market – Industry Trends and Forecast to 2030*. https://www.databridgemarketresearch.com/reports/global-api-management-market

Gawande, A., Gayake, A., Charkha, M., Shewale, S., & Wanjale, K. (2021). Empirical Study On API Security Threats & Exploitation Of Rate Limiting Flaw. *International Journal of Creative Research Thoughts (IJCRT)*. https://ijcrt.org/papers/IJCRT21A6030.pdf

George, D., & Mallery, P. (2016). *IBM SPSS statistics 23 step by step: A simple guide 141 and reference*. Routledge.

Ghani, F. A., Shabri, S. M., Rasli, M. A. M., Razali, N. A., & Shuffri, E. H. A. (2020). An Overview of the Personal Data Protection Act 2010 (PDPA): Problems and Solutions. *Global Business and Management Research: An International Journal*, *12*.

Google, & Temasek & Bain Company. (2022). *e-Conomy SEA 2022*. https://economysea.withgoogle.com/home/

Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). *A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustainable Cities and Society*.

Hammouda, I., Knauss, E., & Costantini, L. (2015). Continuous API Design for Software Ecosystems. *2015 IEEE/ACM 2nd International Workshop on Rapid Continuous Software Engineering (RCoSE)*, *May 2015*. https://doi.org/10.1109/RCoSE.2015.13

Hasan, M. K., Habib, A. K. M. A., Islam, S., Safie, N., Abdullah, S. N. H. S., & Pandey, B. (2023). DDoS: Distributed denial of service attack in communication standard vulnerabilities in smart grid applications and cyber security with recent developments. *Energy Reports*, *9*(June), 1318–1326. https://doi.org/10.1016/j.egyr.2023.05.184

Hasliza, N., Hassan, M., Ahmad, K., & Salehuddin, H. (2020). *Diagnosing the Issues and Challenges in Data Integration Implementation in Public Sector*. *10*(2), 529–535.

Hussain, F., Noye, B., Hussain, R., & Sharieh, S. (2020). Enterprise API Security and GDPR Compliance : Design and Implementation Perspective. *IT Professional*, *22*(5), 81–89. https://doi.org/10.1109/MITP.2020.2973852

Hussain, F., Noye, B., & Sharieh, S. (2019). Current state of API security and machine learning. *IEEE Technology Policy and Ethics*, *4*(2). https://www.ieee.org/content/dam/ieee-org/ieee/web/org/about/futuredirections/future-directions/ieee-future-directions-newsletter-may-2019.pdf

Hussain, F., Salah, R. H., Noye, B., & Sharieh, S. (2020). Enterprise API Security and GDPR Compliance: Design and Implementation Perspective. *IT Professional*, *22*(5).

Jalil, M. R., Harun, Q. N., & Azizi, H. F. M. (2023). The Impact of The Covid-19 Pandemic on The Development of Data Hub & Artificial Intelligence Technology in Malaysia. *International Journal of Interdisciplinary & Strategic Studies*, *4*(6).

Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A Review of Secure and Privacy-Preserving Medical Data Sharing. *IEEE Access*, *7*.

Joe F. Hair Jr, Matthews, L., Matthews, R., & Sarstedt, M. (2017). PLS-SEM or CB-SEM:updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, *1*(2).

Jr., J. F. H., Howard, M. C., & Nitzl, C. (2020). Assessing measurement model quality in PLS-SEM using confirmatory composite analysis. *Journal of Business Research*, *109*.

Krishnamurthy, V. (2020). A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy. Symposium On The GDPR and International Law. *AJIL Unbound*. https://doi.org/doi:10.1017/aju.2019.79

Leng, O. W., & Doris Liew. (2024). An Inquisition into Malaysia's PADU Subsidy Targeting, and Beyond. In *Penang Institute Issues*.

Mändar, R. (2017). *UXP Portal 2.0 Functional Requirements Specification*. https://dspace.ut.ee/bitstreams/89a35789-f3ad-4e7d-b8f3-14ded815e15c/download

Matthes, J. M., & Ball, D. (2018). Discriminant validity assessment in marketing research. *International Journal of Market Research*, *61*(2).

Monaliza, S., Siti Norul Huda, S. A., Madihah, M. S., Azah, A. N., Kamsuriah, A., Hasimi, S., Nurfarahhana, I., Khairul Akram, Z. A., Umi Asma', M., Mohd Haziq, H. N., Azlina, A., Aznul Nizam, N., Novolin, J., & Rafizal, N. (2023). *Laporan Teknikal Projek: PEMBANGUNAN RANGKA KERJA PERKONGSIAN DATA BAGI SEKTOR AWAM MELALUI MyGDX*.

Naz, M., Al-zahrani, F. A., Khalid, R., Javaid, N., Qamar, A. M., Afzal, M. K., & Shafiq, M. (2019). A Secure Data Sharing Platform Using Blockchain and Interplanetary File System. *Sustainability*, *11*. https://doi.org/10.3390/su11247054

Pawan, K., & Rakesh, K. (2019). Issues and Challenges of Load Balancing Techniques in Cloud Computing: A Survey. *ACM Computing Surveys*, *51*(6), 1–35. https://doi.org/https://doi.org/10.1145/3281010

Purwanto, A., & Sudargini, Y. (2021). *Partial Least Squares Structural Squation Modeling (PLS-SEM) Analysis for Social and Management Research : A Literature Review Journal of Industrial Engineering & Management Research*. *2*(4), 114–123.

Serrano, P. A. M., & Oñate, J. J. S. (2021). Integration of RESTFul API to Student Information System for Secured Data Sharing and Single Sign-on. *2021 IEEE 13th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)*. https://doi.org/10.1109/HNICEM54116.2021.9731898

Solove, D. J., & Schwartz, P. M. (2020). *INFORMATION PRIVACY LAW*. Aspen Publishing.

Stiefel, A., & Ananthanarayanan, A. (2023). *API Strategy: Best. Practices for Platform Engineering Leaders*. F5 NGINX.

Sun, S., Ma, H., Song, Z., & Zhang, R. (2022). WebCloud: Web-Based Cloud Storage for Secure Data Sharing Across Platforms. *IEEE Transactions on Dependable and Secure Computing*. https://doi.org/10.1109/TDSC.2020.3040784

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences IJECS-IJENS*, *11*(5).

The Star. (2023). *Selangor launches SelGDX portal for sharing big data across agencies, public sector.*

Tsohou, A., Magkos, E., Mouratidis, H., Chrysoloras, G., Piras, L., Pavlidis, M., Debussche, J., Rotoloni, M., & Crespo, B. G.-N. (2020). Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform. *Information and Computer Security*, *28*(4).

Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU). (2023). *MyGDX : Malaysian Government Data Exchange*. https://www.mygdx.gov.my/ms/landing-page/theme

Yeoh, A. (2023). CyberSecurity Malaysia report: Government sectors suffered most data breaches, while telcos spilled over 400GB of data in H1 2023. *The Star*. https://www.thestar.com.my/tech/tech-news/2023/10/25/cybersecurity-malaysia-report-government-sectors-suffered-most-data-breaches-while-telcos-spilled-over-400gb-of-data-in-h1-2023