

Secure Communication Based on a Classification of Information Security Model (CISM) for Digital Government

Komunikasi Selamat Berasaskan Model Keselamatan Mengikut Pengkelasan Maklumat untuk Kerajaan Digital

Noorazeen Mohd Ali*, Muhamad Azlan Yusof

Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Malaysia

*Corresponding author: Noorazeen Mohd Ali (e-mail: aliazeen@ukm.edu.my)

ABSTRACT

Digital government initiatives increasingly rely on secure digital communication channels to support inter-agency collaboration, service delivery, and data sharing. However, the management of classified and sensitive government information remains challenging due to the risks of data exposure and inadequate access control. This study proposes a Classification Information Security Model (CISM) for Digital Government that integrates information classification, role-based access control, and cryptographic mechanisms to provide security controls according to information sensitivity levels. The proposed model aligns with Malaysian government information classification requirements and supports the implementation of cybersecurity governance frameworks. A proof-of-concept programming package and prototype application were developed to demonstrate the feasibility of the model. Expert validation was conducted to evaluate the suitability and effectiveness of the proposed approach. Findings indicate that CISM can enhance the confidentiality, integrity, and controlled accessibility of government information while supporting secure communication across government agencies. The study contributes a practical security framework that balances security requirements with system performance and operational needs in digital government environments.

Keywords: Digital Government; information security; information classification; access control; cryptography; secure communication; cybersecurity

ABSTRAK

Inisiatif Kerajaan Digital semakin bergantung kepada saluran komunikasi digital yang selamat bagi menyokong kolaborasi antara agensi, penyampaian perkhidmatan dan perkongsian data. Walau bagaimanapun, pengurusan maklumat kerajaan yang sensitif dan terperingkat masih menghadapi cabaran akibat risiko pendedahan data serta kawalan capaian yang tidak mencukupi. Kajian ini mencadangkan Model Keselamatan Mengikut Pengkelasan Maklumat (CISM) yang mengintegrasikan pengkelasan maklumat, kawalan capaian berasaskan peranan dan mekanisme kriptografi untuk menyediakan perlindungan yang bersesuaian mengikut tahap sensitiviti maklumat. Model yang dicadangkan selaras dengan keperluan pengurusan maklumat kerajaan Malaysia serta menyokong pelaksanaan rangka kerja keselamatan siber sektor awam. Sebuah pakej pengaturcaraan dan aplikasi prototaip dibangunkan bagi membuktikan kebolehlaksanaan model tersebut. Pengesahan pakar dilaksanakan bagi menilai kesesuaian dan keberkesanan pendekatan yang dicadangkan. Dapatan menunjukkan bahawa CISM berupaya meningkatkan kerahsiaan, integriti dan kawalan capaian maklumat kerajaan sambil menyokong komunikasi yang lebih selamat antara agensi kerajaan. Kajian ini menyumbang sebuah kerangka keselamatan praktikal yang mengimbangi keperluan keselamatan, prestasi sistem dan keperluan operasi dalam persekitaran Kerajaan Digital.

Kata kunci: Kerajaan Digital; Model Keselamatan Mengikut Pengkelasan Maklumat (CISM); Kawalan Capaian Berasaskan Peranan (RBAC); Kriptografi; Keselamatan Maklumat; Komunikasi Selamat; Keselamatan Siber Sektor Awam

PENGENALAN

Transformasi digital sektor awam telah mempercepat penggunaan aplikasi web, perkhidmatan awan dan platform komunikasi digital bagi meningkatkan kecekapan penyampaian perkhidmatan kerajaan. Walau bagaimanapun, peningkatan penggunaan teknologi digital turut memperluaskan permukaan serangan siber. Ancaman seperti pendedahan data sensitif, kegagalan kriptografi dan kawalan capaian yang lemah terus menjadi antara risiko keselamatan utama dalam aplikasi digital kerajaan.

Kajian ini memberi tumpuan kepada komunikasi antara agensi kerajaan yang melibatkan maklumat terperinci. Walaupun garis panduan keselamatan sedia ada menyediakan prinsip umum berkaitan kawalan capaian dan kriptografi, terdapat keperluan untuk suatu model yang boleh memandu pembangunan aplikasi kerajaan secara konsisten. Oleh itu, kajian ini mencadangkan Model Keselamatan Mengikut Pengkelasan Maklumat (CISM) bagi memastikan pemilihan kawalan keselamatan dibuat berdasarkan tahap sensitiviti maklumat.

KAJIAN BERKAITAN

Kajian terdahulu menunjukkan bahawa kawalan capaian merupakan komponen kritikal dalam keselamatan sistem kerajaan digital. Model seperti Mandatory Access Control (MAC), Role-Based Access Control (RBAC) dan Task-Based Access Control (TBAC) telah digunakan secara meluas bagi mengawal akses kepada maklumat sensitif. Dalam konteks aplikasi kerajaan, RBAC sering digunakan kerana kemampuannya memetakan peranan organisasi kepada hak capaian sistem.

Selain kawalan capaian, penggunaan kriptografi merupakan kaedah utama untuk melindungi maklumat semasa penghantaran dan penyimpanan. Algoritma seperti AES, RSA dan infrastruktur kunci awam digunakan secara meluas untuk menjamin kerahsiaan dan integriti data. Kajian-kajian terkini turut menekankan keperluan pendekatan keselamatan berasaskan risiko dan sensitiviti data, khususnya dalam persekitaran kerajaan digital yang melibatkan perkongsian data merentasi pelbagai agensi.

Walaupun pelbagai model keselamatan telah dicadangkan, kebanyakannya tidak mengambil kira keperluan khusus pengkelasan maklumat kerajaan Malaysia. Justeru, kajian ini mengisi jurang tersebut melalui pembangunan model yang menghubungkan pengkelasan maklumat dengan mekanisme kawalan capaian dan kriptografi yang bersesuaian.

METODOLOGI

Kajian ini menggunakan pendekatan pembangunan model dan prototaip. Fasa pertama melibatkan kajian literatur bagi mengenal pasti ancaman keselamatan, keperluan pengkelasan maklumat kerajaan dan teknologi keselamatan yang relevan. Fasa kedua melibatkan pembangunan model CISM yang mengintegrasikan tiga komponen utama iaitu pengkelasan maklumat, kawalan capaian dan kriptografi.

Seterusnya, sebuah pakej pengaturcaraan dan aplikasi prototaip dibangunkan untuk membuktikan kebolehlaksanaan model. Model ini memetakan tahap klasifikasi maklumat kepada mekanisme kawalan capaian tertentu serta cadangan algoritma kriptografi yang sesuai. Akhir sekali, pengesahan pakar dilaksanakan melalui sesi temu bual bagi menilai kesesuaian model dari sudut keselamatan, kebolegunaan dan potensi pelaksanaan dalam sektor awam.

HASIL DAN PERBINCANGAN

Hasil pembangunan menunjukkan bahawa model CISM mampu mengawal akses kepada maklumat berdasarkan peranan pengguna dan tahap sensitiviti maklumat. Integrasi kawalan capaian dan kriptografi membantu mengurangkan risiko pendedahan data sensitif serta akses tanpa kebenaran. Pembangunan prototaip membuktikan bahawa model boleh diimplementasikan dalam aplikasi web tanpa menjejaskan fungsi asas sistem.

Pengesahan pakar menunjukkan persetujuan bahawa model yang dicadangkan dapat meningkatkan tahap keselamatan komunikasi dalam persekitaran Kerajaan Digital. Pendekatan berasaskan

pengkelasan maklumat membolehkan sumber keselamatan digunakan secara lebih optimum berbanding penggunaan satu tahap perlindungan yang sama untuk semua kategori maklumat.

KESIMPULAN

Kajian ini berjaya mencadangkan dan mengesahkan Model Keselamatan Mengikut Pengkelasan Maklumat (CISM) bagi menyokong komunikasi selamat dalam Kerajaan Digital. Model ini menghubungkan pengkelasan maklumat kerajaan dengan kawalan capaian dan kriptografi yang sesuai bagi meningkatkan kerahsiaan, integriti dan ketersediaan maklumat. Hasil kajian menunjukkan bahawa CISM berpotensi menjadi rujukan bagi pembangunan aplikasi kerajaan yang lebih selamat dan seragam pada masa hadapan.

PENGHARGAAN

Penulis mengucapkan setinggi-tinggi penghargaan kepada Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia. Penghargaan turut ditujukan kepada agensi-agensi sektor awam Malaysia serta pengamal keselamatan siber atas input berharga yang diberikan sepanjang proses pengesahan pakar bagi Model Keselamatan Mengikut Pengkelasan Maklumat (CISM). Penulis juga merakamkan penghargaan kepada semua individu dan organisasi yang telah menyumbang, sama ada secara langsung atau tidak langsung, kepada penyelidikan ini.

RUJUKAN

- Abdullah, N., Ahmad, S., & Yusof, Z. 2025. Cybersecurity governance frameworks for public sector digital transformation, *Government Information Quarterly*.
- Almarabeh, T., & AbuAli, A. 2021. Digital government transformation and cybersecurity challenges, *International Journal of Advanced Computer Science and Applications*.
- Khan, M., Rehman, S., & Alharbi, F. 2023. Information classification and data protection in government information systems, *Computers & Security*.
- Lim, K., Tan, C., & Wong, J. 2026. Secure information sharing frameworks in digital government ecosystems, *Journal of Cyber Policy*.
- OECD. 2024. *2023 OECD Digital Government Index: Results and Key Findings*. OECD Publishing.
- OWASP Foundation. 2021. *OWASP Top 10:2021 – The Ten Most Critical Web Application Security Risks*.
- Rahman, M., Ismail, N., & Hassan, R. 2024. Cryptographic approaches for secure digital government services, *IEEE Access*.
- Sharma, P., Gupta, R., & Singh, A. 2022. Role-based access control models for secure e-government systems, *Journal of Information Security and Applications*.