

TANTANGAN DAN DAMPAK KEAMANAN DATA PADA CLOUD COMPUTING DALAM BISNIS PERUSAHAAN

Irwaldi Hendri Yudi¹, Muhammad Donni Lesmana Siahaan²

Universitas Pembangunan Panca Budi

E-mail: irwaldigendri1@gmail.com¹, donnilesmanasiahaan@gmail.com²

Abstrak

Penelitian ini bertujuan untuk mengidentifikasi tantangan dan dampak keamanan data pada cloud computing dalam konteks bisnis perusahaan. Dalam era digital yang semakin berkembang, banyak perusahaan yang beralih ke teknologi cloud untuk mengelola data dan infrastruktur mereka. Namun, penggunaan cloud computing juga membawa tantangan besar terkait dengan risiko keamanan data, seperti akses tidak sah, kebocoran data, dan ancaman cyber lainnya. Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk menganalisis faktor-faktor yang mempengaruhi keamanan data pada cloud computing dan mengidentifikasi dampaknya terhadap operasional dan reputasi perusahaan. Melalui studi pustaka dan wawancara dengan praktisi TI, penelitian ini menyimpulkan bahwa meskipun cloud computing menawarkan banyak keuntungan, perusahaan perlu mengadopsi strategi keamanan yang lebih kuat, termasuk enkripsi data, pengelolaan akses yang ketat, dan audit sistem yang berkala, untuk mengurangi risiko dan dampak yang terkait dengan masalah keamanan data.

Kata Kunci: Keamanan Data, Cloud Computing, Risiko Keamanan, Strategi Keamanan.

Abstract

This study aims to identify the challenges and impacts of data security in cloud computing within the context of business operations. In an increasingly digital era, many companies are transitioning to cloud technology to manage their data and infrastructure. However, the use of cloud computing also brings significant challenges related to data security risks, such as unauthorized access, data breaches, and other cyber threats. This research employs a descriptive qualitative approach to analyze the factors affecting data security in cloud computing and identify its impacts on company operations and reputation. Through literature review and interviews with IT practitioners, the study concludes that while cloud computing offers many advantages, companies need to adopt stronger security strategies, including data encryption, strict access management, and regular system audits, to mitigate the risks and impacts associated with data security issues.

Keywords: Data Security, Cloud Computing, Security Risks, Security Strategies.

1. PENDAHULUAN

Cloud computing telah berkembang pesat dalam beberapa tahun terakhir dan menjadi salah satu komponen penting dalam strategi teknologi informasi perusahaan. Cloud computing merujuk pada pengelolaan dan penyimpanan data serta aplikasi yang dijalankan melalui server yang terhubung ke internet, bukan disimpan secara fisik di server perusahaan. Dengan adopsi cloud computing, perusahaan dapat mengakses sumber daya TI secara lebih efisien, mengurangi biaya infrastruktur, dan meningkatkan fleksibilitas operasional.

Sebagian besar perusahaan, baik kecil maupun besar, beralih ke cloud computing untuk meningkatkan efisiensi bisnis mereka. Penyediaan layanan berbasis cloud memungkinkan perusahaan untuk mengelola data dan aplikasi secara lebih mudah, dengan pembaruan

perangkat lunak otomatis dan skalabilitas yang lebih baik. Keuntungan ini tidak hanya terbatas pada penghematan biaya, tetapi juga pada peningkatan kinerja, aksesibilitas, dan mobilitas bagi pengguna yang tersebar di berbagai lokasi.

Cloud computing menawarkan berbagai keuntungan bagi perusahaan, seperti efisiensi biaya, skalabilitas, dan fleksibilitas. Namun, di balik manfaatnya, tantangan signifikan muncul terkait dengan aspek keamanan data yang menjadi prioritas utama. Ketergantungan perusahaan pada layanan cloud untuk mengelola data penting—seperti informasi pelanggan, keuangan, dan rahasia bisnis—menjadikan perlindungan data sebagai hal yang kritis. Risiko seperti kebocoran data, serangan cyber, atau akses tidak sah dapat mengancam kelangsungan operasional dan reputasi perusahaan. Oleh karena itu, memahami ancaman-ancaman ini serta dampaknya terhadap bisnis menjadi langkah awal dalam merancang strategi keamanan yang lebih baik.

Keamanan data dalam komputasi awan mencakup pendekatan multifaset untuk melindungi informasi sensitif dari ancaman eksternal dan kesalahan manajemen akses internal. Organisasi harus menerapkan langkah-langkah keamanan yang kuat, termasuk enkripsi, kontrol akses, dan kepatuhan terhadap peraturan seperti GDPR dan HIPAA, untuk melindungi data sepanjang siklus hidupnya. Salah satu aspek utama dalam menjaga keamanan data adalah menghadapi ancaman eksternal yang terus berkembang. Lingkungan cloud sangat rentan terhadap berbagai bentuk serangan cyber, termasuk peretasan dan ransomware, yang secara langsung dapat mengancam integritas serta kerahasiaan data. Selain itu, pelanggaran data yang disebabkan oleh akses tidak sah maupun kesalahan konfigurasi sistem menjadi tantangan serius yang harus ditangani melalui pemantauan berkelanjutan dan penerapan strategi manajemen ancaman yang efektif.

Oleh karena itu, perusahaan perlu mengambil pendekatan proaktif dalam mengamankan data di cloud, mulai dari penerapan enkripsi end-to-end, autentikasi multi-faktor, hingga pemantauan sistem secara real-time. Kolaborasi dengan penyedia layanan cloud yang terpercaya dan memiliki rekam jejak keamanan yang kuat juga menjadi kunci penting. Dengan langkah-langkah ini, perusahaan dapat meminimalkan risiko sekaligus memastikan bahwa manfaat cloud computing tetap optimal tanpa mengorbankan aspek keamanan. Keamanan data bukan lagi sekadar opsi, melainkan fondasi yang harus dibangun untuk menjaga keberlanjutan bisnis di era digital.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif untuk menganalisis tantangan dan dampak keamanan data pada cloud computing dalam konteks bisnis perusahaan, dengan mengumpulkan data melalui studi pustaka terhadap jurnal ilmiah, buku, dan laporan terkait serta wawancara mendalam dengan praktisi keamanan TI dan pengelola data perusahaan guna mendapatkan pemahaman komprehensif tentang risiko dan praktik di lapangan. Analisis data dilakukan secara induktif dengan mengidentifikasi pola dan tema seperti ancaman eksternal (peretasan, ransomware), risiko internal (penyalahgunaan akses, kesalahan konfigurasi), dan strategi mitigasi (enkripsi, manajemen identitas) untuk kemudian dikembangkan menjadi rekomendasi praktis berupa peningkatan protokol keamanan, kerangka kerja kepatuhan regulasi, serta program pelatihan karyawan yang dapat diimplementasikan perusahaan guna mengurangi dampak negatif ancaman keamanan data. Hasil penelitian ini diharapkan tidak hanya memberikan pemahaman mendalam tentang tantangan keamanan cloud computing tetapi juga menjembatani kesenjangan antara teori keamanan cyber dengan kebutuhan praktis bisnis di era digital yang terus berkembang.

3. HASIL DAN PEMBAHASAN

Konsep Dasar Cloud Computing

Cloud computing adalah model pengelolaan dan penyediaan sumber daya TI yang memungkinkan akses data, aplikasi, dan layanan melalui internet, tanpa memerlukan perangkat keras atau perangkat lunak yang terpasang secara fisik di lokasi pengguna. Secara umum, cloud computing menawarkan pengelolaan sumber daya komputer, termasuk penyimpanan data dan pemrosesan informasi, secara virtual. Layanan cloud ini biasanya disediakan oleh penyedia pihak ketiga yang mengelola infrastruktur dan perangkat keras yang diperlukan untuk memastikan operasional yang efektif. Cloud computing dibagi menjadi tiga jenis utama: public cloud, di mana layanan dan sumber daya TI dibagi dengan pengguna lain dan dikelola oleh penyedia cloud; private cloud, yang digunakan oleh satu organisasi dengan kontrol lebih besar atas pengelolaannya; dan hybrid cloud, yang menggabungkan keduanya, memberikan fleksibilitas bagi organisasi untuk memilih layanan yang sesuai dengan kebutuhan tertentu.

Cloud computing memberikan fungsi yang sangat beragam dalam operasional bisnis. Salah satu fungsi utama cloud computing adalah sebagai sarana penyimpanan data yang memungkinkan perusahaan menyimpan data dalam jumlah besar dengan biaya yang lebih terjangkau dibandingkan jika harus mengelola server fisik sendiri. Selain itu, cloud computing mendukung pemrosesan data dalam skala besar, yang memberikan keuntungan bagi perusahaan dalam menganalisis dan mengelola data mereka secara lebih efisien. Aplikasi berbasis cloud juga semakin populer karena memungkinkan karyawan untuk mengakses perangkat lunak yang dibutuhkan tanpa harus menginstalnya di setiap perangkat. Oleh karena itu, cloud computing menyediakan platform yang efisien dan terjangkau untuk mendukung berbagai aplikasi yang esensial bagi kelangsungan bisnis perusahaan.

Keuntungan utama dari cloud computing bagi perusahaan adalah efisiensi biaya yang signifikan. Dengan cloud computing, perusahaan tidak perlu mengeluarkan biaya besar untuk membeli perangkat keras atau membangun infrastruktur TI yang mahal. Sebagai gantinya, perusahaan hanya membayar untuk sumber daya yang mereka gunakan, dengan model berbasis langganan atau penggunaan. Keuntungan lain yang tak kalah penting adalah skalabilitas, yang memungkinkan perusahaan menambah atau mengurangi kapasitas penyimpanan dan pemrosesan sesuai dengan kebutuhan. Jika permintaan meningkat, perusahaan dapat dengan mudah menyesuaikan kapasitasnya, dan sebaliknya, mengurangi biaya ketika permintaan menurun. Fleksibilitas yang ditawarkan oleh cloud computing sangat berharga bagi perusahaan yang menginginkan kecepatan dan adaptasi yang tinggi dalam lingkungan bisnis yang dinamis.

Selain itu, cloud computing menawarkan fleksibilitas yang tinggi dalam hal pengelolaan aplikasi dan data. Perusahaan dapat mengakses aplikasi dan data mereka dari mana saja di dunia selama ada koneksi internet, yang sangat meningkatkan mobilitas karyawan dan memungkinkan kolaborasi lintas lokasi. Ini sangat bermanfaat untuk perusahaan dengan tim yang tersebar di berbagai tempat atau dengan pekerja yang sering bekerja dari jarak jauh. Dengan cloud computing, karyawan dapat mengakses dan bekerja dengan data secara real-time tanpa adanya hambatan teknis atau keterbatasan geografis. Ini juga mempercepat proses pengambilan keputusan dan meningkatkan produktivitas tim.

Cloud computing secara signifikan meningkatkan kolaborasi tim melalui aplikasi berbasis cloud yang memungkinkan banyak pengguna bekerja sama secara real-time pada proyek yang sama, seperti yang ditunjukkan oleh platform Google Drive dan Microsoft 365, sehingga mempercepat proses kerja dan meningkatkan hasil kolaborasi. Namun, di balik

manfaatnya yang mencakup efisiensi biaya, fleksibilitas akses, dan peningkatan kolaborasi, perusahaan harus tetap memperhatikan risiko keamanan data yang muncul akibat pengelolaan data di luar infrastruktur internal. Oleh karena itu, pemilihan penyedia layanan cloud yang andal dan penerapan protokol keamanan yang ketat menjadi krusial untuk memastikan perlindungan data sensitif, sehingga perusahaan dapat memanfaatkan seluruh keunggulan cloud computing tanpa mengorbankan aspek keamanan yang vital bagi kelangsungan bisnis.

Tantangan Keamanan Data pada Cloud Computing

Cloud computing memang memberikan berbagai keuntungan dalam hal efisiensi dan fleksibilitas operasional perusahaan, namun juga menghadirkan tantangan keamanan data yang kompleks. Salah satu risiko utama adalah ancaman akses tidak sah melalui metode seperti phishing atau eksploitasi celah keamanan, yang dapat membahayakan data sensitif perusahaan. Untuk mengatasi ini, diperlukan penerapan autentikasi dua faktor dan kontrol akses yang ketat. Selain itu, keamanan data selama proses transfer juga rentan terhadap serangan man-in-the-middle, sehingga penggunaan enkripsi end-to-end menjadi solusi penting untuk melindungi informasi yang dikirimkan melalui internet.

Ancaman lain yang tidak kalah serius adalah potensi kehilangan data akibat kesalahan manusia, kerusakan sistem, atau serangan ransomware yang dapat melumpuhkan operasional perusahaan. Untuk memitigasi risiko ini, perusahaan perlu membangun sistem backup yang andal dan menyusun strategi pemulihan data yang komprehensif. Tanpa mekanisme pemulihan yang memadai, kehilangan data dapat mengakibatkan gangguan operasi yang berkepanjangan dan kerugian finansial yang besar.

Di samping tantangan teknis, perusahaan juga harus menghadapi kompleksitas kepatuhan terhadap berbagai regulasi perlindungan data seperti GDPR dan HIPAA. Penyimpanan data di cloud mengharuskan perusahaan memastikan bahwa penyedia layanan memenuhi semua persyaratan hukum yang berlaku. Ketidakpatuhan terhadap regulasi ini tidak hanya berpotensi menimbulkan denda besar, tetapi juga dapat merusak reputasi perusahaan dan mengakibatkan konsekuensi hukum yang serius. Oleh karena itu, pemilihan penyedia cloud yang memenuhi standar keamanan dan regulasi menjadi aspek krusial dalam strategi keamanan data perusahaan.

Dampak Keamanan Data pada Bisnis Perusahaan

Pelanggaran keamanan data dapat menimbulkan konsekuensi multidimensi bagi perusahaan, terutama dalam aspek finansial dan operasional. Kebocoran data atau serangan cyber tidak hanya berpotensi menimbulkan kerugian langsung berupa denda regulasi (seperti GDPR atau HIPAA) dan biaya pemulihan sistem, tetapi juga menyebabkan kerugian tidak langsung seperti terhentinya operasional bisnis akibat serangan ransomware. Lebih buruk lagi, perusahaan mungkin kehilangan pendapatan selama periode pemulihan dan menghadapi biaya hukum yang signifikan.

Dampak reputasi sering kali lebih sulit diukur namun lebih berkelanjutan. Kepercayaan pelanggan—yang merupakan aset tak berwujud paling berharga—dapat hancur dalam sekejap ketika data mereka bocor. Pemulihan reputasi membutuhkan waktu bertahun-tahun dan investasi besar dalam kampanye transparansi serta program keamanan yang lebih ketat. Selain itu, gangguan pada rantai pasokan akibat ketidakstabilan sistem cloud dapat merusak hubungan dengan mitra bisnis, bahkan berpotensi mengakibatkan kehilangan kontrak strategis.

Dari perspektif strategis, perusahaan juga harus mengalokasikan anggaran tambahan untuk meningkatkan keamanan cyber pascainsiden, termasuk pelatihan karyawan, teknologi enkripsi mutakhir, dan konsultan keamanan. Tantangan regulasi yang semakin ketat turut

memaksa perusahaan untuk berinvestasi dalam sistem kepatuhan, karena kegagalan memenuhi standar perlindungan data dapat memicu sanksi berlapis. Dengan demikian, pendekatan proaktif dalam manajemen risiko keamanan cloud bukan lagi opsi, melainkan kebutuhan kritis untuk menjaga keberlanjutan bisnis di era digital.

Strategi Mengatasi Tantangan Keamanan Data pada Cloud Computing

Untuk mengatasi tantangan keamanan data dalam penggunaan cloud computing, perusahaan perlu menerapkan pendekatan berlapis yang mencakup langkah teknis dan non-teknis. Salah satu strategi teknis utama adalah enkripsi data, baik saat data disimpan (at rest) maupun saat dikirim (in transit). Enkripsi end-to-end memastikan bahwa meskipun data berhasil disusupi oleh pihak tidak berwenang, informasi di dalamnya tetap tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Selain itu, pengelolaan akses yang ketat melalui penerapan autentikasi multi-faktor (MFA) sangat penting untuk mengurangi risiko akses ilegal. MFA memberikan perlindungan tambahan dengan meminta pengguna menunjukkan lebih dari satu bukti identitas sebelum dapat mengakses sistem, sehingga memperkecil kemungkinan pembobolan meskipun kredensial akun berhasil dicuri.

Perusahaan juga perlu melakukan audit keamanan secara berkala dan pemantauan sistem secara real-time untuk mendeteksi potensi ancaman sejak dini. Audit membantu menemukan celah keamanan yang tidak terdeteksi sebelumnya, sementara sistem pemantauan memungkinkan respons cepat terhadap aktivitas mencurigakan. Pemilihan penyedia layanan cloud yang terpercaya juga sangat penting. Penyedia yang baik akan menawarkan fitur-fitur keamanan seperti enkripsi, mitigasi serangan cyber, dan transparansi dalam pengelolaan data. Sertifikasi keamanan serta reputasi penyedia harus menjadi bahan pertimbangan utama dalam pengambilan keputusan.

Aspek manusia juga memegang peranan penting dalam menjaga keamanan data. Banyak kebocoran terjadi karena kesalahan pengguna, bukan semata karena celah teknis. Oleh karena itu, pelatihan dan edukasi keamanan bagi karyawan harus dilakukan secara berkala. Karyawan perlu dibekali pemahaman tentang pentingnya penggunaan kata sandi yang kuat, cara mengenali ancaman seperti phishing, serta kebijakan internal tentang pengelolaan data sensitif. Selain itu, keamanan aplikasi cloud yang digunakan oleh perusahaan juga harus dipastikan melalui proses audit dan verifikasi yang ketat.

Dengan membangun budaya keamanan yang menyeluruh di seluruh lini organisasi, perusahaan dapat secara efektif melindungi data sensitif mereka dari berbagai ancaman yang terus berkembang.

Studi Kasus

Salah satu contoh serangan keamanan yang cukup menggemparkan dunia bisnis adalah kebocoran data pada layanan Amazon Web Services (AWS) tahun 2017. Kasus ini terjadi karena kesalahan konfigurasi oleh pihak ketiga pengguna layanan AWS, yang menyebabkan informasi pribadi jutaan pengguna seperti nama, alamat, dan nomor kartu kredit dapat diakses publik. Meski AWS tidak bersalah secara langsung, kasus ini menyoroti pentingnya pemahaman konfigurasi keamanan oleh penyewa layanan cloud. Contoh lainnya adalah serangan ransomware pada 2019 yang menargetkan perusahaan penyedia cloud besar. Penyerang mengenkripsi data penting dan menuntut tebusan, menyebabkan gangguan operasional yang signifikan. Insiden ini memperlihatkan bahwa ancaman bukan hanya pada pencurian data, tetapi juga pada hilangnya akses terhadap sistem inti perusahaan.

Dari kedua kasus tersebut, terdapat pelajaran penting yang dapat diterapkan oleh perusahaan dalam mitigasi risiko. Penting bagi setiap pengguna layanan cloud untuk melakukan audit konfigurasi secara rutin serta menerapkan manajemen akses yang ketat

seperti autentikasi multi-faktor dan prinsip least privilege. Dalam menghadapi ancaman ransomware, perusahaan harus menyiapkan sistem cadangan (backup) yang aman dan terisolasi dari jaringan utama, serta menguji secara berkala kemampuan pemulihan data. Dengan langkah-langkah ini, dampak serangan dapat ditekan secara signifikan dan pemulihan dapat berlangsung cepat.

Lebih jauh lagi, kedua kasus tersebut menegaskan pentingnya memilih penyedia layanan cloud yang terpercaya dan memiliki rekam jejak keamanan yang baik. Penyedia harus mematuhi standar keamanan industri dan menyediakan fitur seperti enkripsi, pemantauan real-time, dan prosedur pemulihan bencana yang jelas. Selain itu, perusahaan juga harus memperkuat kesadaran keamanan di kalangan karyawan melalui pelatihan rutin tentang praktik perlindungan data dan identifikasi ancaman seperti phishing. Keamanan data di cloud adalah tanggung jawab bersama—bukan hanya milik penyedia layanan, tetapi juga bagian dari strategi menyeluruh perusahaan dalam menjaga kelangsungan bisnis di era digital.

4. KESIMPULAN

Keamanan data dalam cloud computing merupakan tantangan besar yang harus dihadapi oleh perusahaan di era digital saat ini. Serangan cyber seperti kebocoran data dan serangan ransomware dapat menyebabkan kerugian finansial yang signifikan, merusak reputasi perusahaan, serta mengganggu operasional dan kepatuhan terhadap regulasi yang berlaku. Oleh karena itu, perusahaan harus memiliki kebijakan dan strategi keamanan yang komprehensif, mulai dari enkripsi data, pengelolaan akses yang ketat, hingga audit dan pemantauan sistem secara berkala. Pemilihan penyedia layanan cloud yang terpercaya dan transparansi dalam pengelolaan data juga menjadi faktor penting untuk memastikan perlindungan data yang optimal.

Perusahaan sebaiknya melakukan investasi yang signifikan dalam pelatihan keamanan cyber bagi karyawan serta pengembangan sistem backup dan pemulihan data yang efektif. Mengadopsi autentikasi multi-faktor dan memastikan konfigurasi yang benar untuk sistem cloud dapat mencegah kebocoran data akibat kesalahan manusia dan akses tidak sah. Selain itu, perusahaan harus melakukan evaluasi dan audit berkala terhadap penyedia cloud yang dipilih untuk memastikan bahwa mereka memenuhi standar keamanan yang ketat. Dengan langkah-langkah ini, perusahaan dapat mengurangi risiko ancaman keamanan yang ada dan memitigasi dampak dari potensi serangan di masa depan.

5. DAFTAR PUSTAKA

- Agus Setiawan. Keamanan Jaringan dan Informasi di Era Digital. Jakarta: Penerbit Informatika, 2020.
- Alugoku, N. R. "Data Protection in the Cloud: Ensuring Security and Compliance for Organizational Data." *International Journal For Science Technology And Engineering*, vol. 12, no. 12, 2024, hlm. 1590–1596. <https://doi.org/10.22214/ijraset.2024.66087>.
- Arief Gunawan. Manajemen Keamanan Data dalam Sistem Informasi. Bandung: Pustaka Setia, 2018.
- Dedi Setiawan. Pengelolaan Risiko Keamanan Data di Cloud. Surabaya: Pustaka Belajar, 2018.
- Dwi Handayani. Keamanan Data dalam Teknologi Cloud. Semarang: Salemba Empat, 2020.
- Fitriya Hadi. Cloud Computing untuk Bisnis Modern. Malang: Kencana, 2019.
- Iwan Sutrisno. Strategi Keamanan Sistem Informasi. Surabaya: UB Press, 2017.
- Joko Santoso. Keamanan Jaringan Komputer dan Cloud Computing. Yogyakarta: Graha Ilmu, 2020.
- Lesmana, M. D., & Hermansyah, H. "Rancang Bangun Sistem Absensi Menggunakan E-KTP dengan Memanfaatkan Cloud Google Spreadsheet sebagai Media Penyimpanan Berbasis IoT di Politeknik Adiguna Maritim Indonesia Medan." *Journal of Maritime and Education (JME)*, vol. 7, no. 1, 2025, hlm. 808–813.

- Muhamad. Bank Syari'ah: Analisis Kekuatan, Peluang, Kelemahan dan Ancaman. Yogyakarta: Pustaka Pelajar, 2004.
- Nani Widjaja. Aspek Hukum dalam Keamanan Cloud Computing. Bandung: Alfabeta, 2021.
- Ratna Dewi. Penerapan Keamanan Cloud Computing di Perusahaan. Jakarta: RajaGrafindo, 2021.
- Reddy, H. M. "Cloud Security Compliance: Challenges, Solutions, and Impact on Enterprises." *International Journal For Multidisciplinary Research*, vol. 5, no. 4, 2023. <https://doi.org/10.36948/ijfmr.2023.v05i04.19118>.
- Rini Prastiti. Teknologi Cloud Computing dan Keamanannya. Yogyakarta: Andi Offset, 2019.
- Siahaan, A. P. U., Azhar, Z., Siahaan, M. D. L., Iqbal, M., Ramadhan, Z., Fitriani, W., ... & Azir, K. N. F. K. "Comparative Study of Prim and Genetic Algorithms in Minimum Spanning Tree and Travelling Salesman Problem." *International Journal of Engineering and Technology (UAE)*, vol. 7, no. 4, 2018, hlm. 3654–3661.
- Siahaan, M. D. L., Iskandar, I., & Saragih, M. D. A. "Implementation of Hospital Search Application in Binjai Area Using Method Djikstra." *Journal of Science and Social Research*, vol. 7, no. 4, 2024, hlm. 1570–1577.