

Analisis Keamanan Sistem Informasi Terhadap Data Pribadi Pada Sosial Media Facebook

M.Rizqy Pratama¹, Putri²

^{1,2}Prodi Sistem Informasi, Fakultas Teknik dan Ilmu Komputer, Universitas Islam Indragiri,

Email: rizkygeming97@gmail.com¹, putriv8v0@gmail.com²

ABSTRAK

Keamanan data pribadi di media sosial seperti Facebook menjadi isu krusial di era digital saat ini, mengingat berbagai ancaman yang mungkin timbul. Penelitian ini bertujuan untuk menilai aspek perlindungan data pribadi di Facebook melalui pendekatan kualitatif deskriptif. Metode yang digunakan meliputi tinjauan literatur, analisis studi kasus (khususnya kasus Cambridge Analytica), dan wawancara semi-terstruktur dengan pengguna Facebook. Temuan penelitian mengungkapkan bahwa meskipun Facebook telah mengimplementasikan langkah-langkah keamanan seperti enkripsi dan autentikasi dua faktor, terdapat kekurangan dalam kebijakan privasi dan pelaksanaan sistem keamanannya. Kasus seperti Cambridge Analytica menunjukkan adanya kelemahan dalam perlindungan data pribadi yang memerlukan perbaikan. Wawancara dengan pengguna mengungkapkan ketidakpahaman mereka tentang pengaturan privasi dan perlindungan data mereka. Rekomendasi penelitian ini mencakup peningkatan transparansi kebijakan privasi, edukasi pengguna mengenai pengaturan privasi, serta penerapan dan penilaian teknologi keamanan yang lebih baik untuk memperkuat perlindungan data pribadi di Facebook.

Kata Kunci: perlindungan data pribadi, Facebook, kebijakan privasi, enkripsi, analisis kasus

ABSTRACT

The protection of personal data on social media platforms like Facebook has become a crucial issue in the digital age, given the various threats that may arise. This study aims to assess the aspects of personal data security on Facebook using a qualitative descriptive approach. Methods employed include literature review, case study analysis (specifically the Cambridge Analytica case), and semi-structured interviews with Facebook users. The findings reveal that, although Facebook has implemented security measures such as encryption and two-factor authentication, there are shortcomings in its privacy policies and security system implementation. Incidents like Cambridge Analytica highlight weaknesses in personal data protection that need addressing. Interviews with users indicate their lack of understanding regarding privacy settings and data protection. The study recommends enhancing privacy policy transparency, educating users about privacy settings, and applying and evaluating better security technologies to strengthen personal data protection on Facebook.

Keywords: personal data protection, Facebook, privacy policy, encryption, case study

1 PENDAHULUAN

Dalam era teknologi informasi yang terus berkembang, sistem informasi memainkan peran krusial dalam mendukung fungsi dan manajemen organisasi di berbagai bidang. Sistem ini melibatkan integrasi perangkat keras, perangkat lunak, data, prosedur, dan interaksi manusia untuk memfasilitasi pengambilan keputusan serta pengendalian organisasi [1]. Keamanan sistem informasi menjadi aspek penting untuk memastikan bahwa data dan informasi terlindungi dari potensi ancaman yang dapat merusak integritas, kerahasiaan, dan ketersediaan data [2]. Langkah-langkah keamanan yang efektif meliputi kontrol akses, enkripsi, audit, serta pelatihan pengguna untuk menjaga data sensitif dari serangan siber dan pelanggaran privasi.



Gambar 1 Facebook

Facebook, sebagai salah satu platform media sosial terbesar, telah mengalami pertumbuhan signifikan sejak diluncurkan oleh Mark Zuckerberg pada tahun 2004 [3]. Platform ini memungkinkan pengguna untuk berinteraksi, berbagi konten, dan terhubung dengan komunitas di seluruh dunia. Meskipun menyediakan berbagai fitur yang memfasilitasi komunikasi dan berbagi informasi, Facebook menghadapi tantangan besar dalam hal melindungi data pribadi penggunanya. Data yang dikumpulkan oleh Facebook mencakup berbagai informasi seperti identitas, lokasi, preferensi, dan aktivitas online pengguna. Pengelolaan data ini sangat penting untuk mencegah risiko seperti pencurian identitas, pelanggaran privasi, dan serangan phishing [4].

Beberapa insiden pelanggaran data besar, seperti kasus Cambridge Analytica, telah mengungkapkan adanya kelemahan dalam kebijakan privasi dan sistem keamanan Facebook [5]. Kasus tersebut menunjukkan perlunya perbaikan dalam transparansi dan kontrol pengguna atas data pribadi mereka. Meskipun Facebook telah menerapkan teknologi keamanan seperti enkripsi dan autentikasi dua faktor, masih terdapat kekurangan dalam implementasi kebijakan privasi yang perlu ditingkatkan.

Penelitian ini bertujuan untuk mengevaluasi berbagai aspek keamanan data pribadi di Facebook melalui pendekatan kualitatif deskriptif. Dengan melakukan tinjauan pustaka, studi kasus, dan wawancara dengan pengguna, penelitian ini ingin mengidentifikasi kelemahan dalam kebijakan privasi Facebook dan memberikan rekomendasi untuk meningkatkan perlindungan data pribadi di platform tersebut. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan praktik keamanan yang lebih baik di media sosial serta meningkatkan pemahaman dan kesadaran pengguna mengenai perlindungan data pribadi mereka.

2 LANDASAN TEORI

Keamanan Sistem Informasi

Sistem informasi adalah kombinasi dari teknologi informasi dan aktivitas manusia yang menggunakan teknologi tersebut untuk mendukung operasi dan manajemen organisasi. Komponen utama dari sistem informasi mencakup perangkat keras, perangkat lunak, data, prosedur, dan manusia yang bekerja secara sinergis untuk mengumpulkan, memproses, menyimpan, dan menyebarkan informasi yang relevan guna mendukung pengambilan keputusan dan kontrol organisasi[6]. Keamanan sistem informasi, dalam konteks ini, mengacu pada praktik dan kebijakan yang diterapkan untuk melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan yang tidak sah. Hal ini melibatkan berbagai aspek seperti kontrol akses, enkripsi, audit keamanan, dan pelatihan keamanan bagi pengguna untuk memastikan bahwa data yang sensitif, termasuk data pribadi pengguna di media sosial seperti Facebook, terlindungi dengan baik dari berbagai ancaman keamanan siber. Peningkatan kesadaran akan pentingnya keamanan data pribadi sangat krusial mengingat meningkatnya insiden pelanggaran data dan serangan siber yang menargetkan platform media sosial besar[7].

Sosial Media Facebook

Facebook merupakan salah satu platform media sosial terbesar yang diluncurkan oleh Mark Zuckerberg pada tahun 2004[8]. Platform ini memungkinkan pengguna untuk berinteraksi, berbagi konten, dan berkomunikasi dengan teman, keluarga, serta berbagai komunitas di seluruh dunia.

Beberapa fitur yang disediakan oleh Facebook termasuk pembaruan status, pengiriman pesan, berbagi foto dan video, serta grup dan halaman untuk komunitas dan bisnis.

Dalam hal keamanan sistem informasi, Facebook menghadapi berbagai tantangan dalam melindungi data pribadi pengguna. Data yang dikumpulkan oleh Facebook meliputi informasi identitas, lokasi, preferensi, dan aktivitas online pengguna. Melindungi data ini sangat penting mengingat risiko penyalahgunaan yang dapat terjadi, seperti pencurian identitas, pelanggaran privasi, dan serangan phishing[9].

Untuk melindungi data pengguna, Facebook telah mengimplementasikan berbagai langkah keamanan, termasuk enkripsi, autentikasi dua faktor, dan audit keamanan berkala. Selain itu, kebijakan privasi dan kontrol pengguna terhadap data pribadi mereka terus diperbarui untuk memenuhi standar keamanan dan peraturan yang berlaku, seperti General Data Protection Regulation (GDPR) di Uni Eropa[10]. Meskipun demikian, insiden pelanggaran data besar seperti kasus Cambridge Analytica telah menunjukkan perlunya peningkatan terus-menerus dalam kebijakan dan praktik keamanan.

Tantangan utama dalam menjaga keamanan data pribadi di Facebook tidak hanya melibatkan teknologi, tetapi juga aspek edukasi pengguna tentang pentingnya menjaga informasi pribadi dan menerapkan praktik keamanan yang baik. Penelitian lebih lanjut dalam bidang ini sangat diperlukan untuk mengidentifikasi metode yang lebih efektif dalam melindungi data pribadi di platform media sosial.

3 METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif untuk menganalisis keamanan sistem informasi terhadap data pribadi pengguna Facebook. Data dikumpulkan melalui beberapa metode, termasuk tinjauan literatur, studi kasus, dan wawancara semi-terstruktur dengan pengguna Facebook.

Tinjauan literatur dilakukan dengan mempelajari berbagai sumber yang relevan, seperti artikel ilmiah, buku, dan laporan penelitian tentang keamanan data pribadi di media sosial. Studi kasus melibatkan analisis insiden keamanan data yang telah terjadi di Facebook, termasuk kasus Cambridge Analytica, untuk memahami kelemahan dan tantangan dalam melindungi data pengguna.

Wawancara semi-terstruktur dengan pengguna Facebook bertujuan untuk mengumpulkan informasi mengenai persepsi dan pengalaman mereka terkait keamanan data pribadi di platform tersebut. Data yang diperoleh dari berbagai sumber ini kemudian dianalisis menggunakan teknik analisis tematik untuk mengidentifikasi pola dan tema utama terkait keamanan data pribadi di Facebook. Hasil analisis ini akan digunakan untuk mengembangkan rekomendasi yang dapat membantu meningkatkan keamanan data pribadi di platform media sosial tersebut.

4 HASIL DAN PEMBAHASAN

Deskripsi Data

Pertama, tinjauan literatur dilakukan untuk mengumpulkan informasi dari artikel akademis, buku, dan laporan yang berkaitan dengan keamanan data pribadi di platform media sosial. Sumber-sumber ini dipilih untuk memberikan dasar teoritis dan wawasan mendalam mengenai isu-isu keamanan informasi yang ada di Facebook. Literatur yang ditinjau mencakup kajian tentang pelanggaran data, kebijakan keamanan, serta langkah-langkah perlindungan yang diterapkan oleh Facebook.

Kedua, studi kasus berfokus pada insiden keamanan yang signifikan, seperti kasus Cambridge Analytica, untuk mengevaluasi bagaimana data pribadi pengguna dapat disalahgunakan dan mengidentifikasi kelemahan dalam sistem keamanan Facebook. Data yang digunakan dalam studi kasus mencakup laporan investigasi, artikel berita, serta dokumentasi yang relevan dengan kejadian tersebut.

Ketiga, wawancara semi-terstruktur dilakukan dengan beberapa pengguna Facebook untuk menggali pandangan dan pengalaman mereka terkait keamanan data pribadi. Responden wawancara dipilih secara acak untuk memastikan representasi yang beragam dari berbagai demografi dan pola penggunaan Facebook. Wawancara ini bertujuan untuk mendapatkan informasi tentang pemahaman pengguna mengenai kebijakan privasi, pengalaman dengan masalah keamanan, dan langkah-langkah yang mereka ambil untuk melindungi data pribadi mereka di Facebook.

Temuan Utama

Penelitian ini mengungkapkan beberapa hal krusial terkait dengan keamanan data pribadi di Facebook. Berdasarkan tinjauan literatur, meskipun Facebook telah menerapkan berbagai langkah keamanan seperti enkripsi data dan autentikasi dua faktor, terdapat beberapa kekurangan dalam kebijakan privasi dan pelaksanaan sistem keamanan yang memengaruhi perlindungan data pribadi. Misalnya, banyak pengguna yang kurang memahami pengaturan privasi mereka, yang dapat meningkatkan risiko data mereka terpapar atau disalahgunakan.

Studi kasus menunjukkan bahwa insiden pelanggaran data besar, seperti kasus Cambridge Analytica, menyoroti adanya celah dalam sistem keamanan dan kebijakan privasi Facebook. Kasus ini mengilustrasikan bagaimana data pribadi dapat dikumpulkan dan digunakan tanpa izin yang jelas dari pengguna, menunjukkan perlunya peningkatan dalam transparansi dan kontrol pengguna terhadap data mereka.

Hasil wawancara dengan pengguna Facebook mengungkapkan bahwa banyak pengguna merasa cemas tentang privasi mereka, namun sering kali merasa tidak memiliki pengetahuan atau alat yang cukup untuk melindungi data mereka dengan baik. Sebagian besar responden mengakui bahwa mereka jarang mengelola pengaturan privasi atau memahami sepenuhnya hak-hak mereka terkait data pribadi yang mereka berikan kepada platform.

Analisis Data

Analisis data dalam penelitian ini dirancang untuk mengevaluasi informasi yang telah dikumpulkan dari berbagai sumber guna mengidentifikasi pola dan tema utama terkait dengan keamanan data pribadi di Facebook. Proses ini melibatkan pengkodean data dari tinjauan literatur, studi kasus, dan wawancara dengan pengguna Facebook, yang kemudian dikelompokkan ke dalam kategori tematik untuk analisis lebih mendalam.

Melalui tinjauan literatur, terungkap bahwa meskipun Facebook menerapkan teknologi keamanan seperti enkripsi dan autentikasi dua faktor, terdapat beberapa kelemahan dalam kebijakan privasi dan kontrol pengguna. Penelitian menunjukkan bahwa meskipun teknologi canggih sudah diterapkan, masalah privasi tetap ada, terutama terkait dengan pengumpulan dan penggunaan data pribadi oleh pihak ketiga. Literatur juga menunjukkan bahwa kebijakan privasi Facebook sering kali sulit dipahami, yang mengakibatkan ketidaktahuan pengguna tentang bagaimana data mereka diatur dan dilindungi.

Studi kasus, seperti kasus Cambridge Analytica, mengungkapkan bagaimana celah dalam perlindungan data dapat dimanfaatkan untuk tujuan yang merugikan. Kasus ini menyoroti pentingnya evaluasi dan perbaikan berkala terhadap kebijakan dan praktik keamanan untuk mencegah insiden serupa di masa depan. Temuan dari kasus ini menunjukkan perlunya tindakan lebih lanjut untuk menjaga integritas dan keamanan data pribadi di platform besar seperti Facebook.

Hasil wawancara dengan pengguna Facebook memberikan wawasan tentang pandangan dan pengalaman mereka terkait pengelolaan data pribadi. Banyak pengguna merasa kurang paham mengenai pengaturan privasi dan bagaimana melindungi informasi pribadi mereka di platform. Beberapa pengguna juga melaporkan ketidakpahaman tentang bagaimana data mereka digunakan dan dibagikan, yang menunjukkan perlunya peningkatan edukasi tentang pengaturan privasi dan keamanan data.

Analisis data mengidentifikasi beberapa tema utama. Pertama, ada kebutuhan untuk meningkatkan transparansi dalam kebijakan privasi Facebook dengan menyederhanakan dan menjelaskan informasi yang disediakan kepada pengguna. Kedua, penting untuk meningkatkan pendidikan pengguna mengenai pengaturan privasi dan perlindungan data mereka. Ketiga, penerapan teknologi keamanan yang lebih baik dan evaluasi rutin terhadap kebijakan keamanan diperlukan untuk mengatasi kelemahan yang ada.

5 KESIMPULAN

Penelitian ini menunjukkan bahwa meskipun Facebook telah menerapkan berbagai langkah keamanan seperti enkripsi data dan autentikasi dua faktor, masih terdapat kekurangan dalam kebijakan privasi dan implementasi sistem keamanan. Melalui tinjauan literatur, studi kasus, dan wawancara, ditemukan bahwa transparansi kebijakan privasi perlu ditingkatkan, pengguna perlu lebih memahami

pengaturan privasi mereka, dan evaluasi serta pembaruan rutin terhadap teknologi keamanan sangat diperlukan. Untuk meningkatkan perlindungan data pribadi pengguna, Facebook disarankan untuk memperbaiki kebijakan privasi, meningkatkan edukasi mengenai pengaturan privasi, dan melakukan peninjauan rutin terhadap praktik keamanan yang ada.

REFERENSI

- [1] Laudon, K. C., & Laudon, J. P. (2020). Management Information Systems: Managing the Digital Firm. Pearson.
- [2] Whitman, M. E., & Mattord, H. J. (2022). Principles of Information Security. Cengage Learning.
- [3] Zuckerberg, M., & D'Angelo, M. (2004). Facebook Launches: The New Social Network. Harvard Business Review.
- [4] Smith, A. (2021). Social Media Privacy: Understanding Risks and Mitigation. Journal of Cybersecurity.
- [5] Cadwalladr, C., & Graham-Harrison, E. (2018). The Cambridge Analytica Files. The Guardian.
- [6] Laudon, K. C., & Laudon, J. P. (2020). Management Information Systems: Managing the Digital Firm (16th ed.). Pearson.
- [7] Whitman, M. E., & Mattord, H. J. (2011). Principles of Information Security (4th ed.). Cengage Learning.
- [8] Facebook. (n.d.). Company Info. Retrieved from <https://about.fb.com/company-info/>
- [9] Schreuders, Z. C., Ardern, J., & Zavarsky, P. (2013). "Facebook's Privacy Policy and Its Third-Party Partnerships: Lucrative Commitments at the Expense of User Privacy," International Journal of Information Security Science, 2(2), 34-43.
- [10] Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.