E-ISSN : 3025-1311
https://ejournal.warunayama.org/kohesi

Kohesi: Jurnal Multidisiplin Saintek
Volume 10 No 7 Tahun 2025

KEAMANAN DI ERA CLOUD COMPUTING DAN SMARTPHONE

Dini Fadilah Hasibuan[1], Jalaludin[2], M. Sukrom Mirta[3]
Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, UIN Sultan Thaha Saifuddin Jambi
Email: [1]dinifadilahhasibuan12@gmail.com, [2]udin67662@gmail.com, [3]sukrom023@gmail.com,

Jl. Jambi Ma. Bulian KM.16 Simpang Sungai Duren Kab. Muaro Jambi, Jambi 36361
Email: mail@uinjambi.ac.id

ABSTRAK

Perkembangan teknologi digital yang sangat pesat telah membawa perubahan besar terhadap cara manusia berinteraksi dengan data dan informasi. Cloud computing dan smartphone menjadi dua teknologi yang paling berpengaruh dalam kehidupan modern karena mampu memberikan kemudahan akses data di mana saja dan kapan saja. Namun, kemajuan ini juga menghadirkan risiko keamanan yang semakin kompleks, seperti pencurian data, peretasan akun, dan penyalahgunaan informasi pribadi. Penelitian ini bertujuan untuk menganalisis ancaman keamanan pada cloud computing dan smartphone serta memberikan strategi mitigasi yang efektif untuk meningkatkan perlindungan data. Metode penelitian yang digunakan adalah studi literatur dengan mengkaji sumber-sumber akademik, laporan keamanan siber, serta kasus-kasus aktual seperti kebocoran data Facebook (2021) dan peretasan iCloud (2014). Hasil penelitian menunjukkan bahwa keamanan data dapat ditingkatkan melalui penerapan otentikasi dua faktor, enkripsi, manajemen identitas dan akses (IAM), pembaruan sistem, dan peningkatan literasi keamanan bagi pengguna.

Kata kunci: Cloud Computing, Smartphone, Keamanan Siber, Enkripsi, Privasi Data.

ABSTRACT

The rapid development of digital technology has brought about significant changes in the way humans interact with data and information. Cloud computing and smartphones have become two of the most influential technologies in modern life, enabling easy access to data anytime, anywhere. However, these advances also present increasingly complex security risks, such as data theft, account hacking, and misuse of personal information. This study aims to analyze security threats to cloud computing and smartphones and provide effective mitigation strategies to improve data protection. The research method used is a literature review, reviewing academic sources, cybersecurity reports, and actual cases such as the Facebook data leak (2021) and the iCloud hack (2014). The results show that data security can be improved through the implementation of two-factor authentication, encryption, identity and access management (IAM), system updates, and increased security literacy among users.

Article History
Received: Desember 2025
Reviewed: Desember 2025
Published: Desember 2025

Plagiarism Checker No 796
Prefix DOI : Prefix DOI : 10.8734/Kohesi.v1i2.365
Copyright : Author
Publish by : Kohesi

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License

PENDAHULUAN

Transformasi digital telah mengubah pola hidup masyarakat global, di mana setiap aktivitas kini terhubung dengan teknologi berbasis internet. Salah satu inovasi yang memberikan dampak besar adalah cloud computing atau komputasi awan. Teknologi ini memungkinkan pengguna menyimpan data seperti dokumen, foto, dan aplikasi di server online sehingga dapat diakses kapan saja menggunakan berbagai perangkat, terutama smartphone. Namun, meningkatnya ketergantungan pada cloud computing dan smartphone juga memperbesar potensi ancaman terhadap keamanan data. Menurut laporan Cybersecurity Ventures (2023), insiden peretasan dan kebocoran data meningkat hingga 35% setiap tahunnya, terutama pada platform berbasis cloud dan perangkat mobile. Kasus peretasan iCloud tahun 2014 dan kebocoran data Facebook tahun 2021 menjadi bukti nyata bahwa keamanan digital masih menjadi tantangan serius.

Kondisi ini menuntut adanya kesadaran dan penerapan strategi keamanan yang kuat baik dari sisi pengguna, penyedia layanan, maupun pengembang teknologi. Enkripsi data, autentikasi ganda, serta

kebijakan keamanan berbasis privasi menjadi faktor penting dalam menjaga integritas dan kerahasiaan informasi di era digital. Selain itu, peran edukasi pengguna juga sangat diperlukan agar mampu memahami risiko serta cara melindungi diri di dunia maya.

Dengan demikian, pembahasan mengenai keamanan di era cloud computing dan smartphone menjadi sangat relevan untuk dikaji lebih dalam. Artikel ini bertujuan untuk meninjau berbagai tantangan keamanan yang muncul, mengidentifikasi potensi ancaman, serta menawarkan solusi dan pendekatan yang dapat diterapkan guna meningkatkan keamanan digital di tengah pesatnya perkembangan teknologi saat ini.

METODE PENELITIAN

Penelitian ini menggunakan metode studi literatur dengan mengumpulkan dan menganalisis berbagai sumber ilmiah seperti jurnal, laporan keamanan siber, dan berita terkait kasus aktual.

1. **Jenis Penelitian**

Penelitian ini bersifat kualitatif deskriptif, menggambarkan fenomena keamanan digital berdasarkan data sekunder.

2. **Sumber Data**

Sumber data diperoleh dari jurnal ilmiah nasional dan internasional, laporan keamanan, serta kasus nyata yang relevan.

3. **Teknik Analisis Data**

Data dianalisis secara deskriptif untuk menemukan pola ancaman, penyebab, serta strategi keamanan yang efektif.

HASIL DAN PEMBAHASAN

Keamanan pada Media Sosial dan Aplikasi Cloud

Media sosial dan aplikasi cloud telah menjadi target utama serangan siber. Keamanan pada platform ini sangat bergantung pada serangkaian tindakan proaktif oleh pengguna dan penyedia layanan.

Pentingnya Pengamanan:

- **Aplikasi cloud dan smartphone memberikan kemudahan akses data di mana saja dan kapan saja.**
- **Namun, kemajuan ini juga membawa risiko keamanan yang semakin kompleks, seperti pencurian data dan peretasan akun.**
- **Kasus nyata, seperti kebocoran data Facebook tahun 2021 dan peretasan iCloud tahun 2014, membuktikan bahwa keamanan digital merupakan tantangan serius.**

Strategi Keamanan Utama

Untuk mencegah kebocoran data pada media sosial dan aplikasi cloud, langkah-langkah berikut sangat penting:

1. Pengaturan Privasi

Memastikan bahwa data dan aktivitas Anda hanya dapat dilihat oleh pihak yang berhak.

- **Media Sosial: Batasi siapa yang dapat melihat postingan dan informasi profil Anda (misalnya, hanya untuk teman atau koneksi yang dipilih).**
- **Cloud (Penyimpanan Data): Kelola izin berbagi file dengan ketat. Pastikan file sensitif tidak dibagikan secara publik dan hanya diakses oleh pengguna yang berwenang.**

2. Pembatasan Izin Aplikasi

Aplikasi pihak ketiga yang terhubung ke akun Anda dapat menjadi celah keamanan jika dieksploitasi.

- **Tinjauan Rutin: Periksa secara berkala daftar aplikasi yang memiliki izin akses ke akun media sosial atau cloud Anda.**
- **Cabut Izin: Cabut izin akses dari aplikasi yang tidak Anda kenal, tidak lagi digunakan, atau yang meminta izin berlebihan.**

3. Verifikasi Akun dan Otentikasi Kuat

Menggunakan lapisan keamanan berlapis untuk memverifikasi identitas pengguna.

- **Otentikasi Dua Faktor (2FA): Ini adalah strategi keamanan yang efektif. Selalu aktifkan 2FA pada akun media sosial dan cloud Anda untuk mencegah peretasan yang disebabkan oleh kata sandi yang lemah.**
- **Kata Sandi Kuat: Gunakan kata sandi yang kuat dan unik untuk setiap akun.**

4. Enkripsi Data

Enkripsi melindungi kerahasiaan data (confidentiality).

- **Pada aplikasi cloud, data harus dienkripsi baik saat transit (dikirim) maupun saat diam (at rest / disimpan di server) untuk mencegah akses tidak sah.**

5. Pembaruan Sistem dan Edukasi Pengguna

- **Pembaruan Sistem: Selalu lakukan pembaruan sistem dan aplikasi secara berkala (patching) untuk menutup celah keamanan yang mungkin ada.**
- **Edukasi Pengguna: Peningkatan literasi keamanan bagi pengguna sangat penting agar mereka mampu memahami risiko dan cara melindungi diri di dunia maya.**

KESIMPULAN DAN SARAN

KESIMPULAN

1. **Berdasarkan hasil analisis literatur mengenai keamanan pada cloud computing, smartphone, media sosial, dan aplikasi cloud, dapat disimpulkan bahwa perkembangan teknologi digital telah memberikan kemudahan yang signifikan dalam mengakses, menyimpan, dan mengelola data. Namun, kemajuan ini juga diikuti oleh meningkatnya risiko keamanan, termasuk pencurian data, peretasan akun, penyalahgunaan aplikasi pihak ketiga, serta serangan siber seperti malware dan Man-in-the-Middle (MITM).**
2. **Kasus-kasus aktual seperti peretasan iCloud tahun 2014 dan kebocoran data Facebook pada tahun 2021 menunjukkan bahwa ancaman terhadap keamanan digital tidak hanya disebabkan oleh kelemahan sistem teknis, tetapi juga faktor manusia seperti penggunaan kata sandi lemah, pengaturan privasi yang buruk, serta rendahnya literasi keamanan pengguna.**
3. **Strategi keamanan utama seperti penerapan otentikasi dua faktor, enkripsi data, manajemen akses, pembaruan sistem, pengaturan privasi, verifikasi aplikasi pihak ketiga, dan edukasi pengguna terbukti menjadi langkah efektif dalam mengurangi risiko kebocoran data. Dengan demikian, keamanan digital membutuhkan upaya kolaboratif antara pengguna, penyedia layanan cloud, dan pengembang teknologi untuk memastikan perlindungan data yang optimal di era digital yang semakin kompleks.**

SARAN

Berdasarkan hasil pembahasan di atas, beberapa saran yang dapat diterapkan untuk meningkatkan keamanan cloud computing, smartphone, serta media sosial dan aplikasi cloud adalah sebagai berikut:

1. **Penguatan Perilaku Pengguna**
   - **Pengguna wajib memperbarui sistem dan aplikasi secara berkala untuk menutup celah keamanan yang sering menjadi pintu masuk serangan siber.**
   - **Gunakan kata sandi yang kuat dan unik pada setiap akun serta aktifkan otentikasi dua faktor (2FA) guna menambah lapisan perlindungan terhadap akses tidak sah.**
   - **Pengguna perlu meningkatkan kewaspadaan terhadap aplikasi pihak ketiga dengan membatasi izin akses dan secara rutin meninjau aplikasi yang terhubung ke akun mereka.**
2. **Peningkatan Literasi Keamanan Digital**
   - **Edukasi keamanan siber harus ditingkatkan agar masyarakat memahami risiko digital, cara mengamankan data pribadi, serta pentingnya pengaturan privasi di media sosial dan platform cloud.**
   - **Kampanye literasi digital di lingkungan pendidikan, organisasi, dan masyarakat umum sangat diperlukan untuk mengurangi kesalahan pengguna (human error) yang menjadi penyebab utama kebocoran data.**
3. **Penguatan Keamanan oleh Penyedia Layanan Cloud**
   - **Penyedia layanan cloud perlu menerapkan sistem keamanan berlapis seperti enkripsi end-to-end, manajemen identitas dan akses (IAM), deteksi intrusi, dan pemantauan aktivitas secara real-time.**
   - **Penyedia layanan harus memastikan kebijakan privasi dan keamanan diterapkan secara konsisten untuk melindungi data pengguna baik saat transit maupun saat tersimpan (at rest).**
4. **Optimalisasi Pengaturan Privasi dan Manajemen Akses**
   - **Pengguna harus memanfaatkan fitur pengaturan privasi pada media sosial dan layanan cloud untuk membatasi siapa yang dapat mengakses informasi pribadi atau file yang dibagikan.**
   - **Pada aplikasi cloud, penting untuk memastikan bahwa file sensitif tidak dibagikan secara publik dan hanya dapat diakses oleh pihak yang berwenang.**
5. **Penguatan Kerja Sama dan Kepatuhan terhadap Kebijakan Keamanan**
   - **Diperlukan kerja sama antara pengguna, penyedia layanan, lembaga pendidikan, dan pemerintah untuk menciptakan ekosistem digital yang aman.**
   - **Pengembangan kebijakan keamanan yang berbasis privasi dan standar global harus terus ditingkatkan agar mampu menghadapi ancaman keamanan yang berkembang.**

DAFTAR PUSTAKA

Cybersecurity Ventures. (2023). Global Cybersecurity Report 2023.

Ghofururrohim, N. M., Wicaksono, R. N., & Faristiana, A. R. (2023). Pengaruh Smartphone Terhadap Anak Usia Dini. *Education: Jurnal Sosial Humaniora Dan Pendidikan*, *3*(2), 129-146.

Nugraha, R. (2023). Cloud Computing dan Transformasi Digital di Indonesia. Jurnal Teknologi Informasi, 7(2), 55–62.

Putri, A. (2021). Analisis Kasus Kebocoran Data Facebook Tahun 2021. Jurnal Keamanan Siber Indonesia, 4(1), 15–22.

Rahardjo, F. (2024). Cybersecurity Trends in Cloud Infrastructure. Jurnal Sistem Informasi dan Teknologi, 8(3), 101–112.

Satrinia, D., Yutia, S. N., & Matin, I. M. M. (2022). Analisis Keamanan dan Kenyamanan pada Cloud Computing. *Journal of Informatics and Communication Technology (JICT)*, *4*(1), 85-91.

Setiawan, A., & Yulianto, E. (2020). Pengantar Keamanan MediaDigital. *Informatika. Bandung*.

Susanto, A., & Wibowo, R. (2022). Keamanan Informasi pada Perangkat Mobile. Jurnal Informatika dan Teknologi Digital, 5(1), 33–41.

Tandy, J., & Siswono, S. (2013). Cloud Computing dan Dampaknya Terhadap Bisnis. *ComTech*, *4*(2), 687-695.

Pratama, R.V., Hasrullah (2025). Pengembangan Sistem Rekomendasi Buku Untuk Meningkatkan Minat Baca dengan Pendekatan Hybrid Filtering. Jurnal Inovasi Global, 3 (1). 3031-0512.