JSI (Jurnal Sistem Informasi) Universitas Dirgantara Marsekal Suryadarma
p-ISSN: 2355-9675
e-ISSN: 2541-3228

Implementasi Keamanan dan Pengembangan Desain Aplikasi menggunakan Statistical Analysis System (SAS)

Peniarsih[1,*], Iswandir [2]
[1]Sistem Informasi, Universitas Dirgantara Marsekal Surydarma, Indonesia
[2]Manajemen Informatika, Universitas Dirgantara Marsekal Suryadarma, Indonesia
peniarsih18@gmail.com, iswandir11@gmail.com

Article Info

Article history:

Submitted April 17, 2025
Accepted May 9, 2025
Published July 15, 2025

Kata Kunci*:*

Aplikasi Digital
Pengembangan Aplikasi
Statistical Analysis System (SAS)

ABSTRAK (10 PT)

Perkembangan teknologi informasi menuntut pengembangan aplikasi yang aman dan efisien. Penelitian ini mengimplementasikan prinsip Security by Design menggunakan Statistical Analysis System (SAS) untuk meningkatkan keamanan aplikasi. Metode kualitatif dengan studi kasus dan analisis komparatif diterapkan, meliputi studi literatur, identifikasi ancaman, penerapan SAS, serta evaluasi keamanan. Hasil pengujian menunjukkan: (1) Enkripsi data dengan AES-256 mencapai validitas 100%, (2) Otentikasi biometrik memiliki akurasi 98,5%, (3) Deteksi serangan real-time berhasil mengidentifikasi 89% ancaman, dan (4) Penerapan least privilege mengurangi akses ilegal sebesar 72%. Analisis komparatif membuktikan bahwa aplikasi dengan SAS memiliki lebih sedikit kerentanan dan respons lebih cepat terhadap ancaman. Tantangan utama meliputi kebutuhan sumber daya dan pelatihan pengembang. Kesimpulannya, integrasi SAS dan Security by Design secara signifikan meningkatkan keamanan aplikasi dalam aspek kerahasiaan, integritas, dan ketersediaan data. Penelitian ini merekomendasikan penerapan prinsip keamanan sejak tahap awal pengembangan untuk aplikasi yang tangguh dan andal.

Corresponding Author:

Peniarsih
Department of Information Systems,
Universitas Dirgantara Marsekal Suryadarma,
Email: * peniarsih18@gmail.com

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat, khususnya di bidang pengembangan aplikasi, telah membawa perubahan signifikan dalam cara data dan informasi dikelola, diproses, serta disebarluaskan. Aplikasi-aplikasi yang terus berkembang di berbagai sektor, seperti *e-commerce*, perbankan, pemerintahan, dan kesehatan, semakin bergantung pada pengolahan data yang aman dan efisien . Dengan meningkatnya ketergantungan pada aplikasi digital, risiko terhadap ancaman keamanan siber pun semakin besar. Keamanan informasi dan data menjadi prioritas utama bagi pengembang aplikasi dan perusahaan yang bergerak di bidang teknologi (Awaludin, 2019). Dalam era digital yang didominasi oleh data, keamanan informasi menjadi pilar utama pengembangan aplikasi. Organisasi di berbagai sektor, mulai dari keuangan hingga kesehatan, mengandalkan data sensitif untuk pengambilan keputusan dan operasional. Transformasi digital akan mendorong peningkatan signifikan dalam pengembangan aplikasi berbasis web serta mobile untuk berbagai sektor, termasuk keuangan, perdagangan, dan logistik. Perkembangan dengan diiringi dengan meningkatnya ancaman keamanan siber yang mengancam kerahasiaan, integritas, dan ketersediaan data. Serangan siber seperti pencurian data, manipulasi sistem, dan eksploitasi kerentanan menjadi tantangan serius bagi pengembang aplikasi. Pengembang yang

masih mengabaikan pentingnya implementasi keamanan secara menyeluruh dalam tahap awal pengembangan aplikasi. Aplikasi yang baru menerapkan langkah-langkah keamanan setelah aplikasi selesai dikembangkan atau bahkan setelah terjadi insiden kebocoran data.

Era digital aplikasi perangkat lunak telah menjadi bagian integral dari kehidupan. Aplikasi menangani data sensitif serta melakukan fungsi penting (Awaludin, 2018). Oleh karena itu, memastikan keamanan aplikasi ini sangat penting untuk melindungi informasi pengguna, menjaga kepercayaan, dan mencegah potensi kerugian finansial atau reputasi.Pendekatan tradisional untuk keamanan aplikasi seringkali bersifat reaktif, yaitu mengatasi kerentanan setelah ditemukan. Namun, pendekatan ini terbukti tidak memadai dalam menghadapi lanskap ancaman yang terus berkembang. Untuk mengatasi tantangan ini, paradigma "keamanan oleh desain" telah muncul sebagai pendekatan yang lebih proaktif dan efektif. Keamanan oleh desain mengintegrasikan pertimbangan keamanan ke dalam setiap tahap siklus hidup pengembangan perangkat lunak (SDLC) (Arnomo & Kurniawan, 2024), mulai dari pengumpulan persyaratan dan desain hingga implementasi dan pengujian. Dengan membangun keamanan ke dalam fondasi aplikasi, pengembang dapat mengurangi risiko kerentanan dan memastikan bahwa keamanan menjadi bagian intrinsik dari produk akhir. Mmengeksplorasi implementasi keamanan oleh desain dalam konteks pengembangan aplikasi menggunakan SAS (*Statistical Analysis System*). SAS adalah rangkaian perangkat lunak yang banyak digunakan untuk analitik data tingkat lanjut, kecerdasan bisnis, dan manajemen data. Dengan memanfaatkan prinsip-prinsip keamanan oleh desain, pengembang SAS dapat membuat aplikasi yang tidak hanya kuat dan andal tetapi juga aman dan tangguh terhadap berbagai ancaman keamanan (Awaludin, 2020). Pembahas konsep dan praktik utama keamanan oleh desain, termasuk pemodelan ancaman, desain aman, dan pengujian keamanan. Selain itu, kami akan memberikan mengilustrasikan penerapan prinsip-prinsip ini dalam pengembangan aplikasi SAS. Tujuan kami adalah untuk memberikan panduan komprehensif bagi pengembang SAS yang ingin membangun aplikasi yang aman dan terjamin. Pendekatan semacam ini dikenal dengan pendekatan keamanan "terlambat" dan seringkali tidak efektif untuk mengurangi risiko secara signifikan, karena penting untuk memperkenalkan konsep Keamanan oleh Desain (*Security by Design*) yang menekankan pada penerapan prinsip-prinsip keamanan sejak tahap perancangan dan pengembangan aplikasi itu sendiri. Penelitian membahas bagaimana implementasi Keamanan oleh Desain melalui SAS dapat meningkatkan tingkat keamanan aplikasi secara keseluruhan, serta menganalisis dampaknya terhadap efektivitas pengembangan aplikasi yang aman, efisien, dan minim risiko. Dengan pendekatan ini, diharapkan dapat tercipta aplikasi yang tidak hanya berfungsi dengan baik, tetapi juga mampu melindungi data dan informasi pengguna dari ancaman yang terus berkembang.

Keamanan aplikasi menjadi semakin penting di era digital ini (Aini et al., 2024), terutama dengan meningkatnya ancaman siber dan sensitivitas data yang dikelola oleh aplikasi. Pendekatan "keamanan oleh desain" (*security by design*) memastikan bahwa keamanan dibangun ke dalam aplikasi sejak awal proses pengembangan, bukan ditambahkan sebagai pemikiran, Seiring dalam meningkatnya kompleksitas data dan aplikasi, ancaman keamanan siber j semakin canggih. Serangan siber dapat mengakibatkan kebocoran data, kerugian finansial, dan kerusakan reputasi yang signifikan. Oleh karena itu, pendekatan proaktif dalam mengamankan aplikasi, yaitu "keamanan oleh desain" (*security by design*), penting SAS (*Statistical Analysis System*) memainkan peran penting dalam analisis data yang kompleks dan mendalam. Keamanan oleh desain mengintegrasikan prinsip-prinsip keamanan ke dalam setiap tahap pengembangan aplikasi, bukan sebagai tambahan setelah aplikasi selesai dibuat. Pendekatan ini memastikan bahwa keamanan menjadi bagian integral dari arsitektur dan fungsionalitas aplikasi.

2. METODE

Metodologi digunakan yaitu pendekatan penelitian kualitatif dengan studi kasus serta analisis komparatif. Studi Literatur Langkah pertama adalah melakukan studi literatur yang mendalam memahami konsep dasar dari Keamanan oleh Desain (*Security by Design*), *Software Assurance Security* (SAS) , hubungan keduanya dalam konteks pengembangan aplikasi. Literatur yang digunakan meliputi jurnal ilmiah, buku, laporan industri, serta standar keamanan yang relevan. ancaman keamanan siber terkini dan *best practices* dalam pengembangan aplikasi

Identifikasi Pengembangan Aplikasi pengembangan aplikasi yang menjadi objek penelitian yang dianalisis. Siklus hidup pengembangan perangkat lunak (SDLC – *Software Development Life Cycle*) yang digunakan (Achmad Ramadhany & Peniarsih, 2022). Identifikasi akan meliputi tahap perancangan, pengembangan, pengujian, hingga pemeliharaan aplikasi. Proses ini akan dibandingkan

antara pengembangan aplikasi yang menerapkan prinsip Keamanan oleh Desain menggunakan SAS dan aplikasi yang tidak mengintegrasikan prinsip-prinsip keamanan secara sistematik.

Analisis Komparatif Untuk mengukur keberhasilan implementasi Keamanan oleh Desain menggunakan SAS, hasil dari aplikasi yang menerapkan prinsip tersebut akan dibandingkan dengan aplikasi yang tidak mengintegrasikan prinsip keamanan sejak awal. Perbandingan ini dilakukan berdasarkan beberapa indikator seperti jumlah kerentanannya, respons terhadap ancaman, dampaknya terhadap performa dan kualitas aplikasi. Pengumpulan Data dan Analisis Kualitatif Data dikumpulkan dalam studi kasus, wawancara, dan hasil pengujian akan dianalisis secara kualitatif (Mukaromah, 2020). Analisis ini bertujuan untuk mengevaluasi dampak penerapan Keamanan oleh Desain terhadap pengembangan aplikasi yang lebih aman dan dapat diandalkan. Temuan dari analisis ini akan digunakan untuk memberikan rekomendasi bagi pengembang aplikasi dan organisasi terkait

3. HASIL DAN PEMBAHASAN

Pembahasan penelitian yang diperoleh dari berbagai metode pengumpulan data akan dianalisis serta dibahas untuk mengevaluasi efektivitas implementasi Keamanan oleh Desain (Security by Design) dalam pengembangan aplikasi menggunakan Software Assurance Security (SAS) (Mohamad, Steghöfer, & Scandariato, 2021) (Rindell, Ruohonen, Holvitie, Hyrynsalmi, & Leppänen, 2021). Pembahasan ini mencakup hasil dari wawancara dengan pengembang, observasi proses pengembangan, studi kasus implementasi SAS, serta hasil pengujian.

Data Uji untuk Enkripsi Data

Algoritma: AES (*Advanced Encryption Standard*)

Data Uji	Proses Enkripsi	Perhitungan Validasi
Teks asli: "DataSensitive123" Kunci enkripsi: "K3yEnkripsi2024" (256-bit)	1. Teks asli diubah menjadi blok 128-bit. 2. Proses enkripsi AES dilakukan dengan 14 putaran (rounds) untuk kunci 256-bit. 3. Hasil enkripsi: "a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6" (contoh ciphertext).	**Kriteria**: Ciphertext tidak dapat dikembalikan tanpa kunci dekripsi. **Hasil**: 100% valid (teks asli hanya dapat diakses dengan kunci yang benar).

Data Uji untuk Otentikasi Pengguna

Metode: Otentikasi Biometrik (Sidik Jari)

Data Uji	Perhitungan Akurasi:
Jumlah percobaan: 200 Percobaan berhasil: 197 Percobaan gagal: 3	Tingkat Keberhasilan=(Percobaan BerhasilTotal Percobaan)×100 =(197200)×100=98.5%

Data Uji untuk Deteksi Serangan

Metode: Pemantauan Jaringan (*Real-time Monitoring*)

Data Uji	Perhitungan Akurasi:
Total ancaman terdeteksi: 89 Ancaman yang berhasil di-blok sebelum ekskalasi: 80 Ancaman yang lolos: 9	Presentase Deteksi=(Total AncamanAncaman Terblokir)×100=(8980)×100=89.9%=89%

Data Uji untuk Manajemen Izin

Prinsip: *Least Privilege*

Data Uji	**Perhitungan Akurasi**:
Jumlah akses ilegal sebelum implementasi: 50 Jumlah akses ilegal setelah implementasi: 14	Pengurangan Risiko=(Akses AwalAkses Awal−Akses Baru)×100=(5050−14)×100=72%

Kriteria	**Metode**	**Data Uji**	**Hasil**
Enkripsi Data	AES-256	Teks: "DataSensitive123"	100% valid
Otentikasi Pengguna	Biometrik	200 percobaan	98.5% akurasi
Deteksi Serangan	Pemantauan Jaringan	89 ancaman	89% terdeteksi
Manajemen Izin	*Least Privilege*	50 → 14 akses ilegal	72% pengurangan risiko

4. KESIMPULAN

Penelitian ini membuktikan bahwa penerapan prinsip Security by Design dengan memanfaatkan Statistical Analysis System (SAS) secara signifikan meningkatkan keamanan aplikasi. Hasil pengujian menunjukkan keberhasilan dalam berbagai aspek: enkripsi data AES-256 mencapai validitas sempurna (100%), otentikasi biometrik memiliki akurasi tinggi (98,5%), sistem deteksi serangan mampu mengidentifikasi 89% ancaman, dan penerapan least privilege mengurangi akses ilegal sebesar 72%. Pendekatan proaktif ini terbukti lebih efektif dibandingkan metode tradisional yang bersifat reaktif, dengan mengurangi kerentanan dan meningkatkan respons terhadap ancaman. Meskipun implementasinya memerlukan sumber daya dan pelatihan tambahan, manfaat jangka panjang dalam melindungi data sensitif dan menjaga integritas aplikasi sangat signifikan. Oleh karena itu, penelitian ini merekomendasikan integrasi keamanan sejak tahap awal pengembangan (Security by Design) sebagai solusi optimal untuk membangun aplikasi yang tangguh, andal, dan siap menghadapi tantangan keamanan siber yang terus berkembang.

DAFTAR PUSTAKA

Achmad Ramadhany, & Peniarsih. (2022). Sistem Informasi Penelitian Lppm Di Universitas Dirgantara Marsekal Suryadarma Berbasis Web. *Jurnal Sistem Informasi*, *9*(1), 119–128.

Aini, H., Awaludin, M., Gani, A. G., Informatika, M., Dirgantara, U., & Suryadarma, M. (2024). *Rancang Bangun Sistem Perhitungan Jumlah Penumpang Pesawat Dengan Sensor Seat Pessanger*. *22*(2), 12–23.

Arnomo, S. A., & Kurniawan, D. E. (2024). Metode Agile Scrum Dalam Pengembangan Sistem Pengendali Stok Barang. *Jurnal Desain Dan Analisis …*.

Awaludin, M. (2018). Penerapan Algoritma Rc4 Pada Operasi Xor Untuk Keamanan Pesan Pada Smartphone Berbasis Web. *Jurnal Sistem Informasi Universitas Suryadarma*, *4*(1), 16–22. https://doi.org/10.35968/jsi.v4i1.71

Awaludin, M. (2019). Penerapan Algoritma K-Means Clustering Pada K-Harmonic Means Untuk Schedule Preventive Maintenance Service. *Jurnal Sistem Informasi Universitas Suryadarma*, *6*(1), 1–17. https://doi.org/10.35968/jsi.v6i1.271

Awaludin, M. (2020). Application Of Analytical Hierarchy Process Method For Employee Performance Evaluation At Pt Xyz. *JSI (Jurnal Sistem Informasi) Universitas Suryadarma*, *7*(1), 137–150.

Mohamad, M., Steghöfer, J.-P., & Scandariato, R. (2021). Security assurance cases—state of the art of an emerging approach. *Empirical Software Engineering*, *26*(4), 70. https://doi.org/10.1007/s10664-021-09971-7

Mukaromah, E. (2020). Pemanfaatan Teknologi Informasi dan Komunikasi dalam Meningkatkan Gairah Belajar Siswa. *Indonesian Journal of Education Management and Administration Review*, *4*(1), 179–185.

Rindell, K., Ruohonen, J., Holvitie, J., Hyrynsalmi, S., & Leppänen, V. (2021). Security in agile software development: A practitioner survey. *Information and Software Technology*, *131*, 106488. https://doi.org/https://doi.org/10.1016/j.infsof.2020.106488