Inovan Publisher

Orbit: Jurnal Ilmu Multidisplin Nusantara

| ISSN (Online) 3064-5883 |
https://creativecommons.org/licenses/by/4.0/
DOI: https://doi.org/10.63217/orbit.v1i3

Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Data Pengguna Pada Aplikasi Dana

Farhan Saputra[1], Nofri Satriawan[2], Raihan Saputra[3],
[1]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, farhansaputra121@gmail.com
[2]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, nofrisatriawan3@gmail.com
[3]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, raihansaputra0502@gmail.com

Corresponding Author: farhansaputra121@gmail.com[1]

Abstract: *This research aims to explore the implementation of security management in enhancing user data security on the DANA application, a popular e-wallet service in Indonesia. With the increasing use of digital wallets, concerns about data security, such as data breaches, identity theft, and cyberattacks, have become critical. The study is guided by three main research questions: 1) How does DANA improve user trust? 2) What security management strategies does DANA apply in its application? 3) What is the impact of security management on the DANA application? The research employs a case study approach, combining literature reviews and user feedback, to analyze the effectiveness of DANA's security measures, including encryption, multi-factor authentication (MFA), real-time threat detection, and user education. The findings highlight that DANA's security management strategies significantly contribute to increased user trust and security, enhancing the overall user experience and loyalty. This research provides insights into the role of security management in securing user data and fostering trust in e-wallet applications.*

Keyword: *Security Management, Data Security, DANA Application, E-wallet*

Abstrak: Penelitian ini bertujuan untuk mengeksplorasi penerapan manajemen sekuriti dalam meningkatkan keamanan data pengguna pada aplikasi DANA, sebuah layanan dompet digital yang populer di Indonesia. Dengan semakin meningkatnya penggunaan dompet digital, kekhawatiran mengenai keamanan data, seperti kebocoran data, pencurian identitas, dan serangan siber, menjadi hal yang sangat penting. Penelitian ini mengacu pada tiga pertanyaan penelitian utama: 1) Bagaimana cara DANA meningkatkan kepercayaan pengguna? 2) Apa saja strategi manajemen sekuriti yang diterapkan oleh DANA dalam aplikasinya? 3) Seberapa besar pengaruh manajemen sekuriti terhadap aplikasi DANA? Penelitian ini menggunakan pendekatan studi kasus yang menggabungkan tinjauan pustaka dan umpan balik pengguna untuk menganalisis efektivitas langkah-langkah sekuriti yang diterapkan DANA, termasuk enkripsi, autentikasi multi-faktor (MFA), deteksi ancaman secara real-time, dan edukasi pengguna. Temuan penelitian menunjukkan bahwa strategi manajemen sekuriti DANA

berkontribusi signifikan terhadap peningkatan kepercayaan dan keamanan pengguna, serta meningkatkan pengalaman dan loyalitas pengguna secara keseluruhan. Penelitian ini memberikan wawasan tentang peran manajemen sekuriti dalam mengamankan data pengguna dan membangun kepercayaan pada aplikasi dompet digital.

Keyword: Manajemen Sekuriti, Keamanan Data, Aplikasi DANA, Dompet Digital

PENDAHULUAN

Dalam era digitalisasi saat ini, penggunaan e-wallet atau dompet digital telah menjadi bagian penting dari sistem pembayaran modern. Teknologi yang terus berkembang pesat telah memengaruhi hampir seluruh aspek kehidupan manusia, termasuk cara bertransaksi. Di Indonesia, penggunaan e-wallet semakin meluas, terutama untuk pembayaran di e-commerce, seiring dengan semakin banyaknya perusahaan yang meluncurkan aplikasi dompet digital. Salah satu perusahaan yang terkemuka adalah PT Espay Debit Indonesia Koe dengan produknya, aplikasi Dana (Rozi, 2022).

Meskipun e-wallet menawarkan kemudahan dalam bertransaksi, pengguna tetap dihadapkan pada risiko keamanan data, seperti pencurian identitas, phishing, malware, dan serangan peretasan. Ancaman ini tidak hanya berpotensi merugikan secara finansial tetapi juga dapat merusak reputasi pengguna (Yazdanifard et al., 2011). Keamanan data pribadi menjadi isu utama yang perlu mendapat perhatian serius. Kasus peretasan besar seperti yang terjadi pada Tokopedia, di mana 91 juta data pengguna diretas, menunjukkan lemahnya perlindungan data pribadi di Indonesia (Persadha, 2020).

Peningkatan pengguna internet yang mencapai 221,56 juta orang pada tahun 2024 semakin memperbesar urgensi akan perlindungan data pribadi. Namun, regulasi hukum di Indonesia masih dinilai belum memadai untuk menjawab tantangan ini, sehingga pengguna internet menjadi rentan terhadap ancaman kebocoran data (Putra, 2020).

Manajemen sekuriti merupakan langkah krusial dalam melindungi sistem, jaringan, dan data dari berbagai serangan potensial (Sudira, 2004). Dalam konteks aplikasi Dana, manajemen sekuriti mencakup perlindungan informasi pengguna yang tersimpan dalam sistem. Sebagai salah satu platform e-wallet terbesar di Indonesia dengan 170 juta pengguna aktif pada tahun 2023, Dana memainkan peran penting dalam menyediakan transaksi yang aman bagi penggunanya. Dengan fungsi-fungsi seperti pembayaran online, top-up saldo, dan investasi, keamanan data pengguna menjadi prioritas utama untuk menjaga kepercayaan terhadap platform ini (Zeithml, 2021).

Hal ini menyebabkan satu elemen kunci yang mempengaruhi kepercayaan pengguna pada aplikasi *e-wallet*. Pengguna akan ragu menggunakan *e-wallet* dan lebih memilih menyimpan uang secara jika mereka yakin bahwa data pribadi mereka tidak aman. Kekhawatiran para pengguna *e-wallet* telah menyebar luas akibat banyak data yang diretas oleh oknum-oknum tertentu pada beberapa tahun terakhir. Oleh karena itu dana harus meningkatkan keamanan data pengguna untuk memastikan aplikasinya aman dan terlindungi dari serangan oknum nakal seperti *hacker* dan agar reputasi aplikasinya tidak jelek di kalangan masyarakat. Dana bisa mengambangkan reputasi positif dengan menerapkan manajemen sekuriti. Berdasarkan latar belakang masalah diatas, maka rumusan masalah pada penelitian ini yaitu:

1. Bagaimana cara Dana meningkatkan kepercayaan pengguna?
2. Apa saja upaya Dana menerapkan menggunakan Manajemen Sekuriti dalam aplikasinya?
3. Seberapa pengaruh Manajemen Sekuriti pada aplikasi Dana?

METODE

Metode penelitian yang digunakan dalam penelitian ini bertujuan untuk memahami penerapan manajemen sekuriti dalam meningkatkan keamanan data pengguna pada aplikasi DANA. Penelitian ini diawali dengan melakukan tinjauan *literatur* yang relevan untuk mengidentifikasi berbagai kerentanan keamanan yang kerap terjadi dalam transaksi *e-wallet* serta mengkaji strategi-strategi manajemen sekuriti yang telah diusulkan atau diterapkan oleh penyedia layanan *e-wallet*. Melalui tinjauan pustaka, penelitian ini mendapatkan pemahaman awal mengenai ancaman keamanan yang umum terjadi dalam ekosistem transaksi digital, khususnya yang berhubungan dengan perlindungan data pengguna.

Selanjutnya, penelitian ini mengumpulkan data melalui studi kasus dari para pengguna yang pernah mengalami serangan atau penipuan dalam menggunakan aplikasi *e-wallet*. Data ini diharapkan dapat memberikan wawasan tentang modus operandi yang umum digunakan oleh pelaku serangan, seperti metode *phishing*, rekayasa sosial, atau penyalahgunaan data pengguna lainnya. Dari studi kasus ini, peneliti menganalisis contoh-contoh kasus keamanan yang telah berhasil maupun yang gagal dalam implementasi strategi manajemen sekuriti pada aplikasi *e-wallet*, termasuk DANA.

HASIL DAN PEMBAHASAN

Hasil

Manajemen Sekuriti

Manajemen sekuriti merupakan serangkaian langkah yang diambil untuk mengelola keamanan dan mencegah kerugian yang disebabkan oleh ancaman yang dapat mengganggu sistem atau operasi. Konsep manajemen sekuriti melibatkan penerapan prinsip-prinsip yang efektif dan efisien untuk melindungi aset dan data penting dari potensi kerugian (Pradhana & Wibowo, 2020). Dengan demikian, tujuan utamanya adalah untuk mengidentifikasi, mencegah, dan mengurangi risiko yang dapat menimbulkan gangguan atau kerugian besar bagi suatu organisasi atau sistem.

Manajemen sekuriti terdiri dari dua elemen penting, yakni "manajemen" dan "sekuriti". Kata *manajemen* merujuk pada proses mengatur atau mengelola yang mencakup empat fungsi utama, yaitu perencanaan, pengorganisasian, pengarahan, dan pengawasan atau pengendalian. Fungsi ini bertujuan untuk memastikan bahwa setiap langkah yang diambil dalam pengelolaan sekuriti berjalan dengan baik dan efektif (Pradhana & Wibowo, 2020). Sedangkan, *sekuriti* mengacu pada serangkaian kegiatan yang dimulai dari perencanaan, pengorganisasian, pelaksanaan, hingga pengawasan dan pengendalian yang dilakukan secara terintegrasi dan profesional. Semua kegiatan ini bertujuan untuk mengurangi dan mencegah kerugian yang mungkin timbul akibat ancaman, baik yang bersifat internal maupun eksternal (Nova et al., 2023).

Manajemen sekuriti berfokus pada pencegahan kerugian yang dapat terjadi akibat ancaman yang berpotensi merusak sistem, baik itu ancaman fisik maupun digital. Proses ini memerlukan perencanaan yang matang, pengorganisasian yang efisien, serta pengawasan yang terus-menerus untuk memastikan bahwa setiap kebijakan dan prosedur yang diterapkan dapat mengurangi risiko dan melindungi sumber daya yang ada (Nova et al., 2023). Manajemen sekuriti yang efektif tidak hanya melibatkan perlindungan terhadap aset fisik, tetapi juga data dan informasi yang semakin penting dalam era digital.

Kebocoran Data

Kebocoran data pribadi menjadi salah satu masalah serius yang dapat merugikan pengguna, terutama dalam konteks aplikasi digital seperti DANA. Kebocoran ini terjadi ketika pihak yang tidak bertanggung jawab berhasil memperoleh informasi pribadi pengguna melalui

berbagai metode, termasuk panggilan telepon yang mengatasnamakan pihak resmi aplikasi, atau serangan berbasis teknik *phishing*. *Phishing*
adalah suatu metode penipuan di mana pelaku menyamar sebagai entitas yang sah, dengan tujuan untuk memperoleh informasi sensitif pengguna, seperti kata sandi, nomor rekening, atau data keuangan lainnya (Gundlach, 2020). Teknik ini sering kali digunakan untuk mengelabui pengguna agar memberikan data pribadi mereka, yang pada akhirnya dapat dimanfaatkan untuk kepentingan ilegal.

Permasalahan kebocoran data ini menimbulkan tantangan besar bagi perlindungan data pribadi, yang seharusnya dilindungi oleh kebijakan dan peraturan yang memadai. Oleh karena itu, perlindungan hukum terhadap data pribadi pengguna aplikasi DANA harus mencakup pengaturan yang jelas dari pemerintah dan otoritas keuangan. Di Indonesia, perlindungan data pribadi sudah diatur dalam Undang-Undang Perlindungan Data Pribadi (UU PDP), yang memberikan dasar hukum untuk menangani kebocoran data dan memberikan hak kepada pengguna untuk mengontrol data pribadi mereka (Sudirman, 2023). UU ini bertujuan untuk memastikan agar setiap penyelenggara aplikasi atau platform digital bertanggung jawab terhadap pengamanan data pribadi pengguna.

Pengguna aplikasi DANA juga harus lebih berhati-hati terhadap risiko kebocoran data yang dapat timbul akibat perilaku mereka sendiri, seperti membagikan informasi pribadi secara berlebihan di media sosial atau platform digital lainnya. Kesadaran akan risiko yang muncul dari berbagi informasi pribadi secara sembarangan sangat penting untuk mengurangi paparan terhadap ancaman kejahatan siber. Pengguna perlu memahami pentingnya menjaga kerahasiaan informasi sensitif, serta mengenali tanda-tanda potensi serangan phishing dan teknik manipulasi lainnya yang dapat digunakan oleh pelaku kejahatan siber (Gundlach, 2020).

Konsep Keamanan Data

Konsep keamanan data adalah aspek penting dalam pengelolaan informasi, terutama di era digital saat ini. Definisi keamanan data:

1. Pengertian umum keamanan data merujuk pada langkah-langkah dan kebijakan yang diterapkan untuk melindungi data dari akses yang tidak sah, kerusakan tau kehilangan (Ujung & Nasution, 2023).
2. Aspek keamanan data melibatkan beberapa aspek utama yaitu, kerahasiaan, integritas, dan ketersediaan (Daulay et al., 2023).

Tujuan Keamanan Data

Tujuan dari keamanan data adalah melindungi informasi dari penggunaan yang tidak sah dan menjamin keamanan integritas data, menerapkan kebijakan keamanan yang ketat, organisasi dapat mencegah kebocoran data yang dapat merugikan reputasi dan kepercayaan pengguna, dan pengawasan terhadap akses dan penggunaan data sangat penting untuk mendeteksi ancaman keamanan (Yel & Nasution, 2022).

Aplikasi Dana

Dompet digital merupakan aplikasi yang memudahkan pengguna untuk melakukan transaksi keuangan secara daring menggunakan perangkat mobile. Salah satu dompet digital yang populer di Indonesia adalah DANA, yang tersedia di Google Play Store dan menawarkan berbagai kemudahan dalam transaksi digital. DANA dirancang untuk mendukung pembayaran digital tanpa kartu (cashless dan cardless), baik untuk transaksi online maupun offline. Dengan adanya aplikasi ini, pengguna dapat dengan mudah melakukan berbagai transaksi keuangan seperti pembelian pulsa, pembayaran tagihan listrik, top-up saldo, serta transaksi lainnya yang terkait dengan kebutuhan sehari-hari (Larasati et al., 2022).

Fitur-fitur yang ditawarkan oleh DANA memungkinkan pengguna untuk melakukan berbagai aktivitas secara efisien dan tanpa perlu menggunakan uang tunai. Dalam hal ini, DANA berperan sebagai solusi praktis untuk pembayaran transaksi digital, sehingga mempermudah pengelolaan keuangan pengguna. Selain itu, DANA juga menyediakan layanan investasi, yang memberikan kesempatan bagi pengguna untuk menambah saldo investasi mereka secara mudah melalui aplikasi ini. Keamanan juga menjadi prioritas utama dalam aplikasi DANA, dengan sistem yang dirancang untuk memastikan kenyamanan dan perlindungan data pengguna saat melakukan transaksi (Larasati et al., 2022).

Tujuan utama dari pengembangan aplikasi DANA adalah untuk menyediakan sebuah platform pembayaran yang cepat, nyaman, dan aman bagi penggunanya. Aplikasi ini tidak hanya menawarkan kemudahan transaksi finansial, tetapi juga memberikan akses kepada pengguna untuk mengelola berbagai kebutuhan keuangan mereka secara lebih praktis, terutama di era digital yang semakin berkembang pesat. Dengan berbagai fitur yang terintegrasi dalam satu aplikasi, DANA semakin populer di kalangan masyarakat Indonesia sebagai solusi keuangan digital yang andal.

Penerapan Manajemen Sekuriti pada Aplikasi DANA

Penerapan manajemen sekuriti dalam aplikasi dana memiliki peran vital dalam meningkatkan keamanan pengguna. DANA menerapkan berbagai strategi untuk memastikan keamanan data pengguna, termasuk enkripsi tingkat tinggi seperti *Advanced Encryption Standard* (AES) untuk melindungi data selama penyimpanan dan transmisi. Selain itu, *autentikasi multi-faktor* (MFA) digunakan untuk memberikan lapisan keamanan tambahan, mengurangi risiko akses tidak sah (Azhari et al., 2024)

Tantangan dalam Manajemen Sekuriti

Meskipun berbagai langkah telah diambil, masih ada tantangan yang dihadapi oleh DANA dalam penerapan manajemen sekuriti:

1. **Ancaman Serangan Siber yang Semakin Kompleks**: Jenis ancaman seperti *phishing*, *ransomware*, dan serangan zero-day memerlukan strategi dan teknologi keamanan yang terus diperbarui.
2. **Perlindungan Data Pribadi**: Dalam lingkungan digital yang dinamis, menjaga privasi pengguna menjadi tantangan tersendiri seiring dengan perkembangan regulasi perlindungan data.

Tabel 1. Penelitian Terdahulu

No	Author (Tahun)	Judul Penelitian	Hasil Penelitian	Perbedaan/ *Novelty*	Persamaan
1.	Saputra, F., Soesanto, E., Cahyaningtyas, K. I., & Hakim, Z. L. (2024)	Penerapan Manajemen Security Terhadap Cyber Crime di Kominfo	manajemen keamanan yang efektif di Kementerian Komunikasi dan Informatika (Kemenkominfo) harus menjadi bagian integral dari strategi berkelanjutan dalam menghadapi ancaman siber. Langkah-langkah yang diterapkan, seperti kebijakan keamanan siber, pemantauan dan deteksi kejahatan siber, manajemen akses,	lebih menekankan pada kebijakan keamanan siber di sektor pemerintah, khususnya di Kementerian Komunikasi dan Informatika, untuk menghadapi ancaman siber secara umum.	pentingnya manajemen keamanan untuk melindungi data dan sistem dari ancaman siber, serta penerapan kebijakan dan langkah-langkah mitigasi untuk menjaga keamanan.

			program pendidikan dan pelatihan, serta rencana tanggap darurat keamanan, perlu dievaluasi dan ditingkatkan secara terus-menerus untuk memastikan relevansi dan efektivitasnya dalam menghadapi perkembangan ancaman siber yang semakin kompleks.		
2.	Zahwani, S. T., & Nasution, M. I. P. (2024).)	Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital	erlindungan data pribadi merupakan isu krusial di era digital yang memerlukan perhatian serius. Penelitian mengungkapkan bahwa peningkatan edukasi dan kesadaran masyarakat dapat membantu meminimalkan risiko kebocoran data dan melindungi privasi individu. Temuan penting dari penelitian ini mencakup tingkat kesadaran masyarakat tentang perlindungan data pribadi, faktor-faktor yang memengaruhinya, serta dampak negatif yang timbul akibat kurangnya pemahaman terhadap perlindungan data pribadi.	lebih mengarah pada kesadaran masyarakat secara umum tentang pentingnya perlindungan data pribadi di dunia digital.	isu perlindungan data pribadi, dengan fokus pada upaya untuk mengurangi risiko kebocoran data dan meningkatkan kesadaran akan pentingnya menjaga keamanan informasi pribadi di era digital.
3.	Soesanto, E., Salsabilah, F., Abadi, I. C., & Rizky, M. (2023).	Peran Manajemen Sekuriti Bank BRI untuk Menjaga Kepercayaan Nasabah	Bank BRI menerapkan asesmen keamanan yang menyeluruh dalam setiap proses bisnis untuk memastikan keberlanjutan dan profitabilitas yang optimal. Menghadapi ancaman kejahatan siber yang terus berkembang, bank ini membangun kesadaran di kalangan karyawan dan nasabah mengenai pentingnya perlindungan data dan keamanan transaksi. Sebagai langkah pengamanan, Bank BRI mengimplementasikan sistem dua lapis, yaitu	penerapan manajemen sekuriti di sektor perbankan untuk menjaga kepercayaan nasabah dan mencegah kejahatan siber dalam layanan digital perbankan.	mengkaji penerapan sistem keamanan untuk melindungi data pribadi dan transaksi digital, serta menekankan pentingnya kesadaran dan proteksi data sebagai bagian dari strategi manajemen sekuriti di dunia digital.

	Secure Socket Layer (SSL) dan kombinasi ID serta kata sandi untuk mengakses situs resmi mereka,	

Pembahasan

Penerapan Manajemen Sekuriti pada Aplikasi DANA

Dalam upaya meningkatkan keamanan data pengguna, DANA menerapkan beberapa strategi manajemen sekuriti yang berfokus pada proteksi data pribadi dan pencegahan terhadap potensi ancaman siber. Beberapa langkah yang diterapkan DANA dalam manajemen sekuriti meliputi:

1. **Enkripsi Data**
   DANA menggunakan *Advanced Encryption Standard* (AES) untuk mengenkripsi data selama proses penyimpanan dan transmisi. Enkripsi ini bertujuan untuk menjaga kerahasiaan informasi pengguna dari akses yang tidak sah.
2. ***Autentikasi Multi-Faktor* (MFA)**
   Aplikasi ini juga menggunakan autentikasi multi-faktor, yang mengharuskan pengguna untuk melakukan verifikasi tambahan saat melakukan transaksi atau login dari perangkat baru. MFA menambahkan lapisan perlindungan ekstra yang membantu mencegah akses oleh pihak yang tidak berwenang.
3. **Pemantauan dan Deteksi Ancaman *Real-Time***
   DANA juga melakukan pemantauan dan deteksi ancaman secara *real-time*. Dengan teknologi ini, mereka dapat mengidentifikasi dan menangani ancaman siber dengan cepat, seperti upaya peretasan atau Aktivitas Mencurigakan lainnya.
4. **Edukasi Pengguna**
   DANA menyadari pentingnya edukasi kepada pengguna terkait praktik keamanan, seperti penggunaan password yang kuat, kewaspadaan terhadap *phishing*, dan langkah-langkah perlindungan data pribadi lainnya. Edukasi ini bertujuan untuk meningkatkan kesadaran pengguna akan pentingnya menjaga keamanan data mereka

Cara Dana Meningkatkan Kepercayaan Pengguna

Kepercayaan pengguna terhadap aplikasi Dana dapat ditingkatkan melalui beberapa langkah strategis dalam manajemen keamanan dan pelayanan yang transparan. Kepercayaan merupakan faktor yang sangat penting dalam penggunaan aplikasi digital, terutama aplikasi pembayaran dan dompet digital seperti Dana, yang berhubungan langsung dengan transaksi finansial dan data pribadi pengguna. Untuk itu, pendekatan yang tepat dan efektif dalam meningkatkan kepercayaan pengguna perlu diambil dengan serius (Ramadhan & Nur, 2024).

Salah satu langkah pertama yang dapat diambil untuk meningkatkan kepercayaan pengguna adalah dengan memastikan bahwa aplikasi Dana menggunakan sistem keamanan data yang kuat. Keamanan data sangat penting untuk melindungi informasi pribadi dan transaksi pengguna dari ancaman pihak ketiga. Dalam hal ini, Dana telah mengimplementasikan teknologi canggih seperti enkripsi untuk melindungi data pengguna, termasuk data transaksi dan informasi pribadi seperti nomor kartu kredit, alamat, dan data sensitif lainnya (Faizal et al., 2023).

Enkripsi adalah salah satu metode yang paling efektif untuk melindungi data dalam proses transmisi, karena data yang terenkripsi hanya dapat diakses oleh pihak yang memiliki kunci yang sesuai. Dengan menggunakan enkripsi, aplikasi Dana dapat mencegah peretasan dan pencurian data yang dapat merusak kepercayaan pengguna (Pratama, 2024).

Aplikasi Dana juga dapat mengimplementasikan autentikasi dua faktor (2FA). Sistem ini meminta pengguna untuk memverifikasi identitas mereka melalui dua langkah yang berbeda

sebelum dapat mengakses akun mereka. Langkah pertama biasanya adalah memasukkan kata sandi, dan langkah kedua bisa berupa kode verifikasi yang dikirimkan ke perangkat pengguna melalui SMS atau aplikasi autentikasi lainnya (Erwin et al., 2023). Penelitian oleh Rofi (2022) menunjukkan bahwa penggunaan autentikasi dua faktor dapat mengurangi potensi ancaman terhadap akun pengguna dan memberikan lapisan perlindungan tambahan. Dengan adanya autentikasi dua faktor, risiko kebocoran data akibat peretasan dapat diminimalkan, sehingga meningkatkan kepercayaan pengguna terhadap keamanan aplikasi Dana.

Dana juga dapat meningkatkan keamanan dan mengurangi risiko operasional dengan mengadopsi standar keamanan internasional, seperti PCI DSS (Payment Card Industry Data Security Standard). PCI DSS adalah standar yang mengatur perlindungan data pengguna kartu kredit dan debit, yang diterima secara global oleh industri finansial dan teknologi pembayaran. Penggunaan standar PCI DSS, sebagaimana diungkapkan oleh Rofi (2022), terbukti efektif dalam mengurangi potensi risiko operasional, seperti pencurian data kartu kredit atau kebocoran informasi transaksi. Dengan mematuhi standar ini, Dana dapat menunjukkan komitmennya terhadap keamanan data pengguna dan meningkatkan kepercayaan publik terhadap aplikasi mereka.

Langkah penting lainnya adalah edukasi kepada pengguna mengenai pentingnya perlindungan data pribadi. Pengguna yang tidak sadar akan ancaman terhadap data pribadi mereka cenderung lebih rentan terhadap penipuan atau pencurian data. Oleh karena itu, Dana perlu menyediakan informasi dan panduan yang jelas kepada pengguna mengenai cara melindungi data mereka saat menggunakan aplikasi. Ini dapat mencakup langkah-langkah seperti penggunaan kata sandi yang kuat, mengenali tanda-tanda phishing, dan tidak membagikan informasi sensitif secara sembarangan. Sebagaimana diungkapkan oleh Zahwani dan Nasution (2024), kesadaran masyarakat tentang perlindungan data pribadi di era digital sangat penting. Edukasi ini tidak hanya membantu pengguna menjaga data mereka sendiri, tetapi juga meningkatkan tingkat kepercayaan mereka terhadap aplikasi yang mereka gunakan, karena mereka merasa dilindungi dan mendapatkan informasi yang transparan tentang keamanan.

Transparansi dalam kebijakan privasi dan pengelolaan data pribadi juga memainkan peran yang sangat penting dalam meningkatkan kepercayaan pengguna. Dana perlu memberikan informasi yang jelas dan mudah dipahami mengenai bagaimana data pengguna dikumpulkan, disimpan, dan digunakan. Pengguna harus merasa yakin bahwa data mereka tidak akan disalahgunakan atau dibagikan tanpa izin. Kebijakan privasi yang jelas, yang menjelaskan dengan rinci mengenai perlindungan data dan hak-hak pengguna, juga dapat membantu membangun kepercayaan. Dengan memiliki kebijakan yang transparan, Dana dapat menunjukkan komitmennya untuk melindungi data pengguna dan memberikan layanan yang adil (Endrosava & Afiliasi, 2024).

Agar aplikasi Dana tetap aman dalam jangka panjang, perusahaan perlu melakukan pemantauan dan audit keamanan secara berkala. Proses ini bertujuan untuk memastikan bahwa sistem keamanan yang ada tetap efektif dan sesuai dengan perkembangan teknologi serta ancaman yang muncul. Selain itu, audit keamanan juga dapat membantu menemukan celah-celah yang mungkin belum terdeteksi dan memungkinkan perbaikan sebelum masalah lebih besar terjadi (Silitonga & Arsjah, 2024).

Upaya Dana Menerapkan Manajemen Sekuriti Dalam Aplikasinya

Dana, sebagai aplikasi dompet digital yang mengelola transaksi dan data pengguna, menerapkan manajemen sekuriti yang efektif untuk mengatasi berbagai risiko siber yang dapat mengancam integritas aplikasi dan melindungi data pengguna. Keamanan merupakan salah satu aspek paling vital dalam aplikasi keuangan digital, mengingat tingginya nilai dan kepekaan informasi yang dikelola. Oleh karena itu, Dana mengambil langkah-langkah yang tegas dalam

memitigasi risiko-risiko ini, dengan salah satunya mengembangkan sistem deteksi dan pemantauan yang kuat untuk mendeteksi potensi ancaman dan serangan siber secara dini. Sistem ini berfungsi untuk memantau aktivitas yang mencurigakan dalam waktu nyata, sehingga jika ada potensi serangan atau kebocoran data, tindakan pencegahan dapat segera dilakukan untuk meminimalisir kerugian (Azhari et al., 2024).

Dana juga mengimplementasikan kebijakan keamanan yang ketat dalam pengelolaan identitas dan akses pengguna. Keamanan identitas pengguna menjadi hal yang sangat krusial karena aplikasi ini mengelola informasi sensitif seperti nomor rekening, riwayat transaksi, dan data pribadi lainnya. Oleh karena itu, Dana memastikan bahwa setiap akses ke akun pengguna dilindungi dengan tingkat autentikasi yang tinggi. Dalam hal ini, enkripsi memainkan peran yang sangat penting. Teknologi **enkripsi** yang digunakan dalam transaksi atau pengiriman data memastikan bahwa informasi yang ditransfer hanya dapat dibaca oleh pihak yang berwenang, mencegah pihak ketiga yang tidak berhak mengakses data tersebut (Alia et al., 2024).

Penerapan autentikasi yang ketat juga diupayakan melalui autentikasi dua faktor (2FA), yang merupakan tambahan perlindungan untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses aplikasi. Dengan autentikasi dua faktor, pengguna diharuskan untuk memasukkan kode verifikasi selain kata sandi, yang umumnya dikirimkan melalui SMS atau aplikasi otentikator, sehingga memberikan lapisan keamanan tambahan. Pendekatan ini secara signifikan mengurangi kemungkinan akses tidak sah yang dapat membahayakan data dan transaksi pengguna (Syarifal., 2023).

Menurut Fachrudin et al. (2024), kebijakan keamanan yang jelas dan penanganan risiko yang tepat sangat penting dalam melindungi data dan informasi pengguna. Dalam konteks ini, Dana telah mengimplementasikan kebijakan yang tidak hanya melindungi data pengguna secara fisik, tetapi juga memastikan bahwa seluruh sistem aplikasi berjalan sesuai dengan standar keamanan internasional yang berlaku. Penerapan Secure Socket Layer (SSL), misalnya, menjamin bahwa semua komunikasi antara pengguna dan server Dana terenkripsi, membuat data yang dikirimkan lebih aman dari ancaman peretasan atau intersepsi oleh pihak ketiga.

Dengan adanya sistem keamanan yang komprehensif ini, Dana dapat menjaga integritas informasi transaksi pengguna. Sistem SSL dan autentikasi dua lapis memberikan rasa aman yang tinggi bagi pengguna, yang tahu bahwa informasi mereka terlindungi dari ancaman peretasan yang semakin canggih. Adanya perlindungan seperti ini sangat penting, mengingat data yang tidak terproteksi dengan baik dapat dengan mudah jatuh ke tangan yang salah, yang berpotensi menyebabkan kerugian besar bagi pengguna maupun pihak aplikasi (Muni, 2024).

Pengaruh Manajemen Sekuriti Pada Aplikasi Dana

Manajemen sekuriti memiliki peran yang sangat penting dalam menentukan keberhasilan aplikasi digital, termasuk Dana, yang merupakan salah satu aplikasi dompet digital yang populer di Indonesia. Keamanan aplikasi bukan hanya masalah teknis, melainkan juga merupakan faktor yang mempengaruhi kepuasan pengguna secara signifikan. Penelitian yang dilakukan oleh Andika et al. (2024) menunjukkan bahwa sekitar 38,9% dari tingkat kepuasan pengguna Dana dipengaruhi oleh kualitas layanan dan keamanan aplikasi. Hal ini membuktikan bahwa pengguna sangat menghargai aspek keamanan dalam penggunaan aplikasi digital, terutama dalam konteks transaksi finansial yang melibatkan data pribadi dan informasi sensitif lainnya.

Keamanan aplikasi Dana mencakup beberapa elemen yang sangat krusial, seperti proteksi terhadap data pribadi pengguna, pengamanan transaksi, serta perlindungan terhadap ancaman siber. Mengingat bahwa aplikasi Dana memproses transaksi keuangan yang melibatkan uang, maka adanya potensi risiko yang terkait dengan peretasan, kebocoran data, atau penggunaan aplikasi oleh pihak yang tidak sah sangat mungkin terjadi. Oleh karena itu, kebijakan keamanan yang diterapkan dalam aplikasi Dana menjadi salah satu faktor penentu

utama bagi pengguna dalam memutuskan untuk terus menggunakan aplikasi tersebut. Keamanan yang kuat memberikan rasa aman dan kenyamanan bagi pengguna dalam melakukan berbagai transaksi, yang pada gilirannya meningkatkan kepercayaan mereka terhadap aplikasi ini I(Safalla, 2024).

Kepercayaan yang dibangun melalui manajemen sekuriti yang baik secara langsung berkontribusi terhadap peningkatan loyalitas pengguna. Ketika pengguna merasa bahwa data pribadi dan transaksi mereka dilindungi dengan baik, mereka lebih cenderung untuk terus menggunakan aplikasi tersebut. Hal ini juga berhubungan dengan keputusan pengguna untuk merekomendasikan aplikasi Dana kepada orang lain, yang berpotensi meningkatkan jumlah pengguna baru dan memperkuat posisi aplikasi tersebut di pasar. Dalam hal ini, manajemen sekuriti yang efektif tidak hanya berfungsi untuk melindungi data, tetapi juga untuk membangun hubungan yang lebih kuat antara aplikasi dan penggunanya (Nur et al., 2024).

penelitian yang dilakukan oleh Saputra et al. (2024) menjelaskan bahwa manajemen sekuriti yang efektif di sektor digital dapat meminimalkan berbagai risiko yang dihadapi oleh pengguna. Risiko ini mencakup potensi ancaman kejahatan siber seperti peretasan, penipuan, atau pencurian identitas, yang dapat merugikan pengguna dan merusak reputasi aplikasi. Dengan mengimplementasikan kebijakan dan teknologi keamanan yang tepat, Dana dapat mengurangi kemungkinan terjadinya insiden seperti itu, sehingga pengguna merasa lebih aman dan nyaman. Dalam jangka panjang, pengelolaan keamanan yang baik tidak hanya membantu mengurangi risiko, tetapi juga meningkatkan keberlanjutan penggunaan aplikasi karena pengguna merasa terlindungi dan diprioritaskan oleh pengembang aplikasi.

KESIMPULAN

Penerapan manajemen sekuriti pada aplikasi DANA sangat penting dalam menjaga keamanan data pengguna dan meningkatkan kepercayaan mereka terhadap aplikasi. Melalui langkah-langkah seperti enkripsi data, autentikasi multi-faktor, pemantauan ancaman secara real-time, serta edukasi kepada pengguna, DANA berhasil menciptakan lingkungan yang lebih aman untuk transaksi digital. Keamanan yang diterapkan tidak hanya berfungsi untuk melindungi data pribadi dan transaksi pengguna, tetapi juga memperkuat loyalitas dan kepercayaan pengguna terhadap aplikasi. Dengan demikian, manajemen sekuriti memiliki pengaruh besar dalam memastikan keberlanjutan penggunaan aplikasi serta mencegah risiko ancaman siber yang dapat merugikan pengguna.

Untuk meningkatkan efektivitas manajemen sekuriti, DANA perlu terus mengembangkan dan memperbarui teknologi keamanan sesuai dengan perkembangan ancaman siber yang semakin canggih. Selain itu, penting bagi DANA untuk terus melakukan audit dan pemantauan sistem keamanan secara berkala guna mengidentifikasi celah atau potensi risiko yang belum terdeteksi. DANA juga disarankan untuk lebih fokus pada edukasi pengguna mengenai praktik keamanan digital, serta meningkatkan transparansi dalam kebijakan privasi dan pengelolaan data pengguna. Dengan langkah-langkah tersebut, DANA dapat lebih meningkatkan kepercayaan pengguna dan memperkuat posisinya di pasar dompet digital.

REFERENSI

Alia, R., Firdausy, F. A., & Lutfiana, S. A. (2024). ANALISIS EFEKTIVITAS PERLINDUNGAN HUKUM TERHADAP NASABAH DALAM TRANSAKSI PERBANKAN DIGITAL. Causa: Jurnal Hukum dan Kewarganegaraan, 7(3), 1-10.

Azhari, F., Sumarno, S., Fauzi, A., Pratama, D. R., Musyafa, M. A., Nawawi, M. R., & Ghaffar, N. S. A. (2024). Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet. *Jurnal Kewirausahaan Dan Multi Talenta*, *2*(2), 138–147.

Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia: Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, *3*(2), 145-160.

Daulay, A. P. E., Febriana, V., Kita, A. D. A., Gunawan, S., & Nurbaiti, N. (2023). Keamanan dalam Sistem Database Sebagai Sumber Informasi Manajemen Terhadap Perlindungan Data. *EDU SOCIETY: JURNAL PENDIDIKAN, ILMU SOSIAL DAN PENGABDIAN KEPADA MASYARAKAT*, *3*(2), 988–991.

Endrosava, A. A., & Afiliasi, S. (2024). Peran Regulasi Modern dalam Menjaga Integritas Sistem Hukum Perbankan Digital. Jurnal Multidisiplin Ilmu Akademik, 1(6), 228-235.

Erwin, E., Pasaribu, A. W., Novel, N. J. A., Thaha, A. R., Adhicandra, I., Suardi, C., ... & Syafaat, M. (2023). Transformasi Digital. PT. Sonpedia Publishing Indonesia.

Faizal, M. A., Faizatul, Z., Asiyah, B. N., & Subagyo, R. (2023). Analisis Risiko Teknologi Informasi Pada Bank Syariah: Identifikasi Ancaman Dan Tantangan Terkini. Jurnal Asy-Syarikah: Jurnal Lembaga Keuangan, Ekonomi Dan Bisnis Islam, 5(2), 87-100.

Fachrudin, R., Respaty, E., Adilah, I. S., & Sinlae, F. (2024). Peranan Penting Manajemen Sekuriti di Era Digitalisasi. *Nusantara Journal of Multidisciplinary Science*, *1*(6), 99-107.

Hijriani, H., Nur, M. N. A., Ali, A., Ali, A., & Siregar, W. A. (2023). Literasi Digital Perlindungan Hukum Terhadap Data Pribadi Nasabah Pengguna Electronic Wallet. Sultra Research of Law, 5(2), 85-95.

Hikmah, A., & Nurlinda, R. A. (2023). Pengaruh Persepsi Manfaat Dan Persepsi Keamanan Terhadap Niat Menggunakan Melalui Kepercayaan Konsumen Pada Aplikasi Dompet Digital DANA. *Journal of Management and Creative Business*, *1*(4), 181-202.

Hutapea, Y., Fauzi, A., Dwiyanti, A., Alifah, F. A., Andina, N., & Jati, S. M. D. (2024). Peran Manajemen Sekuriti Dalam Mencegah Resiko Kerugian Terhadap Keuangan Digital. *Jurnal Kewirausahaan dan Multi Talenta*, *2*(2), 148-161.

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*, *4*(5), 625-632.

Larasati, F. A., Ratnawati, D. E., & Hanggara, B. T. (2022). Analisis Sentimen Ulasan Aplikasi Dana dengan Metode Random Forest. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *6*(9), 4305–4313.

Muni, A., Kom, S., & Kom, M. (2024). KRIPTOGRAFI UNTUK KEAMANAN SISTEM INFORMASI Copyright@ 2024 by Abdul Muni, S. Kom., M. Kom., dkk. PENERBIT KBM INDONESIA.

Nur, A., Wulandari, A. P., Azzahra, A. A., Nurjanah, H., & Prizy, A. R. (2024). FAKTOR YANG MEMPENGARUHI KEPERCAYAAN KONSUMEN TERHADAP KEAMANAN E-COMMERCE. Kohesi: Jurnal Sains dan Teknologi, 5(1), 51-60

Nafi'ah, R. (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce. *Cyber Security Dan Forensik Digital*, *3*(1), 7-13.

Ningrum, D. A., Fauzi, A., Syaridwan, A., Putri, I. A., Putri, N. M., & Putri, S. A. (2023). Peran Manajemen Sekuriti Terhadap Keputusan Pembelian pada Pengguna Aplikasi Shopee (Studi Pustaka Manajemen Sekuriti). *Jurnal Ilmu Manajemen Terapan*, *4*(5), 731-737.

Nova, S. D., Soesanto, E., Moses, H., & Ramadan, R. (2023). Analisis dan Pengembangan Sistem Manajemen Sekuriti pada PT. Denso Manufacturing Indonesia. *Jurnal Ilmiah Wahana Pendidikan*, *9*(13), 225–236.

Pitura, R. C., & Rachma, N. (2022). Pengaruh Persepsi Kemudahan Dan Persepsi Keamanan Terhadap Keputusan Penggunaan E-Wallet Shopeepay Di Kalangan Generasi Millenial

(Studi Pada Mahasiswa Manajemen UNISMA Angkatan 2018). *E-JRM: Elektronik Jurnal Riset Manajemen*, *11*(25).

Pradhana, F. A., & Wibowo, P. (2020). Analisis Pola Komunikasi Petugas pada Manajemen Sekuriti di Lembaga Pemasyarakatan. *Gema Keadilan*, *7*(3), 139–154.Rofi, N. (2022). Analisis manajemen resiko operasional pengguna aplikasi e-wallet "Dana" dengan implementasi PCI DSS. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *9*(5), 1786-1794.

Putra, R. G., Fauzi, A., Prasetyo, E. T., Pratama, S. R., Ramadhan, I. D., Febriyanti, F., & Nurlela, S. (2023). Pentingnya Manajemen Security di Era Digitalisasi. 2(1). https://doi.org/10.38035/jim.v2i

Pratama, A. (2024, September). KRIPTOGRAFI MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD (AES-128) UNTUK MENGAMANAN FILE KEPENDUDUKAN PADA KELURAHAN SUDIMARA BARAT. In Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI) (Vol. 3, No. 2, pp. 49-57).

Ramadhan, G., & Nur, A. (2024). ANALISIS PENGGUNAAN MOBILE WALLET UNTUK TRANSAKSI e-commerce DI KALANGAN MILENIAL. Kohesi: Jurnal Sains dan Teknologi, 4(11), 41-50.

Rahayu, P., & Rangkuti, S. (2022). Analisis Manajemen Risiko Penggunaan Aplikasi E-Commerce dalam Transaksi Penjualan CV. Roti Aroma Bakery dan Cake Shop Medan. *Bisnis-Net Jurnal Ekonomi dan Bisnis*, *5*(1), 55-68.

Rofi, N. (2022). Analisis manajemen resiko operasional pengguna aplikasi e-wallet "Dana" dengan implementasi PCI DSS. *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial*, *9*(5), 1786-1794.

Rozi, A. S. (2022). *PENGARUH KEAMANAN, KEMANFAATAN DAN KEPERCAYAAN TERHADAP KEPUASAN DALAM MENGGUNAKAN APLIKASI E-WALLET DANA* (Doctoral dissertation, Universitas Putra Bangsa).

Safalla, N. J. (2024). PERLINDUNGAN HUKUM KONSUMEN TERHADAP TINDAK PIDANA PENCURIAN DATA PRIBADI DALAM TRANSAKSI E-COMMERCE DI INDONESIA (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).

Silitonga, C. A., & Arsjah, R. J. (2024). ANALISIS PERSIAPAN PEMANFAATAN DIGITALISASI PENGALIHAN ANGGARAN BIAYA OPERASIONAL BERBASIS WEB (STUDI KASUS PADA PT XYZ). Jurnal Ekonomi Trisakti, 4(1), 123-134.

Syafrial, H. (2023). Literasi digital. Nas Media Pustaka.

Saputra, F., Soesanto, E., Cahyaningtyas, K. I., & Hakim, Z. L. (2024). Penerapan Manajemen Security Terhadap Cyber Crime di Kominfo. *IJM: Indonesian Journal of Multidisciplinary*, *2*(1).

Saputri, D. A. E., Ernawati, I. A., Rabbaanii, N. A. N., & Satriani, A. D. (2023). Penerapan AAA Security Dalam Aplikasi BNI Mobile Banking. *Indonesian Journal of Innovation Multidisipliner Research*, *1*(2), 63-73.

Septia, G., Ningsih, R. A., Faadhilah, S. D. N., & Anugrah, D. (2024). PERLINDUNGAN HUKUM TERHADAP PENGGUNA APLIKASI E-WALLET DANA ATAS KEJAHATAN LINK PHISING DAN HACKING PADA LAYANAN DIGITAL. Letterlijk, 1(1), 66-82.

Silalahi, P. R., Daulay, A. S., Siregar, T. S., & Ridwan, A. (2022). Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online. *Profit: Jurnal Manajemen, Bisnis dan Akuntansi*, *1*(4), 224-235.

Soesanto, E., Telaumbanua, K. K., Dzaky, M., & Sherenika, F. N. (2023). SISTEM MANAJEMEN SEKURITI PADA PT TELKOM INDONESIA. *Abdi Jurnal Publikasi*, *1*(6), 519-524.

Surahman, F. (2023). Tantangan Dalam Menjaga Keamanan Data Official Statistics dari Serangan Cybercrime. *Madani: Jurnal Ilmiah Multidisiplin*, *1*(11).

Tony Sitinjak, M. M. (2019). Pengaruh persepsi kebermanfaatan dan persepsi kemudahan penggunaan terhadap minat penggunaan layanan pembayaran digital Go-Pay. *Jurnal manajemen*, *8*(2).

Umiyati, I., Putri, T. E., & Maya, N. (2021). Social Influence, Usability And Security On The Intensity Of DANA e-Wallet Use. *JASS (Journal of Accounting for Sustainable Society)*, *3*(01).

Ujung, A. M., & Nasution, M. I. P. (2023). Pentingnya Sistem Keamanan Database untuk melindungi data pribadi. *Jurnal Sistem Informasi Dan Informatika*, *1*(2), 44–47.

Yel, M. B., & Nasution, M. K. M. (2022). Keamanan informasi data pribadi pada media sosial. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92–101.

Yuwinanto, H. P. (2015). Privasi online dan keamanan data. *Palimpsest*, *31*(11).

Zahwani, S. T., & Nasution, M. I. P. (2024). Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital. *Journal of Sharia Economics Scholar (JoSES)*, *2*(2).