Jurnal Kewirausahaan dan Multi Talenta (JKMT)
E-ISSN : 2962-8873
P-ISSN : 2964-6049
Siber Nusantara Publisher
+62 811 7404 445 http://siberpublisher.org siberpublisher.info@gmail.com Jalan Marina Indah Raya No. 1 Pantai Indah Kapuk, Kamal Muara, Penjaringan, Jakarta Utara, Indonesia.
DOI: https://doi.org/10.38035/jkmt.v2i2
Received: 10 April 2024, **Revised:** 22 Mei 2024, **Publish:** 10 Juni 2024

Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet

Farhan Azhari[1], Sumarno Sumarno[2], Achmad Fauzi[3], Demas Rizky Pratama[4], Muhammad Adityn Musyafa[5], Muhammad Rifa Nawawi[6], Naufal Shafly Abdul Ghaffar[7]
[1]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: farhanazhari210@gmail.com
[2]Dosen Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: sumarno@dsn.ubharajaya.ac.id
[3]Dosen Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: achmad.fauzi@dsn.ubharajaya.ac.id
[4]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: rizkydem36@gmail.com
[5]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: adityn22@gmail.com
[6]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: muhammadrifanawawi@gmail.com
[7]Mahasiswa Program Studi Manajemen, Universitas Bhayangkara Jakarta Raya, Indonesia, email: saflinaufal21@gmail.com

[*]Corresponding Author: Farhan Azhari[1]

Abstract**:** *The implementation of security management is crucial in ensuring the security of electronic transactions, especially in the context of using e-wallets. E-wallet has become one of the popular solutions in conducting online transactions, but it is often vulnerable to cyber attacks and identity theft. This paper aims to explore security management strategies and practices that can be applied to enhance user security in e-wallet transactions. The method used involves literature study and data analysis to identify common security threats faced by e-wallet users as well as mitigation measures that can be taken to reduce such risks. Some of the strategies discussed include data encryption, multi-factor authentication, suspicious transaction monitoring, and user education on digital security practices. It is expected that the understanding and implementation of these security management practices will provide better protection for e-wallet users and increase their confidence in using electronic transaction services.*

Keywords: *Security Management, User Security, E-wallet Transactions*

Abstrak: Penerapan manajemen sekuriti merupakan hal yang krusial dalam menjamin keamanan transaksi elektronik, terutama dalam konteks penggunaan e-wallet. E-wallet menjadi

salah satu solusi populer dalam melakukan transaksi online, namun sering kali rentan terhadap serangan cyber dan pencurian identitas. Tulisan ini bertujuan untuk mengeksplorasi strategi dan praktik manajemen sekuriti yang dapat diterapkan untuk meningkatkan keamanan pengguna pada transaksi e-wallet. Metode yang digunakan melibatkan studi literatur dan analisis data untuk mengidentifikasi ancaman keamanan yang umum dihadapi oleh pengguna e-wallet serta langkah-langkah mitigasi yang dapat diambil untuk mengurangi risiko tersebut. Beberapa strategi yang dibahas meliputi enkripsi data, otentikasi multi-faktor, pemantauan transaksi yang mencurigakan, dan pendidikan pengguna tentang praktik keamanan digital. Diharapkan bahwa pemahaman dan penerapan praktik manajemen sekuriti ini akan memberikan perlindungan yang lebih baik bagi pengguna e-wallet dan meningkatkan kepercayaan mereka dalam menggunakan layanan transaksi elektronik.

Kata Kunci: Mananjemen sekuriti, Keamanan Pengguna, Transaksi E-wallet

PENDAHULUAN

Dalam era digitalisasi yang pesat seperti saat ini, penggunaan e-wallet atau dompet digital telah menjadi salah satu tren utama dalam sistem pembayaran. E-wallet memungkinkan pengguna dengan mudah melakukan berbagai transaksi keuangan online, mulai dari membayar tagihan, membeli barang dan jasa, hingga mentransfer uang antar individu. Pesatnya perkembangan transaksi online beberapa tahun terakhir juga secara tidak langsung sangat memudahkan perkembangan sistem pembayaran.(Rozi, 2022) .Namun, seiring dengan kemudahan yang ditawarkan oleh e-wallet, muncul pula tantangan besar terkait dengan keamanan dan perlindungan data pengguna.

Pentingnya keamanan transaksi e-wallet tidak bisa diragukan lagi. Hampir seluruh bidang industri yang ada di dunia tersentuh oleh IT, Salah satunya pada industri keuangan(Purba et al., 2020) Dengan adanya ancaman seperti pencurian identitas, peretasan akun, dan serangan malware, pengguna e-wallet rentan mengalami kerugian finansial dan kerugian lainnya jika tidak dilakukan tindakan pencegahan yang tepat. Oleh karena itu, penerapan manajemen sekuriti menjadi krusial dalam meningkatkan keamanan pengguna pada transaksi e-wallet. Dalam konteks ini, manajemen sekuriti tidak hanya mencakup aspek teknis seperti enkripsi data dan firewall, tetapi juga melibatkan kebijakan, prosedur, dan pengelolaan risiko yang holistik. Dengan menerapkan strategi manajemen sekuriti yang efektif, penyedia layanan e-wallet dapat menjaga integritas, kerahasiaan, dan ketersediaan data pengguna dengan lebih baik, sehingga meningkatkan kepercayaan dan kepuasan pengguna.

pentingnya manajemen sekuriti dalam konteks transaksi e-wallet, menyoroti beberapa tantangan utama yang dihadapi, dan mengeksplorasi strategi dan praktik terbaik untuk meningkatkan keamanan pengguna. Melalui pemahaman mendalam tentang manajemen sekuriti, diharapkan dapat memberikan wawasan yang berharga bagi para penyedia layanan e-wallet dan pengguna dalam menjaga keamanan dan privasi dalam bertransaksi secara digital.

Berdasarkan latar belakang masalah diatas, maka rumusan masalah pada penelitian ini yaitu:

1. Bagaimana tingkat efektivitas manajemen sekuriti saat ini dalam melindungi keamanan pengguna pada transaksi e-wallet?
2. Bagaimana peran kesadaran pengguna dan pelaksanaan praktik keamanan digital dalam meningkatkan perlindungan terhadap transaksi e-wallet?
3. Apa peran manajemen sekuriti yang dapat diterapkan dalam manajemen sekuriti e-wallet untuk mengurangi risiko keamanan?

KAJIAN PUSTAKA

Manajemen Sekuriti

Manajemen sekuriti adalah upaya komprehensif untuk melindungi aset penting suatu organisasi dari berbagai ancaman, kerentanan, dan risiko yang mungkin terjadi. Aset ini meliputi informasi sensitif, infrastruktur TI, perangkat keras, perangkat lunak, jaringan, dan sumber daya lain yang vital bagi operasi organisasi. Proses manajemen sekuriti dimulai dengan penilaian risiko, di mana organisasi mengidentifikasi ancaman potensial, kerentanan dalam sistem, dan potensi dampak dari kejadian merugikan. Berdasarkan penilaian ini, organisasi merancang kebijakan, prosedur, dan praktik keamanan yang sesuai. Ini mencakup pengembangan aturan-aturan, pedoman, dan langkah-langkah untuk mengelola akses, melindungi data, dan merespons insiden keamanan.

Pengendalian akses merupakan bagian penting dari manajemen sekuriti, yang memastikan bahwa hanya orang yang diotorisasi yang dapat mengakses aset yang sensitif. Ini melibatkan penggunaan otentikasi, otorisasi berbasis peran, dan monitoring aktivitas pengguna. Selain itu, organisasi juga menerapkan teknologi keamanan seperti firewall, antivirus, enkripsi, dan deteksi intrusi untuk mencegah serangan dan kebocoran data. Meningkatnya serangan siber dan pembobolan data dalam beberapa tahun terakhir telah meningkatkan kekhawatiran pengguna Internet. Oleh karena itu, pengelolaan data pengguna memerlukan kontrol keamanan yang lebih kuat dan canggih(Ningrum et al., 2023).Pelatihan dan kesadaran menjadi komponen kunci dalam manajemen sekuriti, di mana organisasi memberikan pelatihan kepada karyawan tentang praktik keamanan yang baik dan meningkatkan kesadaran mereka tentang ancaman keamanan yang ada. Manajemen insiden juga merupakan aspek penting, dengan organisasi mempersiapkan diri untuk menangani insiden keamanan dengan cepat dan efisien.

Manajemen sekuriti merupakan pendekatan holistik yang melibatkan kombinasi strategi, kebijakan, prosedur, teknologi, pendidikan, dan pengawasan untuk melindungi aset-aset penting organisasi dari berbagai ancaman dan risiko keamanan. Ini memungkinkan organisasi untuk menjaga keberlangsungan operasional mereka, menjaga reputasi, dan memenuhi kebutuhan para pemangku kepentingan.

Keamanan

Keamanan adalah suatu kondisi atau situasi di mana individu, organisasi, atau sistem dilindungi dari berbagai risiko, ancaman, atau bahaya yang mungkin timbul. Konsep ini mencakup upaya proaktif dan preventif untuk mengidentifikasi, mencegah, mengurangi, atau mengatasi potensi ancaman terhadap aset atau kepentingan yang bernilai. Risiko keamanan dalam penggunaan uang elektronik dapat terjadi dalam bentuk pencurian, penggandaan kartu asli, modifikasi data atau aplikasi pada kartu asli, dan lain-lain.(Sari et al., 2020).Dalam konteks keamanan informasi dan teknologi, seperti e-wallet, keamanan melibatkan perlindungan terhadap integritas, kerahasiaan, dan ketersediaan data serta layanan yang dikomunikasikan, disimpan, atau diproses oleh sistem elektronik. Sistem pembayaran digital ini memberikan dampak yang signifikan terhadap keputusan pembelian, dan penggunaan media elektronik seperti smartphone telah meningkatkan minat dalam mengambil keputusan pembelian. (Fauzi et al., 2023).Keamanan pada e-wallet merujuk pada serangkaian tindakan, prosedur, dan teknologi yang diterapkan untuk melindungi informasi keuangan dan identitas pengguna, serta untuk memastikan keamanan transaksi finansial yang dilakukan melalui platform e-wallet. Ini mencakup perlindungan terhadap akses yang tidak sah, penggunaan data yang tidak sah, manipulasi transaksi, dan ancaman keamanan lainnya yang mungkin mengancam keberlangsungan operasional dan kepercayaan pengguna terhadap platform tersebut.

E-wallet

Menurut (Marhaendra & Mahyuzar, 2023) Uang elektronik adalah metode pembayaran yang diterbitkan berdasarkan nilai moneter yang disetorkan terlebih dahulu kepada penerbitnya. Nilai uang tersebut disimpan secara elektronik pada server media atau chip dan digunakan sebagai alat pembayaran oleh pedagang yang bukan penerbit uang elektronik tersebut.Dompet elektronik adalah jenis teknologi keuangan yang membuat pembayaran lebih nyaman bagi konsumen. (Susanti & Putra, 2023). E-wallet termasuk dalam kategori aset keuangan yang disimpan di server media. E-wallet dapat digunakan melalui aplikasi digital dan juga dapat menyimpan dana untuk melakukan transaksi pembayaran. (Dirnaeni et al., 2021)

Sistem pembayaran digital

Pengertian Pembayaran-pembayaran merupakan proses menukarkan mata uang dengan suatu barang atau jasa maupun informasi Pengertian Pembayaran Digital Sebagai sebuah alat yang menggunakan teknologi via ponsel untuk pembayaran, transfer atau melakukan transaksi lainnya. Pada masa kini berkembangnya teknologi pada sistem pembayaran telah menggeser perannya uang tunai sebagai alat pembayaran menjadi bentuk pembayaran non tunai atau pembayaran elektrik yang yang lebih efektif dan ekonomis.

Penelitian Terdahulu

Tabel 1. Penelitian Terdahulu Yang Relevan

No	Author (Tahun)	Judul Penelitian	Hasil Riset Terdahulu	Perbedaan/ Novelty
1	(Wijaya et al., 2023)	Implementasi Manajemen Sekuriti PT. KAI: K3, Manajemen Risiko, dan Standar Keamanan pada Perlintasan Kereta Api	Kesadaran dan kerja sama masyarakat serta peningkatan langkah- langkah keamanan seperti pemasangan palang pintu mungkin dapat meningkatkan keamanan di perlintasan ini di masa depan.	Perbedaan atau Novelty ada pada variabel E-wallet
2	(F. Saputra et al., 2024)	Penerapan Manajemen Security Terhadap Cyber Crime di Kominfo	Penerapan manajemen keamanan yang efektif di Kementerian Komunikasi dan Informatika perlu menjadi bagian integral dari strategi berkelanjutan dalam menghadapi ancaman siber.	Perbedaan atau Novelty ada pada variabel keamanan pengguna
3	(Fitria et al., 2023)	Manajemen Sekuriti Terintegrasi di PT. Unilever Indonesia Tbk: Ancaman, Manajemen Risiko, Standar Keamanan, dengan Fokus pada SSMKD	menggunakan manajemen risiko untuk menunjukkan komitmen kuat perusahaan untuk menjaga kinerja bisnis yang stabil dan berkelanjutan meskipun menghadapi berbagai masalah	Perbedaan atau Novelty ada pada variabel keamanan pengguna
4	(Oktavira et al., 2023)	Penerapan Manajemen Sekuriti Melalui Keamanan Industrial PT Wings Surya	Manajemen keamanan industrial di PT Wings Surya bertujuan untuk melindungi karyawan, aset perusahaan, dan menjaga operasional perusahaan berjalan lancar.	Perbedaan atau novelty pada variabel E-wallet

5	(Miftahurrizqi et al., 2021)	Analisis Keamanan Sistem Informasi Akdemik Menggunakan Cobit 5 FRAMEWORK Pada SUB Domain DSS05	Kepedulian dan kesadaran terhadap pentingnya keamanan sistem sudah terbangun tetapi tidak didukung oleh pengaturan kebijakan berupa panduan	Perbedaan atau Novelty ada pada variabel E-wallet
6	(Bakri & Irmayana, 2017)	Analisis dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001	Langkah pelaksanaan audit keamanan sistem informasi dilakukan dengan pembuatan pernyataan, identifikasi asset informasi, pembuatan pertanyaan, penentuan kendali berdasarkan temuan-temuan SMKI.	Perbedaan atau Novelty ada pada variabel E-wallet
7	(Susanto et., 2023)	Penerapan Keselamatan Kerja dan Kesehatan Kerja Melalui Manajemen Sekuriti Terhadap Produkivitas Pada PT. Epson	Dalam penerapan keselamatan dan kesehatan kerja dengan produktivitas yang ada pada PT.Epson sudah sangat cukup diterapkan dalam produktivitasnya	Perbedaan atau Novelty ada apa variabel E-wallet
8	(Soesanto et al al., 2023)	Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File dan Pengamanan Cyber pada Yayasan Siber Publisher	Pengamanan cyber berperan terhadap sistem manajemen sekuriti Yayasan Siber Publisher.	Perbedaan atau Novelty ada pada variabel keamanan pengguna
9	(Dewi et al., 2023)	Implementasi Manajemen Keamanan Untuk Meningkatkan Keselamatan Dan Kesehatan Kerja Dalam Rangka Meningkatkan Produktivitas Pada PT. Tera Data Indonusa Tbk	Implementasi Kesehatan dan Keselamatan Kerja (K3) memiliki signifikansi yang tinggi dan dianggap sebagai standar yang harus dipenuhi di lingkungan kerja untuk meningkatkan efisiensi proses kerja dan mengurangi sebanyak mungkin faktor risiko pada semua tahap produksi.	Perbedaan atau Novelty ada pada E-wallet
10	(Ipungkarti, 2023)	Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta	Berdasarkan hasil penelitian dan survey yang telah dilakukan selama 8 hari, didapatkan sebuah hasil yang selaras yang dimana hal tersebut ditunjukkan dari sebuah hasil data Primer mengenai tes pengetahaun para pegawai BPJS Ketenagakerjaan yang menunjukkan hasil cukup bagus untuk pengetahuan para tentang IT Security Awarenes..	Perbedaan atau Novelty ada pada variabel E-wallet
11	(Fachrudin et al., 2024)	Peranan Penting Manajemen Sekuriti di Era Digitalisasi	Hasil penelitian menunjukkan bahwa Di era digitalisasi yang kini tengah berlangsung, manajemen keamanan telah menjadi suatu kebutuhan yang sangat penting bagi perusahaan dan organisasi	Perbedaan atau Novelty ada pada variabel keamanan pengguna

12 (Soesanto, Masyruroh, et al., 2023)	Peranan Manajemen Sekuriti Dalam Mengamankan Dan Memecahkan Masalah PT SK Keris Indonesia	Hasil penelitian ini menemukan bahwa Sistem keamanan di PT SK Keris Indonesia masih belum terkoordinasi dengan baik karena kurangnya pemahaman tentang tugas dan tanggung jawab yang ada di antara kepolisian, petugas Satuan Pengamanan, dan masyarakat sekitar	Perbedaan atau Novelty yang ada pada E-wallet
13 (Islami, 2017)	Tantangan Dalam Imlementasi Strategi Keamanan Siber Nasional Indonesia Ditinjaudari Penilaian Global Cybersecurity Index	Hasilnya menunjukkan terdapat kesenjangan yang signifikan antara negara-negara dalam hal kesadaran, pemahaman, pengetahuan dan kapasitas untuk menerapkan strategi, kapabilitas dan program yang tepat untuk memastikan penggunaan TIK yang aman dan tepat sebagai pendorong pengembangan ekonomi.	Perbedaan atau Novelty ada apa variabel keamanan pengguna
14 (Khunaini et al., 2023)	Mengoptimalkan Sistem Keamanan pada Industri Penerbangan dengan Konsep Dasar Manajemen Sekuriti	Hasil dari penelitian ini menjelaskan pengoptimalan sistem keamanan pada industri penerbangan dapat dilakukan dengan mengidentifikasi ancaman keamanan yang mungkin terjadi, mengevaluasi risiko keamanan, menetapkan strategi manajemen sekuriti	Perbedaan atau Novelty ada pada variabel E-wallet
15 (Putra et al., 2023) Harniati Arfan, 2021)	Pentingnya Manajemen Security di Era Digitalisasi	Manajemen keamanan menjadi suatu kebutuhan yang sangat penting bagi perusahaan atau organisasi di era digitalisasi saat ini..	Perbedaan atau Novelty ada pada Keamanan pengguna

METODE PENELITIAN

Penelitian ini melakukan tinjauan terhadap literatur yang relevan untuk memahami kerentanan keamanan pada transaksi e-wallet dan berbagai strategi manajemen sekuriti yang telah diusulkan atau diterapkan sebelumnya.Dengan cara mengumpulkan data studi kasus dari pengguna transaksi e-wallet yang telah mengalami serangan atau penipuan sebelumnya untuk memahami modus operandi yang umum digunakan oleh penyerang untuk menganalisis kasus-kasus keamanan yang sukses dan tidak berhasil dalam implementasi manajemen sekuriti pada transaksi e-wallet. Menggunakan teknik analisis kualitatif untuk mendapatkan pemahaman yang komprehensif tentang isu-isu tersebut.

HASIL DAN PEMBAHASAN

Bentuk Penerapan Manajemen Sekuriti Guna Meningkatkan Keamanan Penggunaan E-wallet

Tujuan keamanan data adalah untuk menjaga kelangsungan bisnis dan mengurangi hilangnya nilai bisnis dengan membatasi dampak insiden keamanan(L. A. Saputra et al., 2023) Penerapan manajemen sekuriti dalam konteks penggunaan e-wallet adalah krusial untuk memastikan perlindungan yang optimal terhadap informasi dan dana pengguna. Berikut adalah beberapa bentuk penerapan manajemen sekuriti yang dapat meningkatkan keamanan penggunaan e-wallet:

1) Enkripsi Data: Mengenkripsi data sensitif seperti informasi kartu kredit, nomor rekening bank, dan kata sandi pengguna saat disimpan dan ditransmisikan melalui jaringan.

2) Otentikasi Multi-Faktor: Memastikan bahwa setiap transaksi atau akses ke akun e-wallet memerlukan lebih dari satu metode otentikasi, seperti kata sandi, kode verifikasi melalui SMS atau email, atau bahkan biometrik seperti sidik jari atau pengenalan wajah.
3) Pemantauan Transaksi: Mengimplementasikan sistem pemantauan transaksi yang canggih untuk mendeteksi aktivitas yang mencurigakan atau tidak biasa yang dapat mengindikasikan adanya akses ilegal atau penipuan.
4) Pembaruan Keamanan Reguler: Memastikan bahwa platform e-wallet terus-menerus diperbarui dengan patch keamanan terbaru untuk mengatasi kerentanan baru yang ditemukan.
5) Proteksi dari Serangan Siber: Melindungi sistem e-wallet dari berbagai jenis serangan siber seperti serangan phishing, serangan malware, dan serangan DDoS (Denial of Service) dengan menggunakan teknologi keamanan yang tepat.

Dengan menerapkan langkah-langkah ini secara efektif, penyedia layanan e-wallet dapat memastikan bahwa informasi dan dana pengguna tetap aman dan terlindungi dari ancaman keamanan yang ada dan baru. Ini membantu membangun kepercayaan pengguna dan menjaga reputasi platform e-wallet tersebut.

Peran Penting Manajemen Sekuriti Terhadap Keamanan Pengguna E-wallet

Manajemen sekuriti memiliki tanggung jawab utama dalam menjaga keamanan informasi sensitif pengguna, seperti nomor kartu kredit dan data pribadi lainnya. Preferensi menjadi hal penting dilakukan perusahaan-perusahaan e-wallet untuk mengetahui bagaimana atribut- atribut yang sesuai dengan kriteria atau pilihan yang paling diminati oleh para pengguna e-wallet(Perkasa & Setiawati, 2020). Mereka melakukan hal ini dengan menerapkan teknologi enkripsi dan tokenisasi untuk mengamankan data tersebut dari akses yang tidak sah. Selain itu, dengan menggunakan teknik autentikasi multi-faktor dan melalui pemantauan transaksi yang canggih, manajemen sekuriti dapat aktif dalam mencegah penipuan dan aktivitas mencurigakan lainnya yang dapat merugikan pengguna. Tim manajemen sekuriti juga harus siap dan responsif dalam mendeteksi serta menanggapi kejadian keamanan yang terjadi dengan cepat dan efisien, dengan tujuan utama untuk meminimalkan kerugian yang mungkin dialami oleh pengguna e-wallet.

Pengaruh Dari Manajemen Sekuriti Terhadap Keamanan Pengguna E-wallet

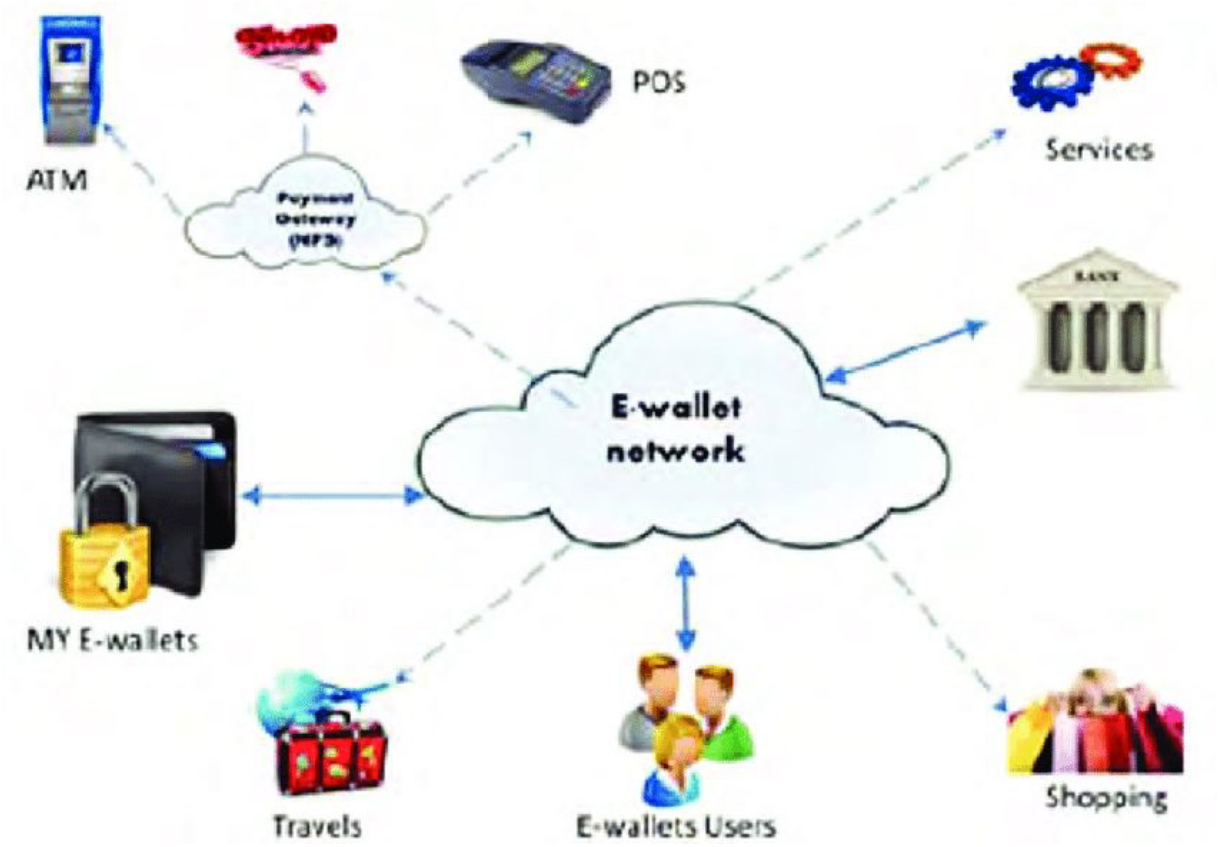
Penggunaan e-wallet atau dompet digital semakin populer dalam masyarakat modern karena kemudahan dan kenyamanannya dalam melakukan transaksi keuangan secara digital. Manajemen sekuriti, atau pengelolaan keamanan informasi, memainkan peran penting dalam menjaga keamanan pengguna e-wallet. Berikut adalah pengaruh manajemen sekuriti terhadap keamanan pengguna e-wallet:

1) Perlindungan Data Pengguna: Manajemen sekuriti bertanggung jawab untuk melindungi data sensitif pengguna e-wallet, seperti informasi pribadi, nomor kartu kredit, dan detail transaksi. Sistem keamanan yang kuat, termasuk enkripsi data, penggunaan sertifikat digital, dan pemantauan transaksi yang mencurigakan, sangat penting untuk mencegah akses tidak sah terhadap informasi pengguna.
2) Keamanan Transaksi: E-wallet menyimpan informasi keuangan pengguna dan memfasilitasi transaksi online dan offline. Manajemen sekuriti harus memastikan bahwa setiap transaksi dilakukan melalui kanal yang aman dan terotentikasi. Langkah-langkah seperti otentikasi dua faktor, penggunaan token keamanan, dan deteksi fraud secara real-time membantu mengurangi risiko transaksi yang tidak sah.
3) Pencegahan Terhadap Serangan Cyber: E-wallet rentan terhadap berbagai jenis serangan cyber, termasuk serangan malware, phishing, dan serangan DDoS (Distributed Denial of Service). Manajemen sekuriti harus terus memperbarui sistem keamanan untuk mengatasi

ancaman tersebut. Pelatihan keamanan bagi pengguna e-wallet juga penting untuk meningkatkan kesadaran mereka terhadap praktik-praktik keamanan digital yang aman.

4) Pengelolaan Risiko Keamanan: Manajemen sekuriti bertanggung jawab untuk mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan yang terkait dengan penggunaan e-wallet. Hal ini mencakup pemantauan sistem secara berkala, pembaruan perangkat lunak keamanan, serta melakukan audit keamanan secara rutin untuk mengidentifikasi celah atau kerentanan yang mungkin ada dalam sistem.

Kerangka Konseptual



Sumber:Gambar riset

Gambar 1. Kerangka Konseptual

KESIMPULAN DAN SARAN

Menerapkan langkah-langkah manajemen sekuriti, keamanan pengguna pada transaksi e-wallet dapat ditingkatkan secara signifikan. Langkah-langkah ini akan membantu melindungi informasi sensitif pengguna dan mencegah akses ilegal atau penipuan. Dengan demikian, pemahaman dan implementasi manajemen sekuriti yang efektif sangat penting dalam menjaga kepercayaan pengguna terhadap e-wallet dan transaksi mereka.

Penerapan manajemen sekuriti dalam transaksi e-wallet memiliki peran vital dalam meningkatkan keamanan pengguna. Dengan mengadopsi praktik-praktik terbaik dalam manajemen risiko, enkripsi data, otentikasi ganda, dan pemantauan transaksi secara real-time, platform e-wallet dapat meminimalkan risiko keamanan yang dihadapi pengguna. Selain itu, penyedia layanan e-wallet harus terus memperbarui sistem keamanan mereka sesuai dengan perkembangan teknologi dan ancaman keamanan terbaru. Dengan demikian, pengguna dapat

lebih percaya diri dalam melakukan transaksi elektronik tanpa khawatir akan kebocoran data atau penipuan.

DAFTAR PUSTAKA

Bakri, M., & Irmayana, N. (2017). *ANALISIS DAN PENERAPAN SISTEM MANAJEMEN KEAMANAN INFORMASI SIMHP BPKP MENGGUNAKAN STANDAR ISO 27001*.

Dewi, A. N., Fitriyani, L., Rindiati, N. E., & Sinlae, F. (2023). Implementasi Manajemen Keamanan Untuk Meningkatkan Keselamatan Dan Kesehatan Kerja Dalam Rangka Meningkatkan Produktivitas Pada PT. Tera Data Indonusa Tbk. *Nusantara Journal of Multidisciplinary Science*, *1*(5). https://jurnal.intekom.id/index.php/njms

Dirnaeni, D., Handrijaningsih, L., Mariani, S., & Anisah. (2021). *PERSEPSI KEMUDAHAN, CUSTOMER RELATIONSHIP MANAGEMENT DAN KUALITAS LAYANAN TERHADAP LOYALITAS PELANGGAN E-WALLET MELALUI KEPUASAN*.

Fachrudin, R., Respaty, E., Adilah, I. S., & Sinlae, F. (2024). Peranan Penting Manajemen Sekuriti di Era Digitalisasi. *Nusantara Journal of Multidisciplinary Science*, *2*(1). https://jurnal.intekom.id/index.php/njms

Fauzi, A., Ashila Salwa, S., Safitri, A., Amelia, E., Julianti, C., & Fazriyah, S. N. (2023). *ANALISIS PENGARUH PENGGUNAAN SISTEM PEMBAYARAN DIGITAL DAN DIGITAL MARKETING TERHADAP KEPUTUSAN PEMBELIAN* (Vol. 2, Issue 1).

Fitria, A. R., Soesanto, E., Uguy, F. C. A., & Sinaga, Z. V. (2023). Manajemen Sekuriti Terintegrasi di PT. Unilever Indonesia Tbk: Ancaman, Manajemen Risiko, Standar Keamanan, dengan Fokus pada SSMKD. *IJM: Indonesian Journal of Multidisciplinary*, *1*. https://journal.csspublishing/index.php/ijm

Ipungkarti, A. A. (2023). Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta. *Jurnal Media Infotama*, *19*(1), 103.

Islami, M. J. (2017). *TANTANGAN DALAM IMPLEMENTASI STRATEGI KEAMANAN SIBER NASIONAL INDONESIA DITINJAU DARI PENILAIAN GLOBAL CYBERSECURITY INDEX*.

Khunaini, A., Fauzi, A., Jumawan, J., Dns, A. S. R., Raya, C. S., Sukma, V. A., & Meliawati, W. (2023). *Mengoptimalkan Sistem Keamanan pada Industri Penerbangan dengan Konsep Dasar Manajemen Sekuriti*. *2*(1), 2829–4599. https://doi.org/10.38035/jim.v2i1

Susanti, N. L. P. R., & Putra, I. M. P. D. (2023). *PENGARUH PERSEPSI KEMUDAHAN, KUALITAS LAYANAN, DAN RISIKO KEAMANAN TERHADAP KEPUTUSAN PENGGUNAAN E-WALLET DALAM TRANSAKSI KEUANGAN*. *12*(03), 407–420. https://ojs.unud.ac.id/index.php/EEB/

Marhaendra, A. N., & Mahyuzar, H. M. (2023). *ANALISIS PENGARUH PERSEPSI KEMUDAHAN DAN PERSEPSI KEAMANAN TERHADAP KEPUASAN PADA PENGGUNA E-WALLET DANA DI KEBUMEN*.

Miftahurrizqi, Windiarti, I. S., & Prabowo, A. (2021). *ANALISIS KEAMANAN SISTEM PADA SISTEM INFORMASI AKADEMIK MENGGUNAKAN COBIT 5 FRAMEWORK PADA SUB DOMAIN DSS05*.

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)*. https://doi.org/10.31933/jimt.v4i5

Oktavira, A. C., Soesanto, E., Pramesti, R. K., Fathna, S. Z., Bhayangkara, U., & Raya, J. (2023). Penerapan Manajemen Sekuriti Melalui Keamanan Industrial PT Wings Surya. *IJM: Indonesian Journal of Multidisciplinary*, *1*. https://journal.csspublishing/index.php/ijm

Perkasa, H. R., & Setiawati, C. I. (2020). *ANALISIS PREFERENSI KONSUMEN DALAM MEMILIH ELECTRONIC WALLET (E-WALLET) DI KOTA BANDUNG*. *7*(2), 3536.

Purba, M., Samsir, & Arifin, K. (2020). *PENGARUH PERSEPSI KEMUDAHAN PENGGUNAAN, PERSEPSI MANFAAT DAN KEPERCAYAAN TERHADAP KEPUASAN DAN NIAT MENGGUNAKAN KEMBALI APLIKASI OVO PADA MAHASISWA PASCASARJANA UNIVERSITAS RIAU*.

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.v2i1

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

Saputra, F., Soesanto, E., Indah Cahyaningtyas, K., & Lukmanul Hakim, Z. (2024). Penerapan Manajemen Security Terhadap Cyber Crime di Kominfo. *IJM: Indonesian Journal of Multidisciplinary*, *2*. https://journal.csspublishing/index.php/ijm

Saputra, L. A., Akbar, F. M., Cahyaningtias, F., Ningrum, M. P., & Fauzi, A. (2023). *Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan*. https://doi.org/10.38035/jpsn.v1i12

Sari, M. A., Listiawati, R., Novitasari, & Vidyasari, R. (2020). ANALISA PENGARUH DAYA TARIK PROMOSI, PERSEPSI KEMUDAHAN, PERSEPSI MANFAAT, PERSEPSI KEAMANAN TERHADAP MINAT PENGGUNAAN E-WALLET. *Ekonomi & Bisnis*, *18*(2), 85–96. https://doi.org/10.32722/eb.v18i2.1992

Soesanto, E., Masyruroh, A. J., Putri, G. A. M., & Maharani, S. P. (2023). Peranan Manajemen Sekuriti Dalam Mengamankan Dan Memecahkan Masalah PT SK Keris Indonesia. *Jurnal Manajemen Riset Inovasi*, *1*(3), 46–57. https://doi.org/10.55606/mri.v1i3.1259

Soesanto, E., Saputra, F., Puspitasari, D., & Putra Danaya, B. (2023). *Determinasi Sistem Manajemen Sekuriti: Analisis Objek Vital, Pengamanan File dan Pengamanan Cyber pada Yayasan Siber Publisher*. *2*(1). https://doi.org/10.38035/jim.v2i1

Susanto, E., Damayanti, V., Samuel, I., & Bramley, H. (2023). *Penerapan Keselamatan Kerja dan Kesehatan Kerja Melalui Manajemen Sekuriti Terhadap Produkivitas Pada PT. Epson*.

Wijaya, C. P., Soesanto, E., Aulia, F., Aisy, H. R., & Auliya, I. (2023). Implementasi Manajemen Sekuriti PT. KAI: K3, Manajemen Risiko, dan Standar Keamanan pada Perlintasan Kereta Api. In *IJM: Indonesian Journal of Multidisciplinary* (Vol. 1). https://journal.csspublishing/index.php/ijm