E-journal Field of Economics, Business, and Entrepreneurship (EFEBE)

PENIPUAN KOMPUTER PADA SISTEM INFORMASI AKUNTANSI: TANTANGAN KEAMANAN DI PERUSAHAAN BERBASIS TEKNOLOGI

Dargio Akbari Sutanto[1], Shafiq Hamam Adingga[2], Fahri Reza Ramadhan[3], Tegar Ryamizard[4]

[12345] Universitas Lampung
sutantodargio@gmail.com, [2] shafiqhamama21@gmail.com, [3] fahrirezaramadhan1@gmail.com, tegaryamiz@gmail.com

Informasi Naskah

Update Naskah:

Dikumpulkan: 10 November 2025
Diterima: 12 November 2025
Terbit/Dicetak: 13 November 2025

Keywords:

Accounting Information Systems, Computer Fraud, Cybersecurity, Internal Controls.

Abstract

This article discusses the security issues faced by technology-driven businesses in the field of Accounting Information Systems (AIS). The use of AIS in the digital age helps companies manage financial data more effectively, but it also brings risks, such as cybersecurity threats and computer fraud. This study, conducted using a qualitative method in the form of a literature review, aims to identify the types of computer fraud that commonly occur in AIS and the challenges companies face in preventing them. Additionally, this paper provides strategic recommendations for enhancing AIS security, including implementing the latest security technologies, strengthening internal controls, and educating employees about cybersecurity threats. By implementing these measures, it is hoped that businesses can reduce their risk of fraud and maintain the accuracy of their financial data.

A. PENDAHULUAN

Sistem Informasi Akuntansi sangat penting bagi bisnis yang mengandalkan teknologi. Sistem Informasi Akuntansi mendukung operasi akuntansi organisasi dengan mencapai tujuan utamanya, yang meliputi peningkatan keterampilan pengambilan keputusan, menurunkan biaya produksi dan meningkatkan kualitas barang dan jasa yang diproduksi, serta meningkatkan efisiensi kinerja bisnis secara keseluruhan (Sari & Hwihanus, 2023). Selain itu, Sistem Informasi Akuntansi menawarkan pengelolaan data keuangan yang lebih efektif, mendukung pengambilan keputusan yang tepat, memberi informasi relevan dan akurat, serta menjamin keamanan data keuangan melalui pengaturan kontrol akses yang tepat (Fakultas Sains dan Teknologi Universitas Airlangga, 2024).

Keamanan dalam SIA menjadi tantangan utama karena sistem ini menyimpan data keuangan yang sangat sensitif dan bersifat krusial dalam pengambilan keputusan bisnis. Ancaman seperti peretasan (*hacking*), pencurian data, dan manipulasi catatan keuangan dapat merusak integritas

* *Corresponding Author.*
Dargio Akbari Sutanto, e-mail : sutantodargio@gmail.com

DOI 10.23960/efebe.v3i1.316

keakuratan, dan kerahasiaan informasi perusahaan. Selain itu, dengan perkembangan teknologi yang cepat, metode serangan juga berevolusi, memaksa perusahaan terus memperbarui strategi keamanan mereka untuk melindungi SIA dari risiko internal dan eksternal yang sifatnya merugikan.

Kasus penipuan komputer yang terkait dengan SIA terus meningkat seiring dengan cepatnya digitalisasi dan penggunaan teknologi di perusahaan. Penjahat siber (*cyber criminals*) makin ahli dalam memanfaatkan kelemahan sistem lewat berbagai cara. Kasus seperti pemalsuan laporan keuangan atau rekayasa transaksi semakin sering terjadi, menyebabkan kerugian finansial yang signifikan dan menurunkan kepercayaan pemangku kepentingan. Oleh karena itu, keamanan SIA menjadi prioritas penting untuk mengantisipasi risiko-risiko tersebut.

B. TINJAUAN PUSTAKA

1. Sistem Informasi Akuntansi

Sri Mulyani (2021) mendefinisikan sistem informasi akuntansi sebagai sekelompok instrumen yang dimaksudkan untuk mengubah data termasuk data keuangan menjadi pengetahuan. Sistem informasi akuntansi yang mendukung pengambilan keputusan memungkinkan pihak yang berkepentingan menggunakan informasi yang dihasilkan untuk berbagai tujuan.

Sementara itu, Laudon & Laudon dalam Lestari (2020) mendefinisikan sistem informasi akuntansi sebagai sekelompok bagian terhubung yang bekerja sama untuk mengumpulkan, memproses, menyimpan, dan mendistribusikan data untuk mendukung prosedur pengambilan keputusan dan pemantauan organisasi.

Sistem informasi manajemen mencakup sistem informasi akuntansi sebagai subsistemnya. Sistem informasi manajemen bertugas mengelola data transaksi dari seluruh aktivitas transaksi yang ada pada suatu waktu tertentu, yang membedakan kedua sistem tersebut satu sama lain. Sistem informasi untuk manajemen secara umum. Seluruh data organisasi baik finansial maupun non finansial dapat dikelola dalam sistem ini untuk menghasilkan informasi bagi suatu bisnis yang selanjutnya akan membantu dalam pengambilan keputusan. Sebaliknya, sistem informasi akuntansi lebih berkonsentrasi pada data yang berkaitan dengan aktivitas transaksi keuangan.

Untuk mendukung operasi bisnis, sistem informasi akuntansi melakukan enam tugas penting. Data tentang transaksi keuangan pertama kali dikumpulkan dan disimpan oleh sistem ini. Setelah dikumpulkan, data diproses untuk memberikan informasi kepada manajemen untuk perencanaan dan pengendalian perusahaan. Untuk lebih memastikan akuntabilitas dan transparansi, sistem ini mengelola semua operasi keuangan dan melakukan kontrol atas aset bisnis. Oleh karena itu, sistem informasi akuntansi meningkatkan kinerja keuangan dalam hal efisiensi biaya dan waktu. Teknologi ini juga memudahkan pemangku kepentingan dalam mengambil keputusan yang tepat dengan menyajikan fakta keuangan secara tepat dan metodis.

2. **Penipuan Komputer (Computer Fraud)**

Kecurangan akuntansi menurut Association of Certified Fraud Examiners adalah suatu bentuk kecurangan yang diketahui oleh individua atau entitas bahwa dampak dari kecurangan tersrbut dapat memberikan kerugian bagi orang lain. Kecurangan akuntansi sering terjadi dan dapat menimbulkan kerugian yang cukup signifikan di hamper semua sector. Keterlibatan pihak internal merupakan alasan yang sering terhadi. Penipu dinilai cukup pinter dalam menbobol informasi-informasi penting perusahaan tanpa sepengetahuan perusahaan, terlebih jika keadaan perusahan tersebut lebih kompleks.

Penipuan komputer didefinisikan sebagai strategi atau tindakan yang dipikirkan oleh seseorang yang menggunakan komputer untuk mencoba berbohong, menipu, atau mengejutkan orang lain, atau menjadi licik, tidak jujur, atau melakukan tindakan tidak adil lainnya untuk mendapatkan keuntungan yang tidak adil. atas mereka Wilkinson & Cerullo dalam Mutia (2020).

Kehadiran sistem informasi akuntansi merupakan angin segar bagi perusahaan dalam mengatasi fenomena fraud. Melalui suatu sistem yang modern bernama sistem informasi akuntansi inilah fraud dapat terdeteksi ditambah dengan kegiatan pengendaliaan internal. Dapat disimpulkan bahwa, penggunaan sisem infromasi akuntansi ini dapat mengurangi fraud pada sebuah perusahaan.

C. METODOLOGI PENELITIAN

Metode penelitian yang digunakan dalam artikel ini adalah metode kualitatif dengan pendekatan *literature review*. Dengan metode penelitian ini, referensi dikumpulkan dari berbagai publikasi, antara lain buku, jurnal, dan artikel ilmiah yang relevan dengan pokok bahasan. Pencarian referensi dilakukan dengan menggunakan kata kunci tertentu untuk memastikan sumber-sumber yang diperoleh tepat dan sesuai. Setelah pengumpulan referensi dilakukan analisis mendalam terhadap masing-masing sumber untuk memperoleh pemahaman yang lebih mendalam mengenai pokok bahasan. Hasil analisis ini
kemudian digunakan untuk menyusun argumen dan kesimpulan yang kuat, memungkinkan kajian teoritis yang lengkap dan berdasarkan literatur yang sudah ada.

D. HASIL DAN PEMBAHASAN

1. Identifikasi Bentuk Penipuan Komputer dalam Sistem Informasi Akuntansi

Rachmad dan Barbara (2019) menjelaskan bahwa ada pula Processing Fraud yang dimana ini merupakan tindakan-tindakan yang menyalahgunakan sistem yang bertujuan untuk melanggar hukum, seperti tindakan-tindakan yang menghabiskan waktu kerja untuk keperluan pribadi. Hal ini dapat dicapai dengan cara melakukan beragam rangkaian aktivitas-aktivitas tertentu selama berjalannya jam kerja ataupun dengan membuat catatan palsu ataupun menjadi alibi. Kemudian juga ada Data Fraud, yang dimana tindakan-tindakan ini merupakan yang menekankan kepada penggunaan dan juga akses yang tidak diizinkannya, yang dimana ini dapat mencakup pencurian data-data. Seperti misalnya saja, seorang peretas data-data pribadi maupun data-data penting (*hacker*) dapat saja melakukan penyerangan terhadap perusahaan yang telah lama dan juga direncanakan untuk diretasnya. Tahap selanjutnya adalah Output Fraud, yang dimana ini teridentifikasi sebagai penipuan yang melibatkan hasil yang berfokus kepada keluaran sistem, seperti halnya tindakan untuk pemalsuan cek. Hal ini biasanya dilakukuan dengan tujuan agar transaksi yang bersifat fiktif agar tampak nyata dan juga valid.

(W. G. Kruse & J. G. Heiser, 2001, sebagaimana dikutip dalam Hidayatullah, 2023) menjelaskan Untuk mempengaruhi opini publik, serangan semantik memerlukan transmisi dan perubahan informasi yang akurat atau tidak akurat, baik melalui sarana teknologi atau cara manual. Sedangkan serangan siber adalah berbagai tindakan jahat yang dilakukan oleh suatu negara, organisasi, atau orang- orang dengan tujuan mencuri, mengubah, atau menghancurkan infrastruktur atau sistem komputer yang menjadi titik lemahnya. Jenis serangan ini dapat terjadi dalam berbagai bentuk, seperti worm Stuxnet, yang memasang spyware atau bahkan menghancurkan infrastruktur penting. Peretas juga dapat menggunakan pemerasan siber, yaitu mereka mengancam akan menggunakan serangan DoS atau DDoS terhadap perusahaan untuk mengambil uang. Dengan serangan yang ditargetkan terhadap negara-negara seperti Georgia dan Estonia, perang siber telah berkembang menjadi ancaman yang signifikan dalam skala global, yang menggarisbawahi pentingnya keamanan siber dalam konflik internasional.

2. Tantangan Keamanan yang Dihadapi Perusahaan Berbasis Teknologi

Perusahaan berbasis teknologi menghadapi berbagai tantangan dalam menjaga keamanan sistem mereka dari penipuan komputer. Salah satu tantangan utama adalah kompleksitas sistem yang terus meningkat, yang membuat sistem lebih rentan terhadap serangan *hacker* jika tidak dikelola dengan baik. Sistem yang tidak terjaga secara optimal menjadi target empuk bagi peretas yang ingin mengambil keuntungan seperti yang dijelaskan oleh Rachmad dan Barbara (2019). Selain itu, banyak perusahaan yang masih kekurangan pengendalian internal yang dapat mengidentifikasi dan menghentikan
penipuan, sehingga memberikan ruang bagi pihak dalam dan luar untuk melakukan aktivitas penipuan.

Tantangan lainnya adalah rendahnya kesadaran karyawan terhadap keamanan siber. Keteledoran dan kurangnya pengetahuan mengenai ancaman cybercrime dapat menjadi faktor utama dalam terjadinya penipuan komputer dan pencurian data di Perusahaan. Hal ini menjadi semakin penting karena karyawan sering kali memiliki akses ke data dan sistem yang dapat disalahgunakan jika tidak diawasi dengan baik. Kombinasi dari kompleksitas sistem, lemahnya pengendalian internal, dan rendahnya kesadaran keamanan siber menempatkan perusahaan pada risiko yang besar .

3. Upaya dan Strategi untuk Mengatasi Penipuan Komputer

Langkah awal yang penting dalam ancaman penipuan komputer adalah meningkatkan kesadaran dan pendidikan pengguna. Bisnis harus melatih karyawannya tentang cara mengenali indikator penipuan termasuk email phishing dan taktik rekayasa sosial. Penelitian mengungkapkan bahwa pencuri sering kali menggunakan teknik rekayasa sosial untuk mengelabui korban agar mengungkapkan informasi pribadi. Dengan meningkatkan kesadaran pengguna, risiko penipuan dapat dikurangi (Faradilla, 2023, sebagaimana dikutip dalam Ramalinda & Rachmat Raharja, 2024). Untuk mencegah penipuan, teknologi keamanan harus diterapkan dengan benar. Sistem dapat dibuat lebih tahan terhadap serangan dengan menggunakan sistem deteksi intrusi (IDS), firewall, dan perangkat lunak antivirus.

Menurut Bwerinofa-Petrozzello, R. (2023) untuk menghindari penyalahgunaan, pemisahan peran memastikan bahwa tidak ada satu individu pun yang memiliki wewenang penuh atas proses transaksi. Misalnya, penerima uang tunai bisa gagal mendokumentasikan atau merekonsiliasi transaksi tersebut. Organisasi juga harus menggunakan prinsip hak istimewa paling rendah ketika menerapkan kontrol akses, yang memungkinkan karyawan memiliki akses hanya terhadap apa yang mereka perlukan untuk menyelesaikan pekerjaan mereka.

Pengendalian fisik juga penting; anggota staf hanya diperbolehkan masuk ke lokasi yang diperlukan untuk pekerjaan mereka, termasuk ruang server. Untuk menjamin bahwa anggota staf memahami protokol dan menyelesaikan tugas sesuai standar, pelatihan dan pengujian rutin dilakukan. Pada akhirnya, bisnis terlindungi dari kehilangan data dan intrusi oleh firewall dan pencadangan rutin.

Menerapkan proses tanggap darurat sangat penting bagi setiap perusahaan yang menangani situasi penipuan. Protokol-protokol ini harus terdiri dari langkah-langkah metodis yang memfasilitasi deteksi cepat terhadap indikator-indikator penipuan, tindakan cepat untuk meminimalkan kerugian, dan rekonstruksi menyeluruh setelah suatu kejadian. Auditor internal dan konsultan hukum adalah contoh staf eksternal dan internal yang perlu dimiliki organisasi untuk mengelola situasi darurat. Untuk menjamin bahwa investigasi dilakukan secara menyeluruh dan tindakan hukum yang tepat dapat diambil terhadap penipu, protokol tanggap darurat juga perlu melibatkan pihak berwenang, seperti polisi atau organisasi penegak hukum lainnya. Teknologi pendeteksi penipuan juga dapat digunakan untuk lebih melindungi terhadap aktivitas yang meragukan dan menghentikan kerugian tambahan.

Perusahaan harus memprioritaskan bantuan kepada korban penipuan selain protokol tanggap darurat. Memberikan informasi dan dukungan yang cukup kepada korban penipuan sangatlah penting karena mereka sering kali mengalami dampak finansial dan psikologis yang serius. Perusahaan dapat membantu korban dengan mengedukasi masyarakat tentang tindakan pencegahan di masa depan, seperti mengamankan data pribadi secara lebih dekat dan menjaga privasi informasi keuangan. Selain itu, korban penipuan dapat memperoleh manfaat dari bantuan keuangan atau layanan terapi untuk membantu mereka mengatasi trauma yang mereka derita. Dengan menawarkan bantuan nyata kepada para korban, organisasi ini menjunjung tinggi kepercayaan publik atas dedikasinya dalam menjaga keselamatan dan kesejahteraan seluruh pemangku kepentingan, sekaligus menjaga mereknya. Hal ini menunjukkan rasa tanggung jawab sosial yang lebih luas sekaligus membina hubungan yang langgeng dengan para pemangku kepentingan.

E. SIMPULAN DAN SARAN

1. Kesimpulan

Sistem informasi akuntansi sangat penting untuk mengelola data keuangan bisnis, khususnya bisnis yang sangat bergantung pada teknologi. Sistem informasi akuntansi memfasilitasi penghematan biaya, meningkatkan efektivitas operasional, dan memberikan data yang tepat yang berkaitan dengan pengambilan keputusan. Di sisi lain, seiring dengan semakin luasnya penggunaan teknologi, risiko keamanan terhadap Sistem Informasi Akuntansi—seperti penipuan komputer—semakin meningkat. Serangan siber termasuk pemerasan siber dan serangan semantik, serta jenis penipuan seperti penipuan pemrosesan, data, dan keluaran, menimbulkan risiko besar yang dapat membahayakan kerahasiaan data perusahaan dan mengakibatkan kerugian finansial yang besar.

Perusahaan harus meningkatkan pengendalian internal, melatih anggota staf tentang bahaya dunia maya secara rutin, dan melakukan audit secara rutin untuk mencari penipuan guna menghindari ancaman tersebut. Elemen penting lainnya dalam menghentikan penipuan adalah menerapkan teknologi keamanan seperti firewall, enkripsi, dan sistem pemantauan waktu nyata. Selain itu, agar dapat bereaksi dengan cepat terhadap situasi penipuan dan melibatkan pihak internal dan eksternal terkait, perusahaan perlu memiliki proses tanggap darurat yang jelas. Bahaya penipuan komputer dapat dikurangi dengan serangkaian taktik yang tepat, menjaga kepercayaan dan keamanan sistem informasi akuntansi bisnis.

.

2. Saran

Berdasarkan hasil kajian dalam artikel ini, terdapat beberapa saran yang dapat diimplementasikan untuk meningkatkan efektivitas dan keamanan Sistem Informasi Akuntansi di perusahaan berbasis teknologi. Pertama, dunia usaha harus terus meningkatkan langkah-langkah keamanan mereka, yang harus mencakup pembaruan perangkat lunak sesering mungkin, memperkuat firewall, menggunakan enkripsi, dan menyiapkan sistem pemantauan real-time untuk mengidentifikasi aktivitas mencurigakan. Untuk mengidentifikasi ancaman tersebut sebelum menimbulkan kerugian yang signifikan, sangat disarankan untuk menerapkan teknologi deteksi penipuan, seperti Intrusion Detection Systems (IDS).

Kedua, perusahaan harus terus mendidik stafnya tentang kesadaran keamanan siber. Mendapatkan pelatihan yang memadai tentang cara mencegah serangan seperti phishing dan rekayasa sosial sangatlah penting, mengingat banyaknya risiko yang mungkin timbul akibat kecerobohan manusia. Selain itu, untuk mengurangi risiko penipuan internal, dunia usaha mendesak untuk meningkatkan pengendalian internal, seperti pemisahan pekerjaan dan membatasi akses hanya pada karyawan yang memerlukannya. Untuk menjamin keamanan dan integritas data di SIA, audit internal dan eksternal secara berkala juga harus dilakukan. Dunia usaha dapat lebih menjaga data keuangan mereka dan menurunkan risiko kejahatan komputer dengan mengambil tindakan pencegahan ini.

DAFTAR PUSTAKA

Amartha, T. B. (2024, Juni 10). E-Wallet Adalah Dompet Digital : Pahami Manfaat,Kelebihan dan Kekurangannya. Diambil kembali dari amartha.com: https://amartha.com/blog/pendana/money-plus/e-wallet-adalah-dompet-digital/

DANA. (2023, Desember 7). Apakah DANA Aman Tanpa Pengawasan OJK? Diambil kembali dari www.dana.id: https://www.dana.id/corporate/newsroom/apakah-dana-aman-tanpa-pengawasan-ojk

Farhan, M. (2024). *Analisis Penggunaan E-Wallet Terhadap Mahasiswa Universitas Islam Sumatera Utara Tahun 2022* (Doctoral dissertation, Fakultas Ekonomi, Universitas Islam Sumatera Utara).

Gopay. (2023, September 5). Cara Lengkap Menggunakan Dompet Digital dan Manfaatnya. Diambil kembali dari gopay.co.id: https://gopay.co.id/blog/dompet-digital

Insana, D. R. M., & Johan, R. S. (2021). Analisis Pengaruh Penggunaan Uang Elektronik Terhadap Perilaku Konsumtif Mahasiswa Pendidikan Ekonomi Universitas Indraprasta PGRI. JABE (Journal of Applied Business and Economic), 7(2), 209-224

Laela Nur Jannah, & Supanji Setyawan. (2022). DAMPAK PANDEMI COVID-19 TERHADAP PENGGUNAAN DOMPET DIGITAL DI INDONESIA. JOEL: Journal of Educational and Language Research, 1(7), 709–716. https:v//doi.org/10.53625/joel.v1i7.1463

Marcomm. (2024, Juni 29). Mengenal E-Wallet, Manfaat, Dan Cara Kerjanya. Diambil kembali dari hasamitra.com: https://hasamitra.com/artikel/mengenal-e-wallet-manfaat-dan-cara-kerjanya

Midtrans. (t.thn.). E-wallet: Pengertian, Cara Kerja, Manfaat dan Contohnya. Diambil kembali dari midtrans.com: https://midtrans.com/id/blog/e-wallet

Nugraha, S. L., & Fauzia, I. Y. (2021). Peran e-wallet dalam penghimpunan zakat, infak, dan sedekah (Studi kasus pada ovo, go-pay, dana, dan link-aja). Journal of Business and Banking, 11(1), 113-127.

PayDo. (2024, April 22). Digital Wallets: Advantages and Disadvantages to Consider. Diambil kembali dari www.linkedin.com: https://www.linkedin.com/pulse/digital-wallets-advantages-disadvantages-consider-paydo-idfgf

Rania, D. (2024, April 5). Survei Dompet Digital Paling Favorit di Indonesia [2024]. Diambil kembali dari jubelio.com: https://jubelio.com/hasil-survei-dompet-digital-paling-favorit-di-indonesia/

Rohmah, F. (2018). Perkembangan Uang Elektronik pada Perdagangan di Indonesia. Jurnal Bisnis dan Manajemen Islam, 6(1), 1-19.

Romadhona., S. (2024, Maret 24). Keberadaan E-wallet, Ini 10 Kelebihan dan Kekurangannya Menurut Riset. Diambil kembali dari umsida.ac.id: https://umsida.ac.id/10-kelebihan-dan-kekurangan-e-wallet-menurut-riset/

Sihombing, J. (2024, Juni 30). Kelebihan dan Kekurangan Tren Dompet Digital. Diambil kembali dari www.rri.co.id: https://www.rri.co.id/lain-lain/791614/kelebihan-dan-kekurangan-penggunaan-tren-dompet-digital

Silalahi, P. R., Safira, R., Hubara, Z. A., & Sari, E. P. (2022). Pengaruh Dompet Digital Terhadap Budaya Belanja Individu di Kota Medan. EKOMBIS REVIEW: Jurnal Ilmiah Ekonomi Dan Bisnis, 10(2), 869-878.

Situmorang, M. K. (2021). Pengaruh Perilaku Konsumen Terhadap Penggunaan Uang Elektronik (Dompet Digital) Sebagai Alat Pembayaran Pada Masa Pandemi Covid–19 di Kota Medan. Maneggio: Jurnal Ilmiah Magister Manajemen, 4(1), 123-130.

Sulistyowati, R., Paais, L., & Rina, R. (2020). Persepsi konsumen terhadap penggunaan dompet digital. ISOQUANT: Jurnal Ekonomi, Manajemen dan Akuntansi, 4(1), 17-34.

Syariah, B. M. (2024, Juli 22). Apa Itu E-wallet? Ini Manfaat dan Cara Menggunakannya. Diambil kembali dari www.megasyariah.co.id: https://www.megasyariah.co.id/id/artikel/edukasi-tips/digital-banking/e-wallet-adalah

Tanjung, A., Tobing, C. T. L., Ar, N. A., & Pane, S. G. (2024). Analisis Sistem Pembayaran Menggunakan Dompet Digital. INTECOMS: Journal of Information Technology and Computer Science, 7(1),

282-289.
Verihubs. (2022, September 13). Kenali Jenis-Jenis Dompet Digital yang Populer di Indonesia. Diambil kembali dari verihubs.com: https://verihubs.com/blog/dompet-digital.