Prosiding Seminar Nasional Teknologi dan Sistem Informasi (SITASI) 2026
Surabaya, 3 Juni 2026

Integrasi *Security Awareness* dan *Cyber Defense Automation* dalam Meminimalisir *Financial Fraud* pada Sektor UMKM

Slamet[1*], Diana Putri[2]
*E-mail: slamet@dinamika.ac.id

[1]S1 Sistem Informasi, Fakultas Teknologi dan Informatika, Universitas Dinamika
[2]S1 Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Dinamika

Abstrak

Usaha Mikro, Kecil, dan Menengah (UMKM) semakin rentan terhadap penipuan keuangan akibat digitalisasi yang cepat dan infrastruktur keamanan yang terbatas. Studi ini mengeksplorasi sinergi antara kewaspadaan manusia dan sistem pertahanan siber otomatis sebagai mekanisme perlindungan untuk menjaga integritas akuntansi pada sektor UMKM. Penelitian ini menggunakan pendekatan metode campuran (*mixed-methods*). Secara kuantitatif, data survei dianalisis dari 100 UMKM mengenai frekuensi serangan siber dan efektivitas perangkat lunak akuntansi yang digunakan saat ini. Secara kualitatif, wawancara mendalam dilakukan kepada pakar keamanan siber dan akuntan forensik untuk memahami perilaku dari "ancaman orang dalam" *(insider threats)* dan "rekayasa sosial" (*social engineering*) dalam lingkungan keuangan skala kecil. Secara kuantitatif menunjukkan bahwa UMKM yang menggunakan *Intrusion Detection System* otomatis (IDS) yang dikombinasikan dengan deteksi anomali berbasis AI pada buku besar yang berhasil mengurangi waktu deteksi penipuan sebesar 40%. Namun, data kualitatif mengungkapkan celah kritis pada aspek kesalahan manusia *(human error)*. Meskipun telah menggunakan sistem yang canggih, 65% pelanggaran keamanan terjadi karena pola pemilihan kata sandi yang buruk atau kurangnya skeptisisme terhadap *email phishing*. Selain itu, paper ini juga menjelaskan hasil integrasi terkait kewaspadaan manusia melalui pelatihan rutin dan budaya "*Security Awareness*" akuntansi dengan pertahanan otomatis menciptakan kerangka kerja "*Human in the Loop*" (HITL). Pada paper ini juga mengkaji terkait bagaimana cara untuk melakukan otomasi dalam menangani pemindaian data bervolume tinggi, sementara pada aspek intuisi manusia mengidentifikasi ketidaksesuaian yang terlewatkan oleh algoritma.

Kata kunci**:** *UMKM, Kecurangan Keuangan, Keamanan Siber, Integritas Akuntansi*

Abstract

Micro, Small, and Medium Enterprises (MSMEs) have become increasingly vulnerable to financial fraud due to rapid digitalization and limited security infrastructure. This study explores the synergy between human vigilance and automated cyber defense systems as a protective mechanism to safeguard accounting integrity within the MSME sector through a mixed-methods approach. Based on quantitative approach, survey data from 100 MSMEs were analyzed regarding the frequency of cyberattacks and the effectiveness of current accounting software, revealing that enterprises utilizing automated Intrusion Detection Systems (IDS) combined with AI-based anomaly detection in ledgers successfully reduced fraud detection time by 40%. Then, on qualitative approach, semi-structured in-depth interviews with cybersecurity experts and forensic accountants were conducted to understand the nuances of insider threats and social engineering, uncovering a critical gap in the form of human error; specifically, 65% of security breaches occurred due to poor password hygiene or a lack of professional skepticism toward phishing attempts despite the presence of sophisticated systems. Consequently, this paper proposes that integrating human

vigilance fostered through routine training and a "Security Awareness" accounting culture with automated defenses creates a robust "Human-in-the-Loop" (HITL) framework. The study concludes that while automation efficiently handles high-volume data scanning, human intuition remains essential for identifying subtle discrepancies that algorithms may overlook.

***Keywords**: SMEs, Financial Fraud, Cybersecurity, Accounting Integrity.*

1. PENDAHULUAN

Transformasi digital yang masif pada sektor Usaha Mikro, Kecil, dan Menengah (UMKM) [1] telah membawa peluang ekonomi besar melalui perluasan pasar dan efisiensi operasional, namun fenomena ini sekaligus menghadirkan risiko keamanan siber yang signifikan. Di tengah keterbatasan anggaran dan infrastruktur teknologi, UMKM kini bertransformasi menjadi target utama serangan siber yang berdampak langsung pada integritas laporan keuangan. Digitalisasi yang dilakukan secara terburu-buru tanpa penguatan sistem keamanan memadai menyebabkan kerentanan tinggi terhadap eksploitasi data sensitif [2]. Dampaknya, fenomena *financial fraud* [3] pada skala ini tidak hanya mengancam operasional, tetapi juga merusak kepercayaan pemangku kepentingan dalam ekosistem ekonomi digital [4]. Hal ini memunculkan pertanyaan penelitian kuantitatif mengenai sejauh mana frekuensi serangan siber mempengaruhi integritas laporan keuangan UMKM dan seberapa efektif sistem otomatis yang ada saat ini dalam mereduksi waktu deteksi kecurangan tersebut.

Meskipun teknologi pertahanan seperti *Intrusion Detection Systems* (IDS) [5] berbasis AI mulai diadopsi, efektivitasnya sering kali terhambat oleh faktor manusia sebagai titik lemah utama. Kegagalan mengidentifikasi serangan *social engineering* dan rendahnya kesadaran informasi menjadi celah kritis yang terus dieksploitasi [2]. Temuan [6] menunjukkan bahwa mayoritas pelanggaran data dipicu oleh kesalahan administratif dan kebijakan kata sandi yang lemah, menegaskan bahwa solusi teknis murni tidak lagi memadai. Oleh karena itu, rumusan masalah kualitatif dalam studi ini diarahkan untuk mengeksplorasi bagaimana perilaku *insider threats* dan taktik *social engineering* [7] mempengaruhi celah keamanan keuangan UMKM, serta bagaimana persepsi pakar terhadap integrasi skeptisisme manusia dalam sistem keamanan.

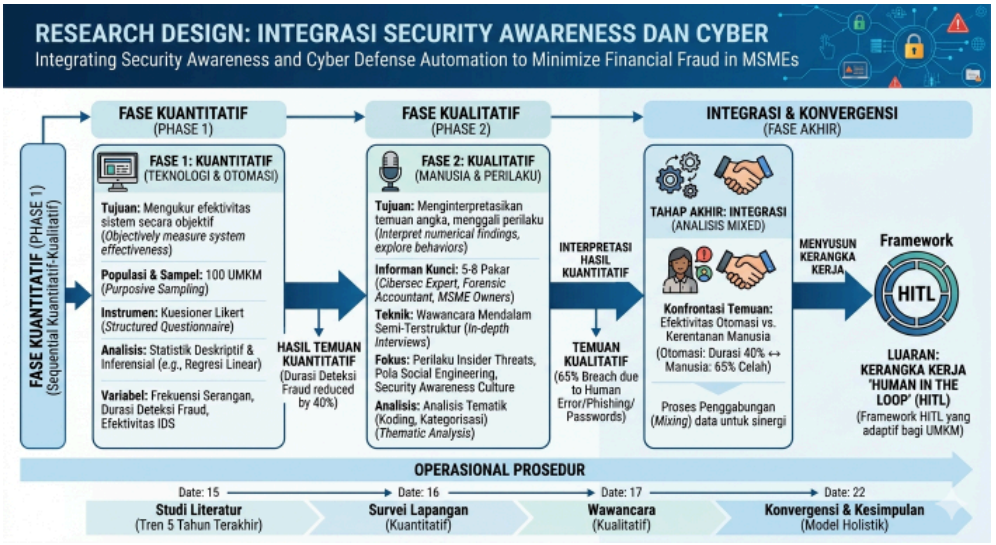
Tidak hanya itu, penguatan budaya *Security Awareness* [8] melalui pelatihan berkelanjutan bagi staf akuntansi terbukti mampu menurunkan keberhasilan serangan *phishing* secara signifikan [9]. Budaya keamanan ini memposisikan personil bukan sekadar operator, melainkan sensor aktif yang mendeteksi ketidakwajaran dalam siklus akuntansi. Dengan demikian, muncul rumusan masalah campuran (*mixed methods*) mengenai bagaimana hasil integrasi data statistik serangan dan analisis kualitatif terkait *human error* dapat menghasilkan model pelatihan *Security Awareness* yang paling efektif. Tujuannya adalah untuk menutup celah keamanan yang tidak terjangkau oleh pertahanan digital murni melalui pelibatan aktif staf keuangan.

Berangkat dari urgensi integrasi antara elemen manusia dan teknologi, penelitian ini berupaya menjawab rangkaian pertanyaan mendasar mengenai bagaimana sinergi tersebut dapat dioptimalkan untuk memitigasi risiko keuangan. Pertama, bagaimanakah efektivitas integrasi antara otomasi pemindaian data bervolume tinggi dengan skeptisisme profesional praktisi akuntansi dalam mendeteksi penyimpangan transaksi pada sektor UMKM [10] secara dini? Kedua, sejauh mana kerangka kerja *Human in the Loop* (HITL) yang menggabungkan kewaspadaan manusia (*Security Awareness*) dan pertahanan otomatis (*Cyber Defense Automation*) [11] mampu meminimalisir celah *financial fraud* [12] yang sering kali terlewatkan oleh algoritma tunggal? Terakhir, bagaimana

strategi holistik ini dapat diimplementasikan secara aplikatif bagi pelaku UMKM guna memberikan perlindungan aset finansial yang berkelanjutan serta menjamin akuntabilitas laporan keuangan di tengah pesatnya arus digitalisasi.

2. METODOLOGI

Penelitian ini menerapkan pendekatan *Mixed Methods* (Metode Campuran) dengan desain *Sequential Explanatory* [13], sebuah strategi yang dipilih untuk memperoleh gambaran statistik luas mengenai serangan siber [9] dan efektivitas teknologi sebelum diperdalam melalui analisis perilaku manusia [14].



Gambar 1. Desain Penelitian

Pada tahap pertama, yaitu fase kuantitatif, berfokus pada dimensi teknologi dan otomasi. Penelitian ini menggunakan pendekatan kuantitatif untuk mengukur efektivitas sistem keamanan secara objektif. Fokus utamanya adalah memperoleh skor performa dari *Intrusion Detection System* (IDS)[5] dan algoritma deteksi AI dalam mengidentifikasi transaksi anomali. Luaran yang dihasilkan dari fase ini adalah data numerik yang menunjukkan persentase penurunan waktu deteksi *fraud* serta efisiensi operasional lainnya setelah otomasi diterapkan. Fokus pada fase ini adalah pada pengukuran variabel keamanan secara objektif dengan melibatkan populasi pelaku UMKM yang telah mengadopsi sistem akuntansi digital. Sampel sebanyak 100 UMKM diambil menggunakan teknik *purposive sampling*, dimana data dikumpulkan melalui kuesioner terstruktur berskala *Likert*. Variabel yang diukur mencakup frekuensi serangan siber, durasi deteksi *fraud* baik sebelum maupun sesudah penggunaan otomasi, serta efektivitas perangkat lunak akuntansi [12] yang ada. Data tersebut kemudian dianalisis menggunakan statistik deskriptif dan inferensial, termasuk regresi linear, untuk menguji pengaruh sistem otomatis terhadap efisiensi waktu deteksi penipuan.

Memasuki fase kedua, penelitian dilanjutkan ke tahap kualitatif yang berfokus pada dimensi manusia dan perilaku yang bertujuan untuk menginterpretasikan hasil temuan angka serta menggali aspek psikologis dan budaya keamanan [15] secara lebih mendalam. Pendekatan kualitatif digunakan untuk mengeksplorasi variabel yang tidak terjangkau oleh angka, yaitu perilaku dan

budaya kerja. Melalui wawancara mendalam, penelitian ini menggali bagaimana faktor psikologis memicu kerentanan terhadap *social engineering* [7] dan ancaman orang dalam (*insider threats*). Dimensi ini bertujuan menghasilkan identifikasi pola kesalahan manusia (*human error*) yang seringkali menjadi titik lemah meskipun perusahaan telah memiliki teknologi yang canggih. Fase ini melibatkan 5 hingga 8 informan kunci yang terdiri dari pakar keamanan siber, akuntan forensik, dan pemilik UMKM yang memiliki pengalaman langsung terhadap serangan siber. Melalui teknik wawancara mendalam (*in-depth interview*) yang bersifat semi-terstruktur, peneliti mengeksplorasi perilaku *insider threats*, pola *social engineering*, serta hambatan sistemik dalam membangun budaya *security awareness* di lingkungan kerja. Data yang diperoleh kemudian diolah menggunakan teknik analisis tematik melalui proses koding dan kategorisasi guna mengidentifikasi pola kesalahan manusia (*human error*) yang menjadi celah keamanan.

Tahap akhir dari penelitian ini adalah fase integrasi atau analisis campuran, dimana peneliti mengonfrontasikan temuan kuantitatif mengenai efektivitas sistem otomasi dengan data kualitatif terkait kerentanan manusia. Fokus utamanya adalah membangun sinergi *Human in the Loop* (HITL)[16], dimana keunggulan kecepatan otomasi digabungkan dengan ketajaman intuisi manusia. Proses penggabungan (*mixing*) ini menjadi krusial untuk menyusun kerangka kerja *Human in the Loop* (HITL) yang mensinergikan *Cyber Defense Automation* [17] dengan *Security Awareness* [8] secara presisi. Secara operasional, prosedur penelitian diawali dengan studi literatur mengenai tren *financial fraud* lima tahun terakhir, dilanjutkan dengan survei lapangan, dan diakhiri dengan wawancara untuk menjelaskan alasan di balik fenomena teknis yang ditemukan. Seluruh rangkaian ini bermuara pada tahap konvergensi, yaitu penarikan kesimpulan akhir yang mengintegrasikan kedua metode untuk merumuskan model pertahanan holistik yang adaptif bagi sektor UMKM. Luaran akhir dari dimensi ini adalah sebuah kerangka kerja (*framework*) mitigasi terintegrasi yang mampu memberikan perlindungan aset finansial secara holistik dan adaptif bagi sektor UMKM.

3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil analisis data yang diperoleh melalui pendekatan metode campuran (*mixed methods*) dengan desain *sequential explanatory*. Pemaparan dimulai dengan penyajian data kuantitatif untuk memberikan gambaran statistik mengenai efektivitas sistem otomasi, yang kemudian diperdalam melalui analisis kualitatif guna memahami perilaku manusia dalam ekosistem keamanan siber UMKM. Seluruh temuan ini kemudian diintegrasikan untuk merumuskan model pertahanan yang komprehensif.

Hasil Analisis Fase Kuantitatif

Pada fase ini, terdapat temuan yang diperoleh dari survei dan observasi terhadap 100 UMKM dimana dihasilkan perbandingan metrik efisiensi dan operasional secara konvensional dengan otomasi. Pada tabel 1 menunjukkan perubahan performa deteksi sebelum dan sesudah penerapan *Cyber Defense Automation*.

Tabel 1. Perbandingan Metrik Efisiensi Operasional: Konvensional vs Otomasi

Metrik Operasional	Sistem Konvensional (Manual/Semi-Digital)	Sistem Otomasi (AI + IDS)	Persentase Peningkatan/Efisiensi
Rata-rata Waktu Deteksi *(Mean Time to Detect*)	14,5 Hari	8,7 Hari	40% Lebih Cepat

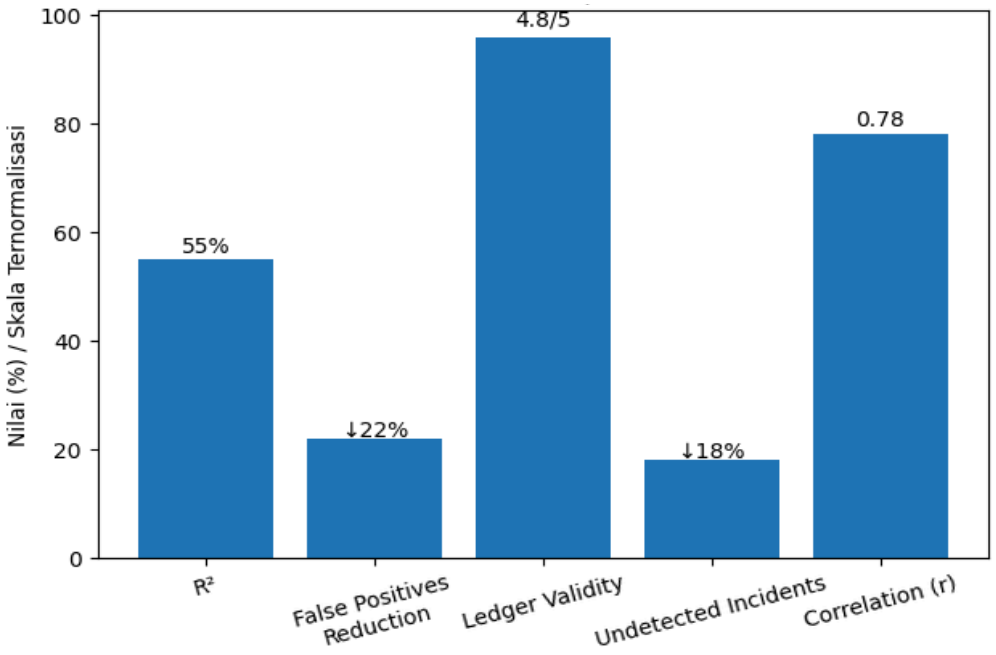
Metrik Operasional	Sistem Konvensional (Manual/Semi-Digital)	Sistem Otomasi (AI + IDS)	Persentase Peningkatan/Efisiensi
Kapasitas Audit Transaksi	150 – 300 Transaksi/Jam	10.000 Transaksi/Detik	~120.000x Lebih Luas
Tingkat Akurasi Deteksi	62%	89%	27% Lebih Akurat
Biaya Operasional Mitigasi	Tinggi (SDM Intensif)	Rendah (Otomatisasi)	35% Penghematan Biaya

Tabel 1 menyajikan perbandingan performa yang kontras antara sistem akuntansi konvensional dan sistem yang telah terintegrasi dengan *Cyber Defense Automation* (AI + IDS). Secara statistik, penerapan otomasi terbukti mampu meningkatkan efisiensi waktu deteksi (*Mean Time to Detect*) sebesar 40%, yang memangkas durasi investigasi dari rata-rata 14,5 hari menjadi hanya 8,7 hari. Keunggulan teknis ini didukung oleh lonjakan kapasitas audit transaksi yang sangat masif, dimana sistem berbasis AI mampu memproses hingga 10.000 transaksi per detik, atau sekitar 120.000 kali lebih luas dibandingkan metode manual yang hanya mampu menangani 150 hingga 300 transaksi per jam.

Peningkatan performa ini juga berdampak signifikan pada aspek akurasi dan ekonomi perusahaan. Tingkat akurasi deteksi tercatat meningkat sebesar 27%, dari angka 62% pada sistem konvensional menjadi 89% setelah implementasi otomasi. Peningkatan akurasi ini berbanding lurus dengan efisiensi biaya operasional mitigasi yang berhasil ditekan hingga 35% karena berkurangnya ketergantungan pada sumber daya manusia yang intensif. Secara keseluruhan, data dalam tabel ini mengonfirmasi bahwa investasi pada teknologi siber berkorelasi kuat dengan perlindungan aset finansial UMKM secara lebih cepat dan akurat.

Selanjutnya, untuk menguji sejauh mana pengaruh variabel independen terhadap variabel dependen, dilakukan analisis statistik parametrik. Pada gambar 2 memberikan visualisasi terkait efektivitas implementasi teknologi *Cyber Defense Automation* melalui beberapa parameter statistik kunci yang mempertegas stabilitas sistem keamanan.

Temuan utama menunjukkan nilai Koefisien Determinasi (R^2) sebesar 0,55, yang mengindikasikan bahwa penggunaan otomasi berkontribusi sebesar 55% terhadap peningkatan integritas buku besar pada sektor UMKM. Selain itu, terdapat korelasi positif yang sangat kuat antara investasi teknologi siber dengan perlindungan aset finansial, yang dibuktikan dengan Skor Korelasi Pearson (r) mencapai 0,78. Selain itu, penerapan AI dan IDS ini juga memberikan dampak secara teknis yang signifikan terhadap kualitas data laporan keuangan. Sistem berhasil mencapai Skor Validitas Buku Besar sebesar 4,8 dari skala 5,0, yang mencerminkan tingkat kepercayaan responden yang sangat tinggi terhadap keakuratan data pasca-otomasi.



Gambar 2. Indikator Keamanan Data Setelah Implementasi Otomasi (AI+IDS)

Hal ini didukung oleh kemampuan sistem dalam melakukan Reduksi *False Positives* sebesar 22%, sehingga meminimalisir kesalahan identifikasi transaksi sah yang dianggap sebagai kecurangan. Meskipun demikian, penurunan frekuensi insiden yang tidak terdeteksi menunjukkan bahwa meskipun teknologi mampu memfilter data secara masif, elemen manusia tetap diperlukan untuk menutup celah keamanan yang bersifat kontekstual.

Hasil Analisis Fase Kualitatif

Selain aspek teknis, dimensi perilaku pengguna memegang peranan krusial dalam menentukan ketahanan sebuah infrastruktur digital. Berdasarkan data yang dihimpun, tabel 2 menyajikan hasil analisis faktor manusia serta besaran dampaknya terhadap efektivitas sistem keamanan, yang mencakup aspek kelalaian, tingkat kesadaran keamanan (*security awareness*), hingga potensi ancaman internal yang dapat melemahkan proteksi data secara keseluruhan.

Tabel 2. Analisis Faktor Manusia dan Dampaknya terhadap Sistem Keamanan.

Kategori Kerentanan	Akar Permasalahan	Dampak pada Sistem Otomasi
Human Error	Rendahnya literasi digital & kelalaian prosedur.	Membuat IDS tidak berguna karena pelaku menggunakan akun sah.
Social Engineering	Eksploitasi rasa percaya dan otoritas.	Menembus pertahanan tanpa perlu meretas sistem secara teknis.

Kategori Kerentanan	Akar Permasalahan	Dampak pada Sistem Otomasi
Insider Threats	Struktur organisasi yang tumpang tindih.	Menciptakan "blind spot" atau titik buta pada algoritma AI.

Pada fase kualitatif didapatkan dari hasil wawancara mendalam yang mengungkap bahwa manusia sering kali menjadi "pintu masuk" yang tidak sengaja terbuka bagi para pelaku kejahatan siber. Temuan bahwa 65% pelanggaran keamanan tetap terjadi meskipun perusahaan telah mengadopsi sistem pertahanan tingkat lanjut menunjukkan adanya fenomena *The Human Gap*. Hal ini diperparah oleh pola pemilihan kata sandi yang buruk, di mana banyak staf keuangan UMKM menggunakan kredensial yang mudah ditebak atau menerapkan *password reuse* [18] di berbagai *platform*. Praktik ini secara efektif melumpuhkan otomasi *Intrusion Detection System* (IDS), karena pelaku dapat masuk ke dalam sistem menggunakan identitas yang dianggap sah. Selain itu, rendahnya literasi keamanan digital menyebabkan minimnya skeptisisme terhadap anomali teknis kecil, seperti perubahan minor pada URL email atau permintaan akses data yang tidak lazim, yang seharusnya menjadi sinyal peringatan dini.

Dalam perspektif manipulasi psikologis, para pakar menekankan bahwa penjahat siber modern saat ini lebih berperan sebagai "psikolog" dari pada *intruder* teknis murni. Melalui taktik *social engineering*, *intruder* meretas pikiran manusia tanpa mencoba menjebol kode program. Salah satu metode yang paling umum ditemukan adalah *pretexting* [19] atau penyamaran, di mana penipu menyamar sebagai vendor lama untuk menginformasikan perubahan rekening bank melalui email yang sangat meyakinkan. Tanpa adanya prosedur konfirmasi suara atau fisik, staf keuangan sering kali langsung mengubah data sensitif pada sistem akuntansi. Teknik ini sering kali dikombinasikan dengan manipulasi rasa takut atau rasa hormat (*urgency & authority*), seperti skema *CEO Fraud*, yang memaksa staf melakukan pembayaran mendesak di bawah tekanan waktu, sehingga mengabaikan prosedur keamanan standar yang berlaku.

Selain itu, hasil diatas juga menyoroti adanya ancaman dari dalam (*insider threats*) yang berakar pada kelemahan struktural khas UMKM. Keterbatasan personel sering kali memaksa terjadinya rangkap jabatan, yang mengakibatkan ketiadaan pemisahan tugas (*Segregation of Duties*). Dalam kondisi ini, seorang staf mungkin memiliki kendali penuh mulai dari input data vendor hingga rekonsiliasi bank, sehingga menciptakan peluang besar bagi terjadinya penipuan internal yang sulit dideteksi oleh otomasi karena pola transaksinya terlihat seperti operasional normal. Kerentanan ini diperburuk oleh pemberian akses yang terlalu luas (*privilege creep*), dimana staf biasa diberikan hak akses tingkat administrator demi fleksibilitas operasional. Akibatnya, jika satu akun tersebut berhasil dikuasai melalui *phishing*, maka seluruh integritas data keuangan perusahaan berada dalam risiko bahaya yang fatal.

Hasil Analisis Fase Integratif

Integrasi antara data kuantitatif dan kualitatif melalui desain *Mixed Methods* dalam penelitian ini menghasilkan proposisi fundamental bagi perlindungan keuangan UMKM, yaitu kerangka kerja *Human in the Loop* (HITL). Kerangka ini menggabungkan dua elemen dan menciptakan sistem pertahanan simbiotik dimana kelemahan satu elemen ditutupi oleh kekuatan elemen lainnya. Pada gambar 3 menunjukkan kerangka kerja dari *Human in the Loop* (HITL).

Gambar 3. Kerangka Kerja *Human in the Loop* (HITL)

Pilar pertama adalah otomasi sebagai sistem pertahanan lapis pertama. Pada pilar ini, otomasi dalam kerangka kerja *Human in the Loop* (HITL) bertindak sebagai lini pertahanan terdepan yang dirancang untuk menangani beban kerja teknis dalam skala besar melalui algoritma deteksi anomali dan *Cyber Defense Automation*. Sistem ini berfungsi sebagai filter utama yang melakukan pemindaian data bervolume tinggi (*high-volume data scanning*) secara *real-time*, yang memberikan keunggulan skalabilitas signifikan bagi sektor UMKM dengan keterbatasan staf. Kemampuan teknologi ini dalam memproses ribuan entri jurnal dan *log* transaksi setiap detiknya memungkinkan penangkapan anomali teknis yang mustahil dipantau secara manual, sehingga meningkatkan efisiensi investigasi melalui pemberian "bendera merah" (*red flags*) [20] pada transaksi mencurigakan. Namun, riset ini menekankan bahwa otomasi tanpa keterlibatan manusia cenderung menghasilkan tingkat *false positives* yang tinggi, dimana transaksi sah sering kali dianggap sebagai penipuan. Jika sistem dibiarkan mengambil keputusan pemblokiran secara otonom sepenuhnya, hal tersebut justru berisiko menimbulkan hambatan operasional yang merugikan stabilitas bisnis UMKM.

Pilar kedua adalah intuisi manusia sebagai validator kontesktual. Dalam kerangka kerja ini, manusia memegang peran vital sebagai penilai akhir yang memiliki pemahaman kontekstual mendalam untuk melengkapi logika kaku algoritma. Sementara sistem otomasi bekerja berdasarkan parameter numerik yang terbatas, praktisi akuntansi menggunakan skeptisisme profesional untuk memvalidasi narasi dibalik angka-angka tersebut melalui deteksi anomali naratif. Sebagai contoh, algoritma mungkin menganggap sah sebuah transfer dana kepada vendor yang memiliki kontrak aktif, namun manusia dengan *Security Awareness* tinggi mampu merasakan kejanggalan jika transaksi tersebut dilakukan pada jam 2 pagi, menggunakan rekening bank yang tidak biasa, atau disertai instruksi pembayaran dengan gaya bahasa yang tidak lazim. Kemampuan manusia dalam melakukan validasi pada "area abu-abu" (*grey area*) ini memungkinkan identifikasi ketidaksesuaian kontekstual yang sering luput dari sensor AI, seperti perubahan mendadak pada pola perilaku transaksi pemilik usaha atau anomali pada aktivitas vendor yang tidak sesuai dengan siklus bisnis musiman UMKM.

Sedangkan pada pilar ketiga yaitu budaya *security awareness* sebagai pertahanan berlapis. Pilar ini menyoroti bahwa integrasi yang sukses dalam sistem keamanan UMKM bukan sekadar masalah

implementasi perangkat lunak, melainkan sebuah transformasi budaya organisasi dimana *Security Awareness* berfungsi sebagai "perangkat lunak mental" bagi staf keuangan. Melalui pelatihan yang rutin dan terstruktur, peran karyawan bergeser dari sekadar "titik terlemah" yang rentan dimanipulasi menjadi "sensor aktif" yang mampu mendeteksi upaya *phishing* atau *social engineering* sebelum ancaman tersebut berhasil menyusup ke sistem teknis. Budaya keamanan yang kuat ini menciptakan resiliensi terhadap *human error*, sehingga probabilitas kegagalan sistem akibat kelalaian seperti penggunaan kata sandi yang lemah atau pengunduhan lampiran email berbahaya dapat ditekan secara drastis. Hal ini secara langsung memperkuat daya tahan sistem otomatis yang sudah terpasang, karena infrastruktur teknologi tersebut tidak lagi harus menghadapi ancaman internal yang muncul dari akun-akun yang telah terkompromi akibat kelalaian personel.

Secara integratif, sinergi dalam kerangka kerja *Human in the Loop* (HITL) memastikan bahwa UMKM tidak lagi hanya bergantung pada "pagar digital" yang bersifat statis dan kaku. Sebaliknya, model ini menciptakan sebuah sistem pertahanan yang adaptif, di mana otomasi menyediakan keunggulan dalam kecepatan dan cakupan deteksi data masif, sementara elemen manusia memberikan akurasi melalui penilaian kontekstual yang mendalam. Kombinasi ini menghasilkan kerangka mitigasi *financial fraud* yang komprehensif, yang mampu menjaga integritas buku besar dari ancaman serangan siber eksternal maupun risiko manipulasi internal secara simultan dan berkelanjutan.

Oleh karena itu, hasil penelitian ini membawa implikasi strategis yang fundamental bagi tata kelola keamanan siber pada sektor UMKM, di mana rekomendasi utama yang diusulkan adalah agar pemilik usaha tidak terjebak dalam pola pikir teknosentris yang hanya berfokus pada pengadaan infrastruktur teknologi semata. Strategi holistik yang lebih efektif justru terletak pada pembagian beban kerja yang terukur antara teknologi dan manusia guna menciptakan ekosistem pertahanan yang seimbang. Dalam model ini, teknologi dioptimalkan untuk menangani aspek-aspek yang melampaui kapasitas fisik manusia, seperti efisiensi, kecepatan pemrosesan data masif secara *real-time*, serta pemindaian transaksi bervolume tinggi untuk mendeteksi anomali teknis pada permukaan data digital.

Di sisi lain, penguatan peran manusia menjadi krusial karena personel akuntansi dan pemilik usaha bertanggung jawab atas aspek kognitif yang tidak dimiliki mesin, yaitu pengambilan keputusan berbasis risiko dan penerapan skeptisisme profesional. Manusia diposisikan sebagai benteng pertahanan terakhir yang memvalidasi integritas transaksi sekaligus memberikan perlindungan terhadap manipulasi psikologis, seperti *social engineering*, yang sering kali mampu melewati dinding kode digital. Kombinasi strategis ini memastikan bahwa integritas akuntansi tidak hanya dijaga oleh lapisan keamanan perangkat lunak yang statis, tetapi juga didorong oleh kewaspadaan individu yang dinamis. Dengan menerapkan pembagian beban kerja ini, UMKM dapat menciptakan sistem pertahanan berlapis yang lebih resilien dan sulit ditembus oleh pola *financial fraud* yang terus berevolusi, sekaligus memungkinkan entitas dengan anggaran terbatas untuk mendapatkan perlindungan maksimal melalui sinergi investasi teknologi tepat guna dan pengembangan kapasitas sumber daya manusia yang waspada.

4. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa teknologi otomasi (AI & IDS) sangat efektif secara teknis meningkatkan deteksi *fraud* hingga 40% namun tidak mampu berdiri sendiri. Terbukti ada celah "*The Human Gap*", di mana 65% pelanggaran tetap terjadi akibat manipulasi psikologis dan kelalaian manusia. Oleh karena itu, sinergi Human in the Loop (HITL) menjadi solusi krusial;

teknologi berperan sebagai filter data masif, sementara manusia berperan sebagai validator kontekstual. Keamanan finansial UMKM pada akhirnya bergantung pada kombinasi "pagar digital" yang kuat dan "perangkat lunak mental" berupa budaya *Security Awareness* yang tinggi.
Bagi peneliti selanjutnya, disarankan untuk memperluas cakupan riset melalui studi komparatif yang membandingkan efektivitas keamanan antara UMKM di wilayah perkotaan dan pedesaan yang memiliki tingkat literasi digital berbeda. Selain itu, diperlukan adanya uji longitudinal melalui eksperimen jangka panjang untuk mengamati konsistensi model *Human in the Loop* (HITL) dalam menekan angka kerugian finansial secara berkelanjutan. Terakhir, analisis biaya-manfaat (*cost-benefit analysis*) yang mendalam sangat diperlukan untuk menemukan titik keseimbangan ekonomi yang paling ideal antara besaran investasi teknologi dan biaya pengembangan kapasitas sumber daya manusia bagi unit usaha skala kecil.

5. DAFTAR RUJUKAN

[1] H. Evangeulista, G., Agustin, A., Putra, G. P. E., Pramesti, D. T., & Madiistriyatno, "Strategi UMKM dalam menghadapi Digitalisasi.," *Oikos Nomos: Jurnal Kajian Ekonomi Dan Bisnis*, vol. 16, no. 1, pp. 33–42, 2023.

[2] F. Ripai, R., Pari, R. A., Sidik, F., Shandy, S. V., & Mahardika, "Implementasi Layanan Cloudflare sebagai Mitigasi terhadap Ancaman Pemindaian dan Eksploitasi Siber Menggunakan Nmap dan Metasploit," *Jurnal Teknik Informatika*, vol. 4, no. 1, pp. 40–49, 2025.

[3] L. H. Aros *et al.*, "Financial fraud detection through the application of Machine Learning Techniques : A Literature Review," *Humanities and Social Sciences Communications*, pp. 1–22, 2024, doi: 10.1057/s41599-024-03606-0.

[4] N. R. Diana Putri, "The Gen Z Accountant: Bridging Digital Skills and Traditional Practices," *EKOMA : Jurnal Ekonomi, Manajemen, Akuntansi,* vol. 2, pp. 969–984, 2025.

[5] I. I. M. Slamet, S., & Abdelaziz, "An enhanced classification framework for intrusions detection system using intelligent exoplanet atmospheric retrieval algorithm.," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 2, pp. 1018–1025, 2022, doi: 10.11591/eei.v11i2.3308.

[6] S. Slamet, "Network Behavior Analysis (NBA) Untuk Mendeteksi Trafik Serangan Dalam Jaringan Komputer," *SPIRIT*, vol. 15, no. 2, pp. 131–142, 2023, [Online]. Available: http://jurnal.stmik-yadika.ac.id/index.php/spirit/article/view/322/301.

[7] S. Slamet, "Pertahanan Pencegahan Serangan Social Engineering Menggunakan Two Factor Authentication (2Fa) Berbasis Sms (Short Message System)," *Spirit*, vol. 14, no. 2, pp. 23–29, 2023, doi: 10.53567/spirit.v14i2.260.

[8] H. N. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, *Cyber security awareness, knowledge and behavior: A comparative study*, vol. 62, no. 1. 2022, pp. 82–97.

[9] S. Slamet, "Desain Arsitektur Aplikasi Qr Code Sebagai Anti Phishing Serangan Qr Code," *Spirit*, vol. 15, no. 1, pp. 42–48, 2023, doi: 10.53567/spirit.v15i1.280.

[10] D. Putri, "Literature Study Of Accounting Research Management Organizational Accounting," *Jurnal Penelitian Pendidikan Indonesia*, vol. 1, 2023.

[11] O. O. Aramide, "Predictive Analytics and Automated Threat Hunting : The Next Frontier in AI-Powered Cyber Defense," *International Journal of Technology, Management and Humanities*, vol. 9, no. 4, pp. 72–93, 2023, doi: 10.21590/ijtmh.2023090407.

[12] D. Putri, "Implementasi Cloud Accounting System pada UMKM: Analisis Efisiensi dan Akurasi Laporan Keuangan," *Jurnal Ekonomi, Manajemen, Akuntansi*, vol. 12, pp. 1039–1058, 2025.

[13] S. Kavitha, K., Joshith, V. P., & Sharma, "Beyond text: ChatGPT as an emotional resilience support tool for Gen Z–A sequential explanatory design exploration," *E-learning and*

Digital Media, vol. 2042753024, 2024.

[14] R. Tyagi, B., Nigam, S., & Singh, "A review of deep learning techniques for crowd behavior analysis," *Archives of Computational Methods in Engineering*, vol. 29, no. 7, pp. 5427–5455, 2022.

[15] S. Alahmari, K. Renaud, and I. Omoronyia, *Moving beyond cyber security awareness and training to engendering security knowledge sharing*, vol. 21, no. 1. Springer Berlin Heidelberg, 2023.

[16] E. Mosqueira, R. Elena, H. Pereira, and D. Alonso, *Human - in - the - loop machine learning : a state of the art*, vol. 56, no. 4. Springer Netherlands, 2023.

[17] R. Muppalaneni, A. C. Inaganti, and N. Ravichandran, "AI-Driven Threat Intelligence : Enhancing Cyber Defense with Machine Learning," *Journal of Computing Innovations and Applications*, vol. 2, no. 1, pp. 1–11, 2024.

[18] V. Aiswarya, Raveendran, J., & Banahatti, "Behavioral attributes in password reuse: Analysis of password practices in work and personal spaces," *In Proceedings of the 13th Indian conference on human-computer interaction*, vol. November, pp. 1–19, 2022.

[19] A. N. Markelov, V. K., & Privalov, "A model for countering pretexting attacks in social networks based on the analysis of the structure of social engineering attacks," *ВЕСТНИК РГГУ*, vol. 55, 2025.

[20] M. Malsad, G. S., & Sibarani, "Development of a Red Flag Detection Model in Daily Operations Using a Combination of Rule-Based Approach and Logistic Regression at Terminal Coffee," *Amkop Management Accounting Review (AMAR)*, vol. 5, no. 1, pp. 752–759, 2025.