BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Persoalan kecurangan atau yang lebih dikenal dengan istilah *fraud* merupakan ancaman sistemik yang senantiasa membayangi integritas perekonomian di berbagai belahan dunia, tidak terkecuali di Indonesia. Sebagai negara dengan dinamika ekonomi yang tinggi, Indonesia menghadapi tantangan yang tidak sederhana dalam menciptakan iklim bisnis yang bersih dan transparan. Karyono (2002) dalam penelitiannya menegaskan bahwa posisi Indonesia seringkali diidentikkan sebagai salah satu negara dengan tingkat korupsi yang memprihatinkan di mata dunia. Realitas ini tercermin dari banyaknya kasus hukum yang melibatkan penyalahgunaan wewenang dan manipulasi keuangan yang ditangani oleh pihak berwajib, namun seringkali menemui jalan buntu dalam penyelesaiannya. Karyono (2002) juga menggarisbawahi bahwa meskipun instrumen hukum, regulasi, dan berbagai lembaga pengawas telah dibentuk dan diperkuat dari waktu ke waktu, keberadaan mereka seolah belum mampu menyentuh akar permasalahan atau memberikan efek jera yang signifikan bagi para pelaku korupsi yang kian mahir menyembunyikan jejaknya.

Dalam konteks akademik dan praktis, pemahaman mengenai *fraud* terus mengalami metamorfosis yang signifikan. Ambarwati et al. (2023) menjelaskan melalui studi literaturnya bahwa teori-teori penyebab kecurangan tidak bersifat statis, melainkan terus berevolusi mengikuti kompleksitas lingkungan bisnis dan perilaku manusia. Dimulai dari konsep klasik *fraud triangle* yang berfokus pada tekanan, peluang, dan rasionalisasi, hingga berkembang menjadi *hexagon theory* yang mencakup variabel yang lebih luas seperti arogansi dan kolusi. Evolusi teoretis ini, menurut Ambarwati et al. (2023), menunjukkan bahwa pendekatan konvensional dalam mendeteksi kecurangan perlu ditinjau kembali secara kritis. Landasan teori yang kuat dan runut sangat diperlukan untuk memberikan "benang merah" dalam kerangka berpikir auditor, sehingga mereka dapat mengidentifikasi

celah-celah kecurangan dalam bidang akuntansi, manajemen, hingga budaya etis organisasi yang semakin terdistorsi.

Tuntutan publik terhadap akuntan dan auditor pun meningkat drastis seiring dengan masifnya skandal keuangan yang merugikan masyarakat luas. Karyono (2002) menyebutkan adanya ekspektasi besar dari masyarakat agar profesi akuntan mampu meningkatkan kompetensi profesionalnya, tidak hanya sebagai pencatat transaksi, tetapi sebagai garda terdepan dalam mendeteksi dan mengungkapkan penipuan. Auditor diharapkan memiliki kepekaan atau "skeptisisme profesional" yang tajam guna memenuhi tanggung jawab moral dan hukum mereka. Hal ini menjadi semakin menantang ketika dunia memasuki era digital, di mana data transaksi tidak lagi tercatat secara fisik di atas kertas, melainkan tersimpan dalam sistem informasi yang sangat kompleks dan dalam volume yang luar biasa besar atau yang sering disebut sebagai era *Big Data*.

Artificial Intelligence (AI) merupakan teknologi yang mampu meniru kemampuan kognitif manusia dalam melakukan pembelajaran, mengenali pola, menganalisis data, dan menghasilkan rekomendasi berdasarkan informasi yang tersedia. Perkembangan AI telah membawa perubahan pada berbagai sektor, termasuk profesi audit, karena teknologi ini mampu membantu auditor dalam mengolah data dalam jumlah besar secara lebih cepat dan efisien dibandingkan metode konvensional Qatawneh (2024). Namun demikian, penelitian ini tidak berfokus pada kemampuan teknologi AI itu sendiri, melainkan pada persepsi auditor terhadap penggunaan Artificial Intelligence**,** yaitu bagaimana auditor memandang manfaat, kemudahan penggunaan, dan efektivitas AI dalam membantu pelaksanaan prosedur audit. Persepsi tersebut menjadi penting karena tingkat penerimaan auditor terhadap teknologi akan memengaruhi intensitas penggunaan AI dalam mendukung proses audit dan deteksi fraud (Mawlidy et al., 2024).

AI dalam bidang audit ini didukung secara empiris oleh penelitian Qatawneh (2024). Dalam studinya, Qatawneh (2024) menemukan bukti statistik yang kuat bahwa penerapan kecerdasan buatan dalam Sistem Informasi Akuntansi

(SIA) berpengaruh secara signifikan terhadap keberhasilan audit dan deteksi kecurangan. Lebih lanjut, Qatawneh (2024) memperkenalkan peran *Natural Language Processing* (NLP) sebagai variabel yang mampu memoderasi hubungan tersebut. NLP memungkinkan mesin untuk memahami bahasa manusia yang tidak terstruktur, seperti catatan dalam jurnal atau korespondensi email, yang seringkali menjadi tempat persembunyian bukti-bukti *fraud*. Dengan demikian, AI tidak hanya bekerja pada data angka, tetapi juga pada data teks, memberikan cakupan analisis yang lebih menyeluruh dalam membongkar praktik-praktik ilegal di dalam perusahaan.

Meskipun perkembangan Artificial Intelligence dalam bidang audit berkembang cukup pesat di berbagai negara, penerapannya di Indonesia masih berada pada tahap awal dan belum dilakukan secara merata oleh seluruh Kantor Akuntan Publik (KAP). Implementasi AI umumnya lebih banyak ditemukan pada KAP berskala besar yang memiliki sumber daya teknologi, investasi digital, dan tenaga profesional yang memadai. Sementara itu, sebagian besar KAP kecil dan menengah masih mengandalkan penggunaan *Generalized Audit Software* (GAS), teknik audit berbantuan komputer *(Computer Assisted Audit Techniques/CAATs*), serta prosedur audit konvensional dalam melaksanakan pemeriksaan. Kondisi tersebut menunjukkan bahwa keberhasilan implementasi AI dalam audit tidak hanya bergantung pada ketersediaan teknologi, tetapi juga dipengaruhi oleh persepsi auditor terhadap manfaat dan kemudahan penggunaan AI dalam mendukung proses audit, khususnya dalam mendeteksi fraud.

Selain kecerdasan buatan, efisiensi kerja auditor dalam lingkungan yang terkomputerisasi sangat ditentukan oleh penggunaan perangkat lunak audit yang mumpuni, yaitu *Generalized Audit Software* (GAS). Darono (2011) menjelaskan bahwa GAS dirancang untuk menjawab keterbatasan auditor saat menghadapi situasi di mana bukti audit fisik sulit ditemukan karena seluruh operasional entitas telah menggunakan sistem informasi komputer. Dalam konteks pemerintahan, Darono (2011) menekankan bahwa penggunaan GAS sangat membantu auditor internal (APIP) dalam melakukan reviu laporan keuangan secara lebih sistematis,

cepat, dan akurat. Penggunaan perangkat lunak ini memungkinkan auditor untuk melakukan ekstraksi data langsung dari basis data klien, melakukan pengujian pengendalian, hingga melakukan analisis tren yang membantu dalam mewujudkan transparansi serta akuntabilitas pengelolaan keuangan negara. Tanpa bantuan GAS, auditor akan terjebak dalam proses manual yang memakan waktu lama dan rentan terhadap kesalahan manusia (*human error*).

Namun, di balik segala kemudahan yang ditawarkan oleh teknologi digital dan audit berbasis komputer, muncul ancaman baru yang tidak kalah berbahaya, yaitu risiko keamanan siber atau *Cybersecurity Client*. Yulie & Mukhtaruddin (2026) memperingatkan bahwa meskipun inovasi seperti sistem akuntansi berbasis *cloud* dapat meningkatkan kualitas laporan keuangan melalui otomatisasi, teknologi ini juga membuka pintu bagi serangan siber yang dapat mengancam privasi, integritas, dan aksesibilitas data keuangan. Risiko ini bukan sekadar ancaman teknis, melainkan masalah tata kelola yang serius. Yulie & Mukhtaruddin (2026) berpendapat bahwa profesi akuntansi kini memiliki peran baru sebagai pemantau risiko siber dan perancang pengendalian internal berbasis teknologi untuk mencegah manipulasi data oleh pihak-pihak yang tidak bertanggung jawab yang ingin menutupi jejak kecurangan mereka.

Besarnya ancaman siber di Indonesia bukanlah isapan jempol belaka. Samudra et al. (2023) mengungkapkan fakta yang mengkhawatirkan berdasarkan data sistem monitoring *traffic* ID-SIRTII, di mana insiden serangan siber di Indonesia tercatat mencapai angka satu juta insiden dan diprediksi akan terus meningkat setiap harinya. Serangan-serangan ini seringkali mengeksploitasi kelemahan pada aplikasi dan sistem yang tidak terawasi dengan baik. Samudra et al. (2023) menegaskan bahwa perlindungan terhadap aset digital kini menjadi perhatian utama perusahaan karena serangan siber tidak hanya merugikan secara finansial, tetapi juga menghancurkan reputasi dan kepercayaan pemangku kepentingan. Dalam dunia audit, keamanan bukti digital sangatlah krusial; jika keamanan siber lemah, maka bukti-bukti *fraud* yang ditemukan bisa dianggap tidak valid karena rentan dimanipulasi.

Relevansi keamanan siber dalam dunia akuntansi juga dibahas secara mendalam oleh Sibarani et al. (2025) melalui pendekatan *Systematic Literature Review*. Mereka memperkenalkan konsep *Cybersecurity Client Accounting* sebagai disiplin yang strategis untuk memastikan keandalan laporan keuangan dan proses audit di tengah kerentanan sistem digital. Sibarani et al. (2025) menyatakan bahwa integritas data yang dijaga oleh sistem *Cybersecurity Client* yang kuat adalah fondasi bagi akuntan untuk dapat memberikan opini yang benar. Tanpa keamanan yang memadai, semua teknologi canggih seperti AI dan GAS akan kehilangan fungsinya karena data yang diolah tidak lagi bisa dipercaya keasliannya. Oleh karena itu, kompetensi digital bagi calon akuntan harus segera diintegrasikan ke dalam kurikulum pendidikan agar mereka siap menghadapi ancaman ini di masa depan.

Keberhasilan implementasi semua teknologi canggih ini baik itu AI, GAS, maupun sistem keamanan siber dalam membantu auditor mengungkap *fraud* sangat bergantung pada tingkat kesesuaian antara teknologi tersebut dengan tugas yang diemban oleh penggunanya. Hal ini sejalan dengan teori *Task-Technology Fit* (TTF). Gama et al. (2021) menjelaskan bahwa kinerja individu dalam menggunakan teknologi informasi sangat dipengaruhi oleh sejauh mana karakteristik teknologi mampu memenuhi kebutuhan dari karakteristik tugas yang dikerjakan. Dalam penelitiannya, Gama et al. (2021) membuktikan bahwa kecocokan ini akan mendorong pemanfaatan teknologi yang lebih optimal, yang pada akhirnya meningkatkan prestasi atau kinerja individu. Jika dikaitkan dengan konteks audit, auditor yang merasa bahwa AI dan GAS sangat sesuai dengan kebutuhan tugas mereka dalam mendeteksi kecurangan, akan memiliki tingkat keberhasilan yang lebih tinggi dalam mengungkap *fraud*.

Selain itu, teknologi juga berkaitan dengan bagaimana individu merespons dan menerima kehadiran alat tersebut. Sihite & Rahmah (2025) menambahkan bahwa dalam organisasi pemerintahan, kesesuaian tugas-teknologi pada aplikasi keuangan sangat krusial dalam meningkatkan kinerja aparatur. Teknologi tidak boleh menjadi beban, melainkan harus menjadi solusi yang mempermudah alur

kerja. Begitu pula dalam dunia pendidikan, Yani (2024) mencatat bahwa AI dapat meningkatkan wawasan dan produktivitas mahasiswa jika dimanfaatkan dengan benar, namun bisa melemahkan kemampuan berpikir jika terjadi ketergantungan yang berlebihan. Hal ini memberikan pelajaran bagi auditor bahwa meskipun teknologi sangat membantu dalam Deteksi *fraud*, keterampilan intelektual dan penilaian profesional auditor tetap menjadi nahkoda utama dalam proses tersebut.

Fenomena dan literatur yang telah dipaparkan di atas menunjukkan adanya urgensi yang mendalam untuk meneliti kembali bagaimana alat-alat modern ini berinteraksi dalam satu bingkai kerja audit. Masih terdapat kesenjangan dalam literatur mengenai bagaimana AI, GAS, dan *Cybersecurity Client* bekerja secara simultan dalam meningkatkan kemampuan Deteksi *fraud*, terutama di tengah dinamika serangan siber yang kian masif di Indonesia. Ketiga variabel teknologi ini bukan merupakan elemen yang berdiri sendiri, melainkan ekosistem digital yang saling mendukung: AI untuk analisis cerdas, GAS untuk pengolahan data masif, dan *Cybersecurity Client* untuk menjamin keamanan dan keabsahan seluruh proses tersebut.

Urgensi Deteksi *fraud* di Indonesia juga semakin meningkat seiring dengan kompleksitas skema kecurangan yang terjadi di era digital. Berdasarkan laporan terbaru dari Survei Fraud Indonesia Survei Fraud Indonesia (2025) yang dirilis oleh *Association of Certified Fraud Examiners* (ACFE) Indonesia Chapter, korupsi masih menempati posisi teratas sebagai jenis kecurangan yang paling merugikan dengan persentase mencapai 47,6%, diikuti oleh penyalahgunaan aset dan kecurangan laporan keuangan. Laporan tersebut juga mengungkapkan bahwa rata-rata kerugian per kasus di Indonesia sangat signifikan, yakni berada pada rentang Rp1 miliar hingga Rp50 miliar.

Meskipun dampak kerugiannya sangat besar, metode pendeteksian melalui audit internal dan eksternal masih menghadapi tantangan besar. Data SFI 2025 menunjukkan bahwa Deteksi *fraud* masih sangat bergantung pada sistem pengaduan (*whistleblowing system*), sementara peran audit dalam mendeteksi

kecurangan secara mandiri masih perlu ditingkatkan melalui pemanfaatan teknologi informasi. Dalam kondisi data transaksi yang masif (*big data*), penggunaan metode sampling konvensional tidak lagi memadai. Oleh karena itu, integrasi Artificial Intelligence (AI**)** untuk deteksi anomali otomatis, penggunaan Generalized Audit Software (GAS) untuk analisis populasi data secara menyeluruh, serta dukungan Cybersecurity Client untuk menjamin integritas bukti digital menjadi kunci utama bagi auditor di Kantor Akuntan Publik (KAP), khususnya di wilayah Jakarta, untuk meningkatkan rasio keberhasilan Deteksi *fraud*.

Berdasarkan latar belakang masalah yang kompleks dan multidimensional tersebut, peneliti merasa sangat penting untuk melakukan kajian lebih mendalam guna memberikan bukti empiris mengenai sejauh mana teknologi-teknologi ini memberikan dampak nyata di lapangan. Oleh karena itu, penelitian ini diberi judul: **"Pengaruh Persepsi Penggunaan Artificial Intelligence, Generalized Audit Software, dan Cybersecurity Client Terhadap Deteksi Fraud"**.

1.2 RUMUSAN MASALAH

1. Apakah Persepsi Penggunaan *Artificial Intelligence* (AI) berpengaruh terhadap Deteksi *fraud* bagi auditor eksternal di KAP Jakarta?
2. Apakah *Generalized Audit Software* (GAS) berpengaruh terhadap Deteksi *fraud* bagi auditor eksternal di KAP Jakarta?
3. Apakah *Cybersecurity Client* yang dimiliki berpengaruh terhadap Deteksi *fraud* bagi auditor eksternal di KAP Jakarta?

1.3 TUJUAN PENELITIAN

Penelitian ini bertujuan untuk menguji hubungan antara variabel independen, yaitu Persepsi Penggunaan *Artificial Intelligence* (AI), *Generalized Audit Software* (GAS), dan *Cybersecurity Client* dengan variabel dependen yaitu Deteksi *fraud*. Selain itu, penelitian ini juga bertujuan untuk menyajikan bukti empiris mengenai

pengaruh variabel-variabel tersebut terhadap Deteksi *fraud* bagi auditor eksternal di KAP Jakarta

1.4 MANFAAT PENELITIAN

a. Manfaat Praktis

Penelitian ini diharapkan dapat memberikan masukan bagi auditor, kantor akuntan publik, dan instansi pemerintahan mengenai pentingnya pemanfaatan teknologi audit digital dalam meningkatkan Deteksi fraud. Hasil penelitian ini juga dapat menjadi pertimbangan dalam meningkatkan kompetensi auditor di era digital.

b. Manfaat Kebijakan

Penelitian ini diharapkan dapat menjadi bahan pertimbangan bagi regulator dan pembuat kebijakan dalam menyusun standar atau pedoman terkait penerapan teknologi audit dan sistem keamanan siber guna mendukung pencegahan dan Deteksi fraud secara lebih efektif.