BAB II
KAJIAN PUSTAKA

2.1 Task-Technology Fit (TTF)

Teori *Task-Technology Fit* (TTF) yang dikemukakan oleh menjadi fondasi intelektual utama dalam penelitian ini. Menurut Gama et al. (2021), kinerja seorang individu dalam lingkungan digital tidak hanya ditentukan oleh seberapa canggih teknologi yang digunakan, melainkan oleh "kecocokan" antara karakteristik teknologi tersebut dengan karakteristik tugas yang harus diselesaikan. Dalam studi akuntansi, tugas seorang auditor adalah mengidentifikasi risiko dan mendeteksi anomali. Oleh karena itu, teknologi seperti AI dan GAS harus memiliki fungsionalitas yang selaras dengan prosedur audit tersebut.

Model *Task-Technology Fit* (TTF) yang dikemukakan oleh Goodhue dan Thompson (1995) merupakan kerangka teoretis yang menekankan bahwa kesuksesan pemanfaatan sistem informasi tidak hanya bergantung pada kualitas teknologi itu sendiri, melainkan pada sejauh mana kemampuan teknologi tersebut selaras (*fit*) dengan tugas yang harus diselesaikan oleh penggunanya. Dalam konteks penelitian audit digital, model ini menjelaskan bahwa Deteksi *fraud* sangat bergantung pada sinkronisasi antara kompleksitas tugas audit dengan kapabilitas teknologi yang digunakan.

Goodhue dan Thompson (1995) merinci bahwa terdapat tiga faktor utama yang saling berinteraksi dan menentukan tingkat keberhasilan dalam model TTF, yang dalam penelitian ini dijabarkan sebagai berikut:

1. Karakteristik Tugas (*Task Characteristics*)

Karakteristik tugas didefinisikan sebagai tindakan yang dilakukan oleh individu dalam mengubah masukan (*input*) menjadi keluaran (*output*) untuk memenuhi tanggung jawab profesinya. Dalam dunia audit, karakteristik tugas

mencakup keragaman tugas, tingkat kesulitan dalam pengumpulan bukti audit, serta kompleksitas transaksi yang diperiksa.

Sejalan dengan temuan Survei Fraud Indonesia (2025), tugas auditor saat ini menghadapi tantangan besar berupa skema korupsi dan transaksi fiktif yang dilakukan secara sistematis. Tugas pengumpulan bukti audit digital memerlukan ketelitian ekstra karena data tidak lagi berbentuk fisik, melainkan tersimpan dalam basis data yang masif (*big data*). Semakin tinggi tingkat ketidakpastian dan kompleksitas data klien, maka semakin besar kebutuhan auditor akan teknologi yang mampu menyederhanakan proses analisis tersebut. Oleh karena itu, karakteristik tugas dalam Deteksi *fraud* menuntut adanya prosedur audit yang tidak lagi bersifat manual, melainkan harus berbasis teknologi untuk menekan risiko deteksi.

2. Karakteristik Teknologi (*Technology Characteristics*)

Karakteristik teknologi merujuk pada fitur-fitur, kapabilitas, dan fungsionalitas yang dimiliki oleh suatu sistem informasi untuk mendukung penyelesaian tugas penggunanya. Dalam penelitian ini, karakteristik teknologi direpresentasikan oleh tiga variabel utama:

a. Persepsi Penggunaan Artificial Intelligence (AI): Memiliki karakteristik berupa algoritma cerdas yang mampu melakukan pembelajaran mandiri (*machine learning*), deteksi anomali secara otomatis, dan analisis pola hubungan (*Social Network Analysis*) yang tidak dapat dilakukan oleh manusia secara manual.
b. Generalized Audit Software (GAS): Memiliki karakteristik berupa kemampuan pemrosesan data dalam jumlah besar secara instan, pengujian populasi secara menyeluruh (100%), dan fungsi kalkulasi matematis yang sangat akurat.
c. Sistem Keamanan (*Cybersecurity Client*): Memiliki karakteristik berupa jaminan integritas data, enkripsi jalur akses, dan perlindungan bukti digital dari manipulasi pihak luar.

Kecocokan terjadi apabila fitur-fitur otomatisasi dan keamanan ini mampu menjawab kebutuhan auditor dalam mengatasi kesulitan pengumpulan bukti digital. Teknologi yang memiliki karakteristik canggih namun tidak relevan dengan kebutuhan tugas auditor tidak akan memberikan nilai tambah dalam Deteksi *fraud*.

3. Karakteristik Individu (*Individual Characteristics*)

Karakteristik individu berkaitan dengan kapasitas, pengetahuan, pengalaman, dan literasi teknologi yang dimiliki oleh auditor dalam mengoperasikan teknologi tersebut. Goodhue dan Thompson (1995) menyatakan bahwa meskipun teknologi sangat canggih dan tugas sangat kompleks, efektivitas sistem tetap bergantung pada kompetensi penggunanya.

Dalam konteks KAP di Jakarta, karakteristik individu auditor eksternal menjadi krusial. Seorang auditor dituntut untuk tidak hanya memiliki pengetahuan akuntansi dan audit, tetapi juga memiliki kemampuan teknis (*IT skill*) untuk mengoperasikan GAS, memahami *output* dari AI, serta memahami protokol keamanan siber saat berkoordinasi dengan tim IT klien. Auditor yang memiliki literasi teknologi yang tinggi akan lebih mampu memanfaatkan fitur-fitur teknologi secara optimal untuk membongkar skema kecurangan yang rumit. Dengan demikian, kapasitas individu berperan sebagai jembatan yang memastikan bahwa potensi teknologi (AI dan GAS) benar-benar dapat diimplementasikan untuk menyelesaikan tugas Deteksi kecurangan sesuai dengan standar SFI 2025.

2.2 Persepsi Penggunaan Artificial Intelligence (AI) dalam Audit

Persepsi Penggunaan Artificial Intelligence (AI) merupakan penilaian, keyakinan, atau pandangan auditor terhadap penggunaan teknologi Artificial Intelligence dalam mendukung pelaksanaan proses audit. Persepsi tersebut menggambarkan sejauh mana auditor meyakini bahwa AI mampu memberikan manfaat, meningkatkan efisiensi pekerjaan, mempermudah proses analisis data, serta membantu auditor dalam mengidentifikasi indikasi fraud. Dalam penelitian ini, yang menjadi fokus bukanlah kemampuan teknologi Artificial Intelligence

secara langsung, melainkan persepsi auditor terhadap penggunaan teknologi tersebut dalam pelaksanaan audit. Semakin positif persepsi auditor terhadap penggunaan AI, maka semakin besar kecenderungan auditor untuk memanfaatkan teknologi tersebut sebagai alat pendukung dalam meningkatkan kualitas proses audit dan menghasilkan bukti audit yang lebih andal.

Artificial Intelligence merupakan salah satu bentuk perkembangan teknologi digital yang mampu meniru kemampuan kognitif manusia melalui proses pembelajaran (*machine learning*), pengenalan pola (*pattern recognition*), analisis data, dan pengambilan keputusan berdasarkan informasi yang tersedia Qatawneh, (2024). Dalam bidang audit, AI dimanfaatkan untuk membantu auditor melakukan analisis terhadap data dalam jumlah besar (*big data*), mengidentifikasi transaksi yang bersifat tidak normal (*anomaly detection*), mengevaluasi pola risiko, serta menghasilkan informasi yang dapat digunakan auditor sebagai dasar dalam pengambilan keputusan audit. Berbeda dengan prosedur audit konvensional yang masih banyak mengandalkan teknik pengujian berbasis sampel, penggunaan AI memungkinkan auditor melakukan analisis terhadap seluruh populasi data sehingga potensi kesalahan maupun indikasi fraud dapat diidentifikasi secara lebih cepat dan akurat (Qatawneh, 2024).

Menurut teori *Task-Technology Fit (TTF)* yang dikemukakan oleh Goodhue dan Thompson (1995), suatu teknologi akan memberikan dampak terhadap peningkatan kinerja apabila teknologi tersebut sesuai dengan karakteristik tugas yang dikerjakan oleh penggunanya. Dalam konteks audit eksternal, auditor memiliki tugas untuk memperoleh bukti audit yang cukup dan tepat, melakukan analisis terhadap transaksi keuangan, mengevaluasi risiko salah saji material, serta mengidentifikasi adanya indikasi fraud. Oleh karena itu, apabila auditor memiliki persepsi bahwa penggunaan Artificial Intelligence mampu mendukung pelaksanaan tugas-tugas tersebut secara lebih efektif, maka auditor akan lebih terdorong untuk memanfaatkan teknologi tersebut dalam proses audit. Dengan demikian, persepsi penggunaan AI menjadi salah satu faktor yang dapat meningkatkan efektivitas

pelaksanaan audit, khususnya dalam mendukung proses deteksi fraud (Goodhue dan Thompson, 1995 & Mawlidy et al., 2024).

Dalam konteks Deteksi Fraud, pemanfaatan Artificial Intelligence memberikan peluang bagi auditor untuk meningkatkan efektivitas proses audit melalui kemampuan analisis data yang lebih cepat, akurat, dan menyeluruh. Artificial Intelligence mampu mengolah data transaksi dalam jumlah besar (*big data*), mengidentifikasi pola transaksi yang tidak biasa (*anomaly detection*), serta membantu auditor dalam mengenali indikasi kecurangan yang sulit ditemukan melalui prosedur audit konvensional berbasis pengujian sampel. Kemampuan tersebut memungkinkan auditor memperoleh informasi yang lebih relevan dalam mengevaluasi risiko dan menentukan prosedur audit lanjutan sehingga proses Deteksi Fraud dapat dilakukan secara lebih efektif.

Penelitian yang dilakukan oleh Qatawneh, (2024) juga menunjukkan bahwa penerapan Artificial Intelligence dalam Sistem Informasi Akuntansi memberikan kontribusi positif terhadap peningkatan efektivitas Deteksi Fraud karena mampu melakukan analisis data secara otomatis dan menghasilkan informasi yang mendukung pengambilan keputusan auditor.

Meskipun Artificial Intelligence menawarkan berbagai manfaat dalam proses audit, implementasinya pada Kantor Akuntan Publik di Indonesia masih menghadapi berbagai tantangan. Penerapan teknologi AI belum dilakukan secara merata karena dipengaruhi oleh kesiapan sumber daya manusia, biaya investasi teknologi, ketersediaan infrastruktur digital, serta kemampuan organisasi dalam mengintegrasikan AI ke dalam prosedur audit. Kondisi tersebut menyebabkan persepsi auditor terhadap penggunaan Artificial Intelligence menjadi faktor yang penting untuk diperhatikan, karena persepsi yang positif akan mendorong auditor untuk menerima dan memanfaatkan teknologi tersebut sebagai alat pendukung dalam pelaksanaan audit sehingga mampu meningkatkan efektivitas Deteksi Fraud menurut (Mawlidy et al., 2024).

Berdasarkan uraian tersebut, dapat dipahami bahwa keberhasilan penerapan Artificial Intelligence dalam proses audit tidak hanya ditentukan oleh kecanggihan teknologi yang digunakan, tetapi juga oleh persepsi auditor terhadap manfaat penggunaan teknologi tersebut. Auditor yang memiliki persepsi positif terhadap penggunaan Artificial Intelligence cenderung lebih terbuka dalam memanfaatkan teknologi untuk mendukung analisis data, mengidentifikasi anomali transaksi, serta memperoleh bukti audit yang lebih andal. Oleh karena itu, persepsi penggunaan Artificial Intelligence dipandang sebagai salah satu faktor yang dapat mendukung efektivitas auditor dalam melaksanakan proses Deteksi Fraud.

2.3 Generalized Audit Software (GAS)

Generalized Audit Software (GAS) adalah perangkat lunak yang dirancang untuk membantu auditor melakukan fungsi audit secara langsung pada data elektronik klien. Darono (2011) memaparkan bahwa penggunaan GAS adalah solusi wajib ketika auditor menghadapi lingkungan *Paperless* (tanpa kertas). Tanpa GAS, auditor hanya bisa melakukan pengecekan secara manual yang rentan terhadap kesalahan (*human error*) dan keterbatasan sampel.

Menurut Darono (2011), GAS memungkinkan auditor untuk melakukan:

1. Ekstraksi Data: Mengambil data langsung dari basis data tanpa mengubah data asli.
2. Analisis Stratifikasi: Mengelompokkan data berdasarkan rentang nilai tertentu untuk melihat penyimpangan.
3. Identifikasi Duplikasi: Mencari nomor faktur atau nominal yang sama yang sering menjadi indikasi korupsi atau *fraud*. Dengan kemampuan ini, GAS secara langsung meningkatkan akurasi dalam penyusunan laporan reviu keuangan pemerintah maupun swasta, sehingga peluang untuk mengungkapkan *fraud* menjadi jauh lebih tinggi (Darono 2011).

Generalized Audit Software memungkinkan auditor melakukan pengujian terhadap seluruh populasi data, mengidentifikasi transaksi yang tidak wajar, serta

menemukan pola penyimpangan yang berpotensi mengarah pada fraud. Oleh karena itu, penggunaan GAS menjadi salah satu teknologi yang mampu meningkatkan efektivitas auditor dalam melakukan deteksi fraud **(**Darono 2011**).**

2.4 *Cybersecurity Client*

Cybersecurity Client merupakan kemampuan organisasi dalam melindungi sistem informasi, jaringan, serta data keuangan dari berbagai ancaman siber yang dapat mengganggu kerahasiaan, integritas, dan ketersediaan informasi. Dalam konteks audit eksternal, keamanan siber klien menjadi salah satu aspek penting karena auditor sangat bergantung pada keandalan data yang diberikan oleh klien selama proses audit Samudra et al. (2023) mengingatkan bahwa tindak pidana siber terus berkembang dengan teknik yang semakin canggih, mengeksploitasi kelemahan sistem informasi untuk mencuri atau memanipulasi data. Di Indonesia, ancaman ini sangat nyata dengan jutaan insiden serangan siber setiap tahunnya yang mengancam kinerja bisnis dan reputasi (Samudra et al. ,2023)

Yulie & Mukhtaruddin (2026) menekankan bahwa profesi akuntan kini harus bertransformasi menjadi pengawas risiko siber. Penggunaan sistem berbasis *cloud* memang efisien, namun sangat rentan jika tidak dibarengi dengan pengendalian internal yang kuat. Sibarani et al. (2025) melalui *Systematic Literature Review* menjelaskan bahwa *Cybersecurity Client Accounting* adalah bentuk integrasi keamanan siber ke dalam praktik akuntansi untuk menjamin bahwa laporan keuangan bebas dari intervensi pihak luar. Jika sistem keamanan lemah, maka bukti digital Deteksi *fraud* bisa dengan mudah dihapus atau diubah oleh pelaku, sehingga keamanan siber merupakan syarat mutlak dalam audit modern (Sibarani et al. ,2025 & Yulie & Mukhtaruddin, 2026).

Dalam konteks audit eksternal, variabel *Cybersecurity Client* dalam penelitian ini didefinisikan sebagai persepsi auditor atas keandalan infrastruktur keamanan siber milik klien. Hal ini mencakup kemudahan akses data yang aman, integritas sistem penyimpanan klien, serta efektivitas koordinasi teknis antara

auditor dengan tim IT klien. Keamanan siber klien yang mumpuni bertindak sebagai *enabler* (pendukung) bagi auditor untuk mengimplementasikan AI dan GAS secara optimal tanpa hambatan teknis atau risiko manipulasi data oleh pihak internal klien.

Dalam penelitian ini, *Cybersecurity Client* didefinisikan sebagai persepsi auditor terhadap kemampuan sistem keamanan siber yang dimiliki klien dalam menjaga kerahasiaan, integritas, dan ketersediaan data audit. Sistem keamanan siber yang baik akan meminimalkan risiko manipulasi data, kehilangan informasi penting, maupun akses oleh pihak yang tidak berwenang. Dengan tersedianya data yang aman dan andal, auditor dapat melaksanakan prosedur audit secara lebih efektif, memperoleh bukti audit yang lebih berkualitas, serta meningkatkan kemampuan dalam melakukan Deteksi Fraud. Oleh karena itu, *Cybersecurity Client* dipandang sebagai salah satu faktor yang dapat mendukung efektivitas proses audit di era digital (Sibarani et al. , 2025 & Yulie & Mukhtaruddin, 2026).

2.5 Teori dan Deteksi *Fraud*

Deteksi Fraud merupakan proses yang dilakukan auditor untuk mengidentifikasi, menemukan, dan mengevaluasi adanya indikasi kecurangan yang dapat menyebabkan salah saji material dalam laporan keuangan. Dalam pelaksanaan audit, Deteksi Fraud dilakukan melalui serangkaian prosedur audit yang bertujuan memperoleh bukti audit yang cukup dan tepat sehingga auditor dapat menilai apakah terdapat indikasi kecurangan yang memerlukan investigasi lebih lanjut. Menurut SA 240, auditor bertanggung jawab untuk memperoleh keyakinan memadai bahwa laporan keuangan bebas dari salah saji material yang disebabkan oleh fraud maupun kesalahan, meskipun auditor tidak bertanggung jawab menjamin seluruh bentuk fraud dapat ditemukan. Oleh karena itu, kemampuan auditor dalam melakukan Deteksi Fraud menjadi bagian penting dalam menjaga kualitas dan kredibilitas proses audit. (Karyono, 2002)

Fraud merupakan tindakan yang dilakukan secara sengaja oleh individu maupun kelompok melalui penyalahgunaan wewenang, manipulasi informasi, atau bentuk penipuan lainnya untuk memperoleh keuntungan tertentu sehingga menimbulkan kerugian bagi pihak lain. Menurut Karyono (2002), proses Deteksi Fraud bukan merupakan pekerjaan yang sederhana karena auditor harus mampu mengenali berbagai karakteristik kecurangan, mengevaluasi area yang memiliki risiko tinggi, serta menggunakan prosedur audit yang sesuai agar indikasi fraud dapat ditemukan secara efektif. Oleh karena itu, auditor dituntut memiliki pengetahuan, pengalaman, dan profesionalisme dalam mengevaluasi bukti audit sehingga mampu membedakan antara kesalahan (*error*) dan kecurangan (*fraud*) menurut (Ambarwati et al., 2023).

Perkembangan teknologi informasi telah mengubah cara auditor melakukan Deteksi Fraud. Jika sebelumnya auditor lebih banyak menggunakan pengujian berbasis sampel secara manual, saat ini proses audit didukung oleh berbagai teknologi yang memungkinkan analisis data dilakukan terhadap seluruh populasi transaksi. Pemanfaatan teknologi tersebut membantu auditor mengidentifikasi pola transaksi yang tidak biasa, mengevaluasi risiko, serta memperoleh bukti audit yang lebih cepat dan akurat. Namun demikian, penggunaan teknologi hanya berperan sebagai alat bantu, sedangkan keputusan profesional mengenai adanya indikasi fraud tetap berada pada auditor berdasarkan hasil evaluasi terhadap bukti audit yang diperoleh.

Selain menggunakan Task-Technology Fit sebagai landasan utama penelitian, penelitian ini juga mengacu pada Fraud Hexagon sebagai teori pendukung untuk memahami berbagai faktor yang mendorong terjadinya fraud. Menurut Rianggi & Novita,(2023), Fraud Hexagon terdiri atas enam elemen yaitu stimulus (*pressure*), capability, collusion, opportunity, rationalization, dan ego. Keenam elemen tersebut menjelaskan berbagai kondisi yang dapat mendorong individu melakukan kecurangan sehingga dapat menjadi perhatian auditor dalam melakukan penilaian risiko dan Deteksi Fraud. Namun demikian, penelitian ini tidak menganalisis faktor penyebab fraud berdasarkan Fraud Hexagon, melainkan

menggunakan teori tersebut sebagai dasar dalam memahami karakteristik fraud yang perlu diwaspadai auditor selama proses audit.

Ketepatan mendeteksi fraud menunjukkan kemampuan auditor dalam mengidentifikasi adanya indikasi kecurangan secara akurat. Kecepatan proses investigasi mencerminkan kemampuan auditor dalam merespons dan menindaklanjuti temuan fraud secara efisien. Sementara itu, validitas bukti digital menggambarkan tingkat keandalan dan kekuatan bukti yang diperoleh auditor dalam mendukung pembuktian kecurangan. Ketiga indikator tersebut digunakan karena mampu merepresentasikan efektivitas auditor dalam mengungkap fraud pada lingkungan audit yang semakin terdigitalisasi.

Untuk memahami berbagai faktor yang dapat memicu terjadinya fraud, penelitian ini juga mengacu pada teori Fraud Hexagon. Menurut Rianggi & Novita (2023) Fraud Hexagon terdiri atas enam elemen yaitu *stimulus (pressure), capability, collusion, opportunity, rationalization, dan ego* yang digunakan untuk menjelaskan faktor-faktor yang mendorong terjadinya kecurangan. Dalam penelitiannya ditemukan bahwa beberapa komponen Fraud Hexagon, yaitu stimulus, opportunity, rationalization, dan ego berpengaruh signifikan terhadap terjadinya fraudulent financial statement.

Berdasarkan uraian tersebut, dapat dipahami bahwa Deteksi Fraud merupakan salah satu tanggung jawab penting auditor dalam memperoleh keyakinan memadai atas kewajaran laporan keuangan. Keberhasilan proses Deteksi Fraud tidak hanya dipengaruhi oleh kompetensi auditor, tetapi juga didukung oleh pemanfaatan teknologi audit yang sesuai dengan kebutuhan tugas auditor. Oleh karena itu, penelitian ini menggunakan variabel Persepsi Penggunaan Artificial Intelligence, Generalized Audit Software, dan Cybersecurity Client untuk menganalisis faktor-faktor yang dapat mendukung efektivitas auditor dalam melakukan Deteksi Fraud.

Meskipun demikian, fokus penelitian ini bukan untuk menganalisis penyebab terjadinya fraud berdasarkan komponen Fraud Hexagon, melainkan untuk mengkaji bagaimana Persepsi Penggunaan *Artificial Intelligence* (AI)**,** *Generalized Audit Software* (GAS)**,** dan *Cybersecurity Client* dapat membantu auditor dalam melakukan Deteksi Fraud. Oleh karena itu, Fraud Hexagon digunakan sebagai teori pendukung untuk memahami karakteristik dan indikator fraud yang dapat menjadi perhatian auditor dalam proses Deteksi Fraud. Pemanfaatan teknologi seperti Artificial Intelligence (AI) dan Generalized Audit Software (GAS) diharapkan mampu membantu auditor dalam mengidentifikasi pola transaksi yang tidak wajar, menganalisis data secara lebih menyeluruh, serta mendukung proses Deteksi Fraud menurut (Ambarwati et al., 2023).

Dengan demikian, Deteksi Fraud dalam audit modern tidak hanya dipengaruhi oleh pemahaman auditor terhadap karakteristik fraud, tetapi juga didukung oleh pemanfaatan teknologi audit yang memadai. Kombinasi antara pemahaman teoritis dan penggunaan teknologi tersebut diharapkan dapat membantu auditor eksternal memenuhi tanggung jawab profesionalnya sebagaimana diatur dalam SA 240 serta meningkatkan efektivitas pelaksanaan Deteksi Fraud.

2.6 Penelitian Terdahulu

No	Peneliti & Tahun	Judul Penelitian	Variabel	Hasil Penelitian
1	Qatawneh (2024)	*The role of artificial intelligence in auditing and fraud detection...*	AI (X1), Fraud Detection (Y), NLP (Moderator)	Menemukan bahwa AI memiliki pengaruh signifikan terhadap efektivitas audit dan deteksi fraud. Kehadiran NLP memperkuat kemampuan AI dalam menganalisis

				data non-numerik.
2	Musfiroh dkk. (2024)	Evolusi Penelitian Accounting Fraud: Analisis Bibliometrik	Accounting Fraud (Y), AI & Big Data (X)	Melalui analisis bibliometrik, ditemukan tren peningkatan integrasi AI dalam riset fraud global sebagai respons atas kompleksitas kecurangan akuntansi modern.
3	Mawlidy dkk. (2024)	Kemampuan *Artifical Intelligence* Terhadap Pendeteksian *Fraud*: Studi Literatur	AI (X1), Integritas Data, Deteksi *Fraud* (Y)	Menegaskan bahwa AI adalah instrumen vital dalam memproses *big data* untuk mitigasi risiko fraud sambil tetap menjaga kerahasiaan data audit.
4	Sibarani dkk. (2025)	*Systematic Literature Review on Cybersecurity Client Accounting*	*Cybersecurity Client* (X3), Digital Accounting, Audit Integrity (Y)	Menyimpulkan bahwa *Cybersecurity Client* bukan lagi opsi, melainkan pondasi utama dalam akuntansi digital untuk menjamin keandalan bukti audit digital.

5	Darono (2011)	Penggunaan *Generalized Audit Software* (GAS) dalam Reviu Laporan Keuangan	GAS (X2), Transparansi, Akuntabilitas (Y)	Membuktikan bahwa GAS memungkinkan auditor pemerintah melakukan reviu yang lebih akurat pada sistem yang sudah tidak memiliki jejak fisik (paperless).
6	Atmawaty (2023)	Pengaruh Teknik Audit Berbantuan Komputer terhadap Efektivitas Audit	TABK/GAS (X2), Efektivitas Audit (Y)	Menunjukkan bahwa alat bantu komputer (GAS) secara langsung meningkatkan kemampuan auditor dalam mendeteksi salah saji material dan fraud.
7	Prayitno & Sinosi (2024)	Peran Pengendalian Internal Berbasis Teknologi	Pengendalian Digital (X), Fraud Detection (Y)	Menekankan bahwa pengendalian internal yang terdigitalisasi sangat efektif dalam menutup celah kecurangan dalam operasional perusahaan.
8	Antonio (2014)	*The impact of technology on audit quality*	Teknologi Audit (X), Kualitas Audit (Y)	Menemukan hubungan positif antara penggunaan teknologi audit dengan peningkatan kualitas hasil audit sehingga

				membantu auditor dalam mendeteksi indikasi kecurangan pada laporan keuangan.

2.7 Pengembangan Hipotesis

2.7.1 Persepsi Penggunaan Artificial Intelligence (AI) terhadap Deteksi *Fraud*

Persepsi Penggunaan Artificial Intelligence (AI) dalam proses audit merupakan penilaian auditor terhadap manfaat penggunaan teknologi AI dalam membantu pelaksanaan tugas audit, khususnya dalam mendukung proses Deteksi Fraud. Berdasarkan teori Task-Technology Fit (TTF) yang dikemukakan oleh Goodhue dan Thompson (1995), suatu teknologi akan memberikan dampak terhadap peningkatan kinerja apabila teknologi tersebut sesuai dengan karakteristik tugas yang dikerjakan oleh penggunanya. Dalam konteks audit, tugas auditor meliputi pengumpulan bukti audit, analisis transaksi, identifikasi anomali, serta penilaian risiko untuk mendeteksi adanya indikasi kecurangan. Oleh karena itu, apabila auditor memiliki persepsi bahwa penggunaan AI sesuai dengan kebutuhan tugas audit, maka pemanfaatan teknologi tersebut diharapkan dapat meningkatkan efektivitas proses Deteksi Fraud.

Penelitian yang dilakukan oleh Qatawneh (2024) menunjukkan bahwa pemanfaatan Artificial Intelligence dalam proses audit mampu meningkatkan kemampuan auditor dalam menganalisis data, mengidentifikasi transaksi yang tidak wajar, serta mendukung proses Deteksi Fraud secara lebih efektif. Sejalan dengan itu, Mawlidy et al. (2024) menjelaskan bahwa *Artificial Intelligence* memiliki kemampuan untuk mengolah *big data*, mengenali pola transaksi yang kompleks, dan membantu auditor dalam mengidentifikasi indikasi fraud yang sulit ditemukan melalui prosedur audit konvensional. Meskipun demikian, efektivitas penggunaan

AI tidak hanya ditentukan oleh kecanggihan teknologi, tetapi juga dipengaruhi oleh persepsi auditor terhadap manfaat penggunaan AI dalam mendukung pelaksanaan tugas audit.

Di Indonesia, perkembangan modus fraud yang semakin kompleks sebagaimana ditunjukkan dalam Survei Fraud Indonesia (2025) menuntut auditor untuk memanfaatkan teknologi yang mampu meningkatkan kualitas proses audit. Apabila auditor memiliki persepsi yang positif terhadap penggunaan Artificial Intelligence, maka auditor akan lebih terdorong untuk memanfaatkan teknologi tersebut dalam proses audit sehingga kemampuan auditor dalam melakukan Deteksi Fraud diharapkan semakin meningkat. Berdasarkan uraian tersebut, hipotesis pertama dalam penelitian ini adalah sebagai berikut.

H1: *Persepsi Penggunaan Artificial Intelligence* berpengaruh positif terhadap Deteksi *Fraud*.

2.7.2 Pengaruh *Generalized Audit Software* (GAS) terhadap Deteksi *Fraud*

Generalized Audit Software (GAS) seperti ACL, IDEA, atau ATLAS merupakan perangkat lunak yang dirancang khusus untuk membantu auditor dalam mengolah data elektronik langsung dari sistem klien. Keunggulan utama GAS adalah kemampuannya untuk melakukan pengujian terhadap 100% populasi data keuangan, sehingga menghilangkan risiko kegagalan deteksi yang sering terjadi akibat metode *sampling* konvensional.

Dalam konteks Survei Fraud Indonesia (2025) kerugian akibat fraud di Indonesia masih tergolong tinggi sehingga auditor dituntut mampu melakukan pemeriksaan secara lebih efektif. Generalized Audit Software (GAS) memungkinkan auditor melakukan berbagai prosedur audit seperti *gap testing*, *duplicate testing*, serta verifikasi transaksi terhadap seluruh populasi data secara lebih cepat dan akurat. Berdasarkan teori Task-Technology Fit (TTF), penggunaan teknologi yang sesuai dengan karakteristik tugas akan meningkatkan kinerja penggunanya Goodhue dan Thompson (1995). Oleh karena itu, apabila auditor

mampu memanfaatkan GAS sesuai dengan kebutuhan proses audit, maka kemampuan auditor dalam melakukan Deteksi Fraud akan semakin meningkat.

H2: *Generalized Audit Software* berpengaruh positif terhadap Deteksi *Fraud*.

2.7.3 Pengaruh *Cybersecurity Client* terhadap Deteksi *Fraud*

Variabel Cybersecurity Client dalam penelitian ini merupakan persepsi auditor terhadap kemampuan sistem keamanan siber yang dimiliki klien dalam menjaga kerahasiaan, integritas, dan ketersediaan data audit. Infrastruktur keamanan siber yang baik tidak hanya berfungsi melindungi data perusahaan dari serangan siber, tetapi juga meningkatkan kepercayaan auditor terhadap keandalan data yang digunakan dalam proses audit. Hal tersebut sejalan dengan penelitian Ismail Darmawan & Muharman Lubis (2024) yang menyatakan bahwa penerapan keamanan siber yang memadai menjadi salah satu faktor penting dalam menjaga kualitas informasi digital.

Keamanan siber klien yang baik akan membantu auditor memperoleh data audit yang lebih andal sehingga proses Deteksi Fraud dapat dilakukan secara lebih efektif. Berdasarkan Survei Fraud Indonesia (2025), perkembangan modus fraud yang semakin kompleks menyebabkan auditor membutuhkan data yang memiliki integritas tinggi agar hasil analisis tidak dipengaruhi oleh manipulasi data. Berdasarkan teori Task-Technology Fit (TTF), kesesuaian antara teknologi yang tersedia dengan kebutuhan tugas auditor akan meningkatkan efektivitas pelaksanaan audit Goodhue dan Thompson (1995). Oleh karena itu, apabila auditor memiliki persepsi bahwa sistem keamanan siber klien mampu menjaga keandalan data audit, maka auditor akan lebih mudah melakukan Deteksi Fraud secara tepat dan akurat.

H3: *Cybersecurity Client* berpengaruh positif terhadap Deteksi *Fraud*.

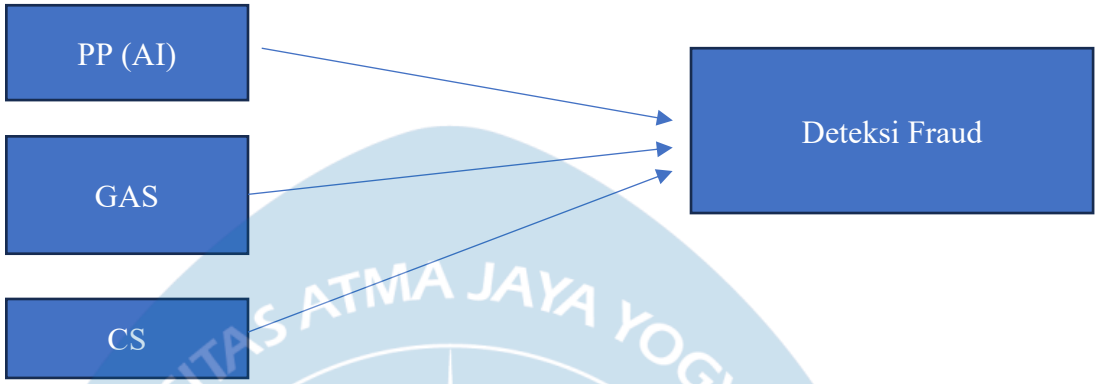
2.7.4 Pengaruh Simultan Persepsi Penggunaan AI, GAS, dan *Cybersecurity Client* terhadap Deteksi *Fraud*

Berdasarkan teori Task-Technology Fit (TTF), penggunaan teknologi akan memberikan manfaat yang optimal apabila teknologi tersebut sesuai dengan karakteristik tugas yang dilakukan oleh penggunanya Goodhue dan Thompson (1995). Dalam proses audit, Persepsi Penggunaan Artificial Intelligence (AI), Generalized Audit Software (GAS), dan Cybersecurity Client merupakan tiga faktor yang saling melengkapi dalam mendukung auditor melakukan Deteksi Fraud secara lebih efektif. AI membantu auditor dalam menganalisis pola transaksi dan mengidentifikasi anomali, GAS membantu auditor melakukan pengujian terhadap data secara menyeluruh, sedangkan Cybersecurity Client mendukung keandalan serta keamanan data yang digunakan dalam proses audit.

Ketiga variabel tersebut memiliki peran yang saling mendukung dalam meningkatkan efektivitas proses Deteksi Fraud. Artificial Intelligence membantu auditor mengidentifikasi pola transaksi yang tidak wajar, Generalized Audit Software mendukung pelaksanaan prosedur audit terhadap seluruh populasi data, sedangkan Cybersecurity Client membantu menjaga integritas, kerahasiaan, dan keandalan data audit. Apabila ketiga faktor tersebut dimanfaatkan secara bersamaan, auditor diharapkan mampu melakukan Deteksi Fraud secara lebih efektif. Kondisi ini juga sejalan dengan perkembangan praktik audit di era digital yang menuntut auditor memanfaatkan teknologi untuk menghadapi kompleksitas fraud yang semakin meningkat sebagaimana dilaporkan dalam (Survei Fraud Indonesia, 2025).

H4: *Persepsi Penggunaan Artificial Intelligence, Generalized Audit Software,* dan *Cybersecurity Client* berpengaruh positif secara simultan terhadap Deteksi *Fraud*

2.8 Kerangka Hipotesis



UNIVERSITAS ATMA JAYA YOGYAKARTA