ABNUS JOURNAL
Your Research Partner

Corelytics: Insights into Business & Accounting Systems (Corelytics)
E-ISSN: 3164-3337 | Vol. 1, No. 4 (2026) | pp. 225-242

# ACCOUNTGUARD AI as Continuous Accounting Intelligence for Early Revenue Fraud Detection in Cashless Companies

**Dea Wulandari[1*], Gabriel Natalia Chintyago[2], Jennifer Rosalind Setiawan[3]**

*Universitas Katolik Darma Cendika, Surabaya, Indonesia[1,2,3]*

***Corresponding author:** deawulandariii5@gmail.com |

Received: 1 September 2026 | Revised: 16 September 2026 | Revised: 14 October 2026 | Published: 6 November 2026

**Abstract**

**Purpose:** This study develops ACCOUNTGUARD AI (Accounting Continuous Intelligence for Revenue Fraud Detection), a continuous accounting intelligence model based on artificial intelligence designed to detect fraud early in the revenue cycle of digital companies operating in a cashless society.

**Research Methodology:** The study uses a conceptual design approach based on a literature review of the revenue cycle, fraud theory, continuous accounting and continuous auditing, artificial intelligence for fraud detection, and the digital payment ecosystem. The review is used to map fraud red flags at each revenue cycle stage and to design a model architecture and a conceptual dashboard prototype.

**Results:** The model consists of four layers, namely a Data Integration Layer, a Feature Engineering Layer, a Hybrid Fraud Detection Engine that combines rule based detection, unsupervised anomaly detection, supervised classification, and graph analytics into a risk score from 0 to 100, and a Human in the Loop Reporting and Escalation Layer. The model monitors every stage from sales order to refund and covers the entire transaction population in real time.

**Conclusions:** ACCOUNTGUARD AI has the potential to accelerate and improve the accuracy of early fraud detection while keeping auditors and management as the final decision makers.

**Limitations:** The model is conceptual and has not been tested with real or simulated transaction data, so its accuracy, cost efficiency, and false positive rate remain unmeasured.

**Contributions:** The study integrates artificial intelligence with revenue cycle controls and revenue recognition principles and offers guidance for companies, auditors, regulators, and system developers.

***Keywords:*** *Artificial Intelligence, Cashless Society, Continuous Accounting, Fraud Detection, Revenue Cycle*

**How to Cite:** Wulandari, D., Chintyago, G. N., & Setiawan, J. R. (2026). ACCOUNTGUARD AI as Continuous Accounting Intelligence for Early Revenue Fraud Detection in Cashless Companies. *Corelytics: Insights into Business & Accounting Systems (Corelytics)*, 1(4), 225-242.

## 1. Introduction

The development of information and communication technology has driven the digital transformation of the economy across many industries. Digitalization has changed not only the way people interact and transact but also the way companies create and capture economic value through their business models (Trischler & Li-Ying, 2023). Digital transformation reshapes organizational structures, value propositions, and operating processes, and it requires firms to adapt their control systems to new forms of data and new risks (Vial, 2019). Companies based on digital platforms, online marketplaces, financial technology, software as a service, and other internet based services have grown significantly as internet penetration and the adoption of digital technology in daily life have increased. This

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co | DOI:10.52909/corelytics.v1i4.468 

phenomenon is reinforced by the emergence of a cashless society in which most payments are made through electronic instruments rather than cash.

The growth of the cashless society has caused the volume of digital transactions to increase rapidly. Payment methods such as mobile banking, digital wallets, the Quick Response Code Indonesian Standard (QRIS), virtual accounts, electronic cards, and payment gateways have become central to modern economic activity. These instruments offer convenience, speed, and efficiency in business transactions (Narendrar et al., 2023). The broader fintech revolution has transformed payments, lending, and other financial services by combining innovation with new forms of disruption (Gomber et al., 2018), while digital finance has expanded access to financial services and supported financial inclusion (Ozili, 2018). However, the rising number and complexity of digital transactions also present new challenges for companies, particularly in maintaining the accuracy of financial records and the security of transactions that occur in real time (Moon et al., 2022).

In accounting, these changes directly affect the revenue cycle, which is the series of activities from receiving customer orders, billing, and collecting payments to recognizing revenue in the financial statements (Fahmi et al., 2022). In digital companies, the revenue cycle no longer runs in a simple and linear way but involves multiple integrated systems, such as transaction platforms, electronic payment systems, customer databases, and the accounting system. Internet related technologies have already reshaped the work of accountants by automating data capture and creating continuous streams of financial information (Moll & Yigitbasioglu, 2019). This complexity produces very large volumes of data that move at high speed, which increases the risk of errors and irregularities in revenue recording.

One of the main risks that arises is fraud in the revenue cycle. Fraud can take many forms, such as fictitious sales, manipulation of revenue recognition, channel stuffing, misuse of digital discounts and vouchers, refund fraud, duplicate invoices, and account takeover used to carry out illegal transactions (Abdallah et al., 2016). Unlike fraud in conventional systems, fraud in digital environments is often hidden among millions of transactions that appear normal, which makes it more difficult to detect quickly (West & Bhattacharya, 2016). As a result, companies may suffer financial losses, present unreliable financial statements, and lose the trust of investors and consumers. Research on publicly listed firms has shown that accounting fraud can remain undetected for years and that data driven methods can identify fraudulent firms more effectively than traditional ratio based models (Bao et al., 2020).

Fraud control has generally been carried out through periodic internal and external audits. These approaches still rely heavily on sampling, so only part of the transaction population is examined (Appelbaum et al., 2017). With digital transactions occurring twenty four hours a day without interruption, traditional audit methods become less effective because they are limited in their ability to detect anomalies quickly and comprehensively (Kokina & Davenport, 2017). Delays in identifying fraud mean that corrective action is often taken only after material losses have occurred. Companies therefore need oversight mechanisms that can operate continuously and in real time through continuous accounting or continuous auditing approaches (Zahirah et al., 2021).

The development of Artificial Intelligence (AI) offers great opportunities to meet this need. AI can process large volumes of data, recognize normal transaction patterns, perform predictive analysis, and detect anomalies automatically and in real time (Hilal et al., 2022). Technologies such as machine learning, deep learning, and graph analytics enable systems to identify high risk transactions, assign risk scores, and generate early warnings before fraud develops into significant losses (Ali et al., 2022). Various studies show that AI achieves higher accuracy than conventional detection methods in identifying complex and dynamic fraud patterns (Kim et al., 2019, Carcillo et al., 2021).

Nevertheless, the implementation of AI in accounting and revenue cycle oversight in Indonesia still faces various challenges. These include suboptimal data quality and integration, limited competence of accounting staff in understanding AI technology, high implementation costs, and the absence of a model that comprehensively integrates AI with the stages of the revenue cycle and with revenue recognition principles under financial accounting standards (Petcu et al., 2024). Concerns about the

transparency of AI decisions also make it difficult for auditors to rely on model outputs without understanding the reasoning behind them (Zhang et al., 2022). These conditions indicate a gap between the potential of AI and its application in accounting oversight practice in digital companies.

Based on these problems, a model is needed that can integrate artificial intelligence with accounting processes on a continuous basis to support the early detection of fraud in the revenue cycle. This study therefore proposes ACCOUNTGUARD AI (Accounting Continuous Intelligence for Revenue Fraud Detection), a continuous accounting intelligence model based on AI that is designed to be embedded in every stage of the revenue cycle of digital companies. The model is expected to monitor transactions in real time, detect fraud indications early, provide automatic risk warnings, and support the presentation of more reliable financial information in the cashless society.

This study addresses three research questions. The first concerns the characteristics and red flags of fraud that arise at each stage of the revenue cycle of digital companies in the cashless society. The second concerns how the ACCOUNTGUARD AI model should be designed as a continuous accounting intelligence framework based on AI for the early detection of revenue cycle fraud. The third concerns the effectiveness and implementation challenges of the model compared with conventional audit and internal control approaches. Accordingly, the study aims to identify fraud red flags in the revenue cycle of digital companies, to design ACCOUNTGUARD AI as an AI based continuous accounting intelligence solution, and to analyze its effectiveness and implementation challenges as an instrument for the early detection of fraud in digital financial transactions.

Theoretically, the study is expected to enrich forensic accounting and continuous auditing research by integrating the perspective of artificial intelligence into the revenue cycle framework. Practically, ACCOUNTGUARD AI is expected to serve as a reference for management, internal audit functions, regulators, and accounting information system developers in designing fraud detection systems that are more responsive, efficient, and reliable for companies operating in the digital economy and the cashless society.

## 2. Literature Review and Hypothesis/es Development

### *2.1 The Revenue Cycle*

The revenue cycle is a recurring set of business activities that starts with receiving customer orders and continues with credit approval, delivery of goods or provision of services or digital products, invoicing, cash collection, and the handling of returns and receivable adjustments (Fahmi et al., 2022). In digital companies, these stages are usually recorded automatically in Enterprise Resource Planning (ERP) systems, Point of Sale (POS) systems, payment gateways, and online marketplace platforms, so transaction data are available in real time but are also vulnerable to manipulation at the integration points between systems.

In conventional companies, most revenue cycle activities follow procedures that are relatively structured and easy to trace. Digital transformation, however, has made the revenue cycle more complex because it now involves multiple connected platforms and systems (Vial, 2019). Ordering, payment, and service delivery can be performed automatically through digital platforms without direct interaction between the company and its customers. In digital companies, transaction data are recorded automatically through ERP, POS, Customer Relationship Management (CRM) systems, payment gateways, mobile applications, and online marketplaces. The integration of these systems allows transactions to be processed in real time and generates very large volumes of data. While this increases operational efficiency, it also creates new risks in the form of data inconsistency, recording errors, and opportunities for manipulation at the integration points between systems (Moll & Yigitbasioglu, 2019).

Revenue recognition adds a further layer of complexity. Under *Pernyataan Standar Akuntansi Keuangan* (PSAK) 72, which adopts International Financial Reporting Standards (IFRS) 15 Revenue from Contracts with Customers, revenue must be recognized when or as the entity satisfies a

performance obligation by transferring promised goods or services to the customer (Ikatan Akuntan Indonesia, 2018). For digital companies that sell subscriptions, bundles, vouchers, and platform services, determining when performance obligations are satisfied requires accurate links between contract data, service usage data, and payment data. The complexity of the digital revenue cycle therefore makes manual verification increasingly difficult, and companies need monitoring mechanisms that can follow every stage of the cycle continuously to ensure that each recorded transaction reflects real economic activity.

### *2.2 Fraud Theory in the Digital Environment*

Fraud is a deliberate act carried out to obtain a benefit by violating rules or misleading other parties. One of the most widely used theories to explain the causes of fraud is the fraud triangle introduced by Donald Cressey, which states that fraud occurs because of three main factors, namely pressure, opportunity, and rationalization. Pressure may arise from financial needs, performance targets, organizational demands, or personal factors. Rationalization is the process by which perpetrators convince themselves that their actions are acceptable. Opportunity arises when weaknesses in internal control allow perpetrators to commit and conceal fraud.

As the business environment has evolved, the fraud triangle has been extended into the fraud diamond by adding capability, which explains that not every individual with pressure, opportunity, and rationalization will commit fraud because the act also requires certain abilities, such as understanding of the system, access to data, the ability to manipulate business processes, and the ability to hide traces. Later models such as the SCORE model further incorporate stimulus, capability, opportunity, rationalization, and ego to explain fraud in modern organizations (Vousinas, 2019). In digital business environments, the opportunity element becomes increasingly dominant because most transactions are processed automatically and in very large volumes. Weak internal controls, insufficient segregation of duties, uncontrolled system access, and the limited capacity of humans to oversee millions of transactions can create fraud opportunities that are difficult to detect with conventional methods (Petcu et al., 2024).

### *2.3 Continuous Accounting and Continuous Auditing*

Continuous accounting is an approach that emphasizes the recording, monitoring, and reporting of financial transactions on an ongoing basis and close to real time, without waiting for the end of an accounting period (Hidayati et al., 2023). This approach has developed alongside the increasing ability of information technology to automate business processes and generate continuous streams of transaction data. It differs from traditional accounting practice, which generally relies on monthly or annual closing processes. In continuous accounting, financial data are updated continuously so that the information available always reflects the current condition of the company, and management can obtain a more accurate picture of operational performance and financial position.

A concept closely related to continuous accounting is continuous auditing, which is the examination of transactions and internal controls carried out automatically using information technology (Zahirah et al., 2021). This approach allows auditors to receive early warnings when deviations, policy violations, or unusual transactions are identified. Big data and analytics have expanded the scope of the modern audit engagement by enabling auditors to analyze entire populations of transactions, combine structured and unstructured data, and apply predictive and prescriptive analytics (Appelbaum et al., 2017). Robotic process automation can further support audit tasks by automating repetitive procedures such as data extraction, reconciliation, and testing, which frees auditors to focus on judgment intensive work (Eulerich et al., 2022). Distributed ledger technologies have also been proposed as a foundation for continuous assurance because they provide tamper resistant, real time records of transactions (Dai & Vasarhelyi, 2017). In digital companies, continuous accounting and continuous auditing are particularly relevant because transactions take place twenty four hours a day, and anomalies can be identified immediately after they occur, so the risk of losses and reporting errors can be minimized from the start.

### *2.4 Artificial Intelligence for Fraud Detection*

Artificial Intelligence (AI) is a technology that enables computer systems to analyze, learn, and make decisions based on available data (Rifky, Kharisma, & Afendi, 2024). In accounting and auditing, AI is used to process large volumes of transaction data, identify behavioral patterns, and detect fraud indications automatically (Issa, Sun, & Vasarhelyi, 2016). Machine learning is one of the most widely used branches of AI. It allows systems to learn from historical transaction patterns and build models that distinguish normal transactions from potentially fraudulent ones, and its strength lies in its ability to adapt to changing transaction patterns without being manually reprogrammed (Asrul, Suryawan, Jana, & Mandias, 2025).

Several approaches are commonly used in fraud detection. Unsupervised learning methods such as Isolation Forest and clustering detect anomalies without requiring labeled fraud data, while supervised learning methods such as Gradient Boosting, Random Forest, and XGBoost classify transactions based on known fraud histories (Ali, Othman, Eisa, Al-Dhaqm, Nasser, Elhassan, Elshafie, & Saif, 2022; Hilal, Gadsden, & Yawney, 2022). Ensemble methods such as AdaBoost combined with majority voting have been shown to improve the detection of fraudulent card transactions (Randhawa, Loo, Seera, Lim, & Nandi, 2018), and hybrid architectures that combine ensemble models with deep learning have outperformed single models in large scale fraud detection systems (Kim, Lee, Shin, Yang, Cho, Nam, Song, Yoon, & Kim, 2019). Combining unsupervised and supervised learning is also effective because unsupervised scores capture novel behavior that supervised classifiers trained on past fraud may miss (Carcillo, Caelen, Kessaci, Oblé, & Bontempi, 2021). Deep learning methods for anomaly detection extend these capabilities to complex and high dimensional data (Pang, Shen, Cao, & van den Hengel, 2022).

AI has also introduced more advanced approaches such as graph analytics to identify suspicious relationships between accounts, customers, devices, and payment accounts, and natural language processing to analyze invoices, transaction notes, and digital communications for fraud indications that cannot be detected from numerical data alone. The quality of the input features is decisive for model performance, and research on card fraud has shown that aggregated and periodic behavioral features substantially improve detection results (Correa, Aouada, Stojanovic, & Ottersten, 2016). Realistic modeling must also consider class imbalance, the delayed availability of fraud labels, and the interaction between alerts and investigators, which shape how fraud detection systems perform in practice (Dal, Boracchi, Caelen, Alippi, & Bontempi, 2018). Recent reviews confirm that AI based fraud detection continues to evolve toward hybrid, adaptive, and explainable systems (Yang, Shukur, & Sahran, 2026).

### *2.5 The Cashless Society and the Digital Payment Ecosystem*

The cashless society refers to a condition in which people increasingly reduce their use of cash and shift to digital payment instruments such as QRIS, digital wallets, mobile banking, virtual accounts, debit cards, credit cards, and other electronic payment services (Moon et al., 2022). This development is driven by technological progress, increasing internet penetration, and changes in consumer behavior that prioritize convenience and speed. Consumer adoption of mobile payments depends on perceived usefulness, trust, and anxiety about security, which shows that the reliability and safety of payment systems are central to their continued use (Patil et al., 2020). AI and other Industry 4.0 technologies have further accelerated the growth of digital financial services by lowering costs and expanding access (Mhlanga, 2020).

For companies, the digital payment ecosystem offers benefits such as faster cash flows, lower transaction costs, more accurate recording, and easier integration with other business systems, since every transaction can be recorded automatically. However, the ecosystem also expands the attack surface because transactions pass through multiple connected platforms and payment service providers. Each integration point can become a source of errors, data manipulation, or system misuse if it is not properly monitored (Moon et al., 2022). The increasing volume of digital transactions also

makes reconciliation more complex, as companies must match transaction data from various payment channels within a short time to ensure the accuracy of revenue records. These conditions show that manual oversight is no longer adequate and that a technology based approach capable of automatic, continuous, and real time monitoring is required.

### *2.6 Explainability and Human Oversight in AI Based Control*

The use of AI in accounting control raises questions of transparency and accountability. Many machine learning models operate as black boxes whose internal reasoning is difficult to explain to auditors, managers, and regulators (Adadi & Berrada, 2018). Explainable artificial intelligence seeks to make model decisions understandable through techniques that reveal which features contribute to a given prediction, and it is increasingly regarded as a prerequisite for responsible AI (Barredo Arrieta et al., 2020). In tree based models such as Gradient Boosting and Random Forest, local explanation methods can attribute each prediction to specific input features and aggregate these attributions into global insights about model behavior (Lundberg et al., 2020). Explainable machine learning has been applied successfully in financial risk management to make credit decisions transparent for supervisors (Bussmann et al., 2021).

For high stakes decisions, some scholars argue that interpretable models should be preferred over post hoc explanations of black box models (Rudin, 2019). In auditing, explainability is necessary because auditors must document the basis of their conclusions and be able to defend them before regulators and courts (Zhang et al., 2022). Explainability and causability also affect user trust and acceptance of AI systems (Shin, 2021), and research on human trust in AI shows that both over reliance and under reliance on automated outputs can lead to poor decisions (Glikson & Woolley, 2020). The literature on human and AI collaboration suggests that the most effective arrangement combines the speed and consistency of AI with human intuition and contextual judgment (Jarrahi, 2018), and that organizations should balance automation with augmentation to avoid losing the expertise needed to question automated outputs (Raisch & Krakowski, 2021). Because fraud patterns change over time, models must also be monitored and retrained to cope with concept drift (Lu et al., 2019).

## 3. Research Methodology

This study uses a conceptual design approach. Rather than testing hypotheses with empirical data, it develops a model that integrates artificial intelligence with revenue cycle controls on the basis of a structured review of the literature. Conceptual design is appropriate when the aim is to propose a new framework that combines insights from several domains and to provide a foundation for later empirical testing. The research process consisted of five stages, which are illustrated in Figure 1.

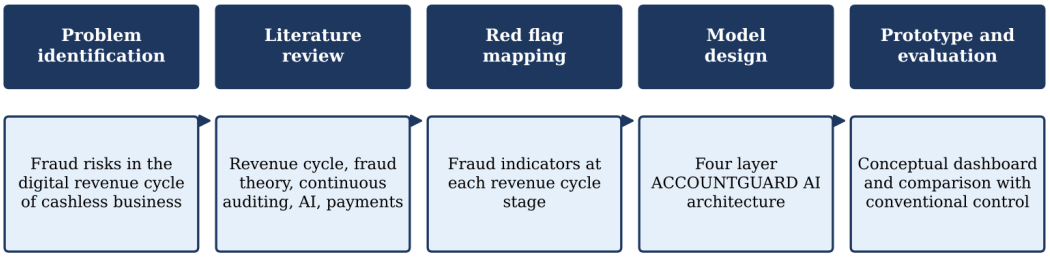



Figure 1. Research design for developing the ACCOUNTGUARD AI model

Figure 1 shows that the study moved from problem identification to literature review, red flag mapping, model design, and finally prototype development and evaluation. The first stage identified fraud risks in the revenue cycle of digital companies operating in the cashless society. The second stage reviewed literature on the revenue cycle, fraud theory, continuous accounting and auditing, AI for fraud detection, and digital payments, which provided the theoretical basis for the model. The third

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co | DOI:10.52909/corelytics.v1i4.468 

stage translated these insights into red flags for each revenue cycle stage, and the fourth stage designed the four layer architecture of ACCOUNTGUARD AI. The final stage developed a conceptual dashboard prototype and compared the model with conventional audit and internal control approaches, which together answer the three research questions of the study.

The literature review covered scientific journal articles, books, and accounting standards related to the themes of the study. Sources were selected based on their relevance to the research questions, with priority given to international journal articles published within the last ten years and indexed with active digital object identifiers. The main themes and representative sources used in the review are summarized in Table 1.

Table 1. Themes and representative sources of the literature review

| Theme | Focus | Representative Sources |
|---|---|---|
| Revenue cycle and digital business | Stages of the revenue cycle, digital transformation, and revenue recognition | Fahmi et al. (2022), Vial (2019), Trischler and Li-Ying (2023), Indonesia (2018) |
| Fraud theory | Fraud triangle, fraud diamond, and SCORE model | Vousinas (2019), Petcu et al. (2024) |
| Continuous accounting and auditing | Real time monitoring, big data audit, and automation | Appelbaum et al. (2017), Eulerich et al. (2022), Dai and Vasarhelyi (2017), Zahirah et al. (2021) |
| AI for fraud detection | Supervised, unsupervised, hybrid, and graph methods | West and Bhattacharya (2016), Carcillo et al. (2021), Hilal et al. (2022), Ali et al. (2022) |
| Digital payments | Cashless society, mobile payment adoption, and payment security | Gomber et al. (2018), Patil et al. (2020), Moon et al. (2022) |
| Explainability and oversight | Explainable AI, trust, and human and AI collaboration | Adadi and Berrada (2018), Lundberg et al. (2020), Zhang et al. (2022), Jarrahi (2018) |

Table 1 shows that the literature review drew on six interrelated themes that together form the conceptual basis of ACCOUNTGUARD AI. The revenue cycle and digital business theme defines the processes that the model must monitor, while fraud theory explains why digital environments create new opportunities for fraud. Continuous accounting and auditing provide the oversight philosophy of the model, and research on AI for fraud detection supplies the analytical techniques used in its detection engine. The digital payment theme describes the data sources and risks of the cashless ecosystem, and the explainability theme justifies the human in the loop design that keeps auditors in control of final decisions. The combination of these themes ensures that the model is grounded in both accounting and technology research rather than in a single discipline.

The analysis followed a thematic synthesis. Findings from the literature were grouped according to the stage of the revenue cycle they addressed, the type of fraud they described, and the detection technique they proposed. These groupings were then used to derive red flags for each revenue cycle stage, to define the features that the model should compute, and to determine the combination of detection techniques that would address both known and unknown fraud patterns. The resulting model was evaluated conceptually by comparing its characteristics with those of conventional audit and internal control approaches and by identifying the main challenges for implementation.

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co | DOI:10.52909/corelytics.v1i4.468 

## 4. Results and Discussions

### *4.1 Fraud Red Flags in the Digital Revenue Cycle*

The first research question concerns the characteristics and red flags of fraud at each stage of the revenue cycle of digital companies. The synthesis of the literature shows that each stage presents specific risks that can be translated into observable indicators. These red flags are summarized in Table 2.

Table 2. Fraud red flags at each stage of the digital revenue cycle

| Revenue Cycle Stage | Typical Fraud Schemes | Red Flags Monitored by the Model |
|---|---|---|
| Sales order and credit approval | Synthetic accounts, fictitious customers, account takeover | New customer profiles with unusual transaction patterns, sudden changes to customer data shortly before a transaction, many accounts sharing one device |
| Order fulfillment | Fictitious sales, channel stuffing | Sales without matching delivery or service usage records, unusual sales spikes near period end |
| Invoicing | Premature or manipulated revenue recognition, duplicate invoices | Invoices inconsistent with contracts or payment schedules, mismatches between service delivery dates and revenue recognition dates under PSAK 72 |
| Cash collection | Misappropriation, lapping, unexplained differences | Unreconciled differences between QRIS, digital wallet, virtual account, card, and bank transfer records |
| Returns and refunds | Refund fraud, voucher abuse, promotion misuse | High refund frequency, refunds without supporting documents, linked accounts repeatedly using vouchers |

Table 2 shows that fraud risk is present at every stage of the digital revenue cycle and that each stage requires different indicators. At the front of the cycle, the main risks relate to customer identity, such as synthetic accounts and account takeover, which can be detected through unusual profiles and device sharing. In the middle of the cycle, the risks shift toward fictitious sales and revenue recognition manipulation, which require the comparison of sales, delivery, and contract data. At the end of the cycle, cash collection and refunds present risks of misappropriation and promotion abuse that can be identified through automatic reconciliation and network analysis. This mapping shows that fraud detection cannot rely on a single indicator and that a model must integrate data from all stages to obtain a complete view of revenue risk.

These findings are consistent with the literature showing that fraud in digital environments is diverse and adaptive (Abdallah, Maarof, & Zainal, 2016; (West & Bhattacharya, 2016)). Account takeover and synthetic identities exploit the absence of physical interaction in digital transactions, while refund and voucher abuse exploit the generosity of promotional policies. Revenue recognition manipulation, on the other hand, reflects the pressure on management to meet growth targets, which is a classic element of the fraud triangle and its extensions (Vousinas, 2019). The variety of schemes underlines the need for a detection system that combines multiple techniques rather than relying on fixed rules alone.

### *4.2 The ACCOUNTGUARD AI Architecture*

The second research question concerns the design of the model. ACCOUNTGUARD AI is a continuous accounting intelligence model based on AI that is designed to monitor, analyze, and detect fraud early and continuously at all stages of the revenue cycle of digital companies. Unlike traditional audit approaches, which are periodic and retrospective, ACCOUNTGUARD AI operates in real time by using transaction data that flow continuously from the company's operational systems. The core

concept of the model is to integrate accounting processes, internal control, and AI into a single monitoring mechanism that runs automatically and continuously, so that every transaction is not only recorded as accounting data but also assessed for risk before it affects the financial statements. The architecture of the model is presented in Figure 2.

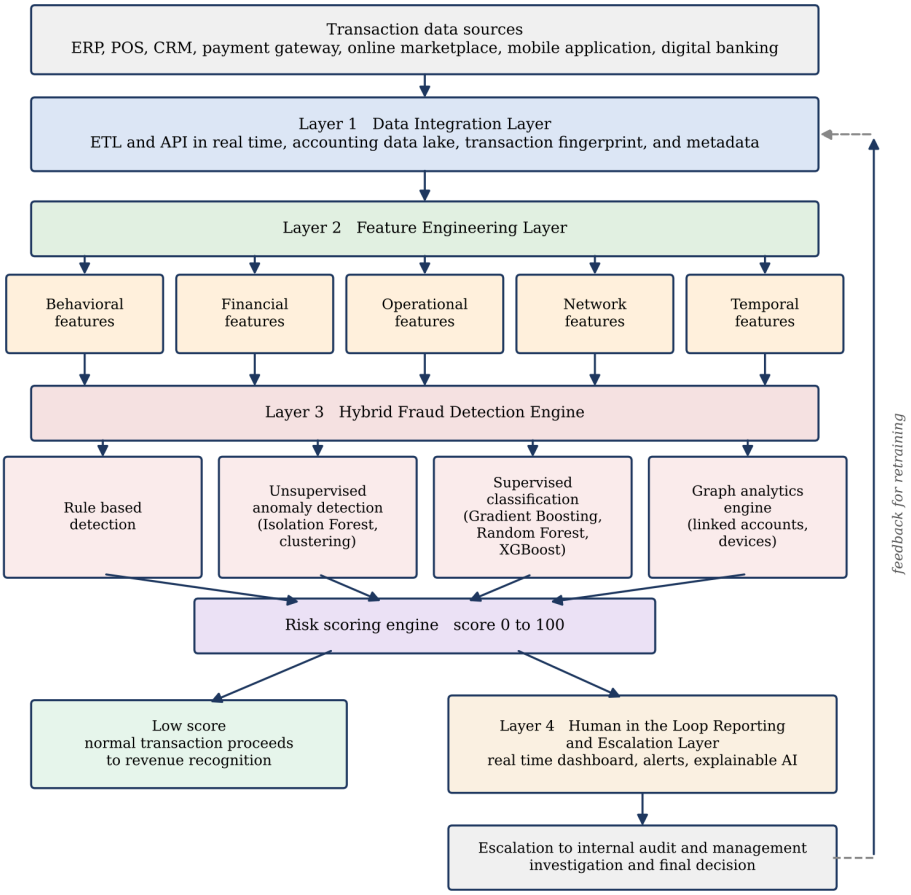



Figure 2. Architecture of the ACCOUNTGUARD AI model

Figure 2 shows that ACCOUNTGUARD AI consists of four connected layers that process transaction data from the source systems to the final decision. Data from ERP, POS, CRM, payment gateways, online marketplaces, mobile applications, and digital banking enter the Data Integration Layer, which consolidates them in an accounting data lake. The Feature Engineering Layer then transforms the raw data into five groups of risk features, which feed the Hybrid Fraud Detection Engine with its four detection components. The outputs of these components are combined into a risk score from 0 to 100, which determines whether a transaction proceeds normally to revenue recognition or is escalated through the Human in the Loop Reporting and Escalation Layer to internal audit and management. The dashed feedback line shows that the results of investigations are returned to the model for retraining, so that the system continues to learn from new fraud patterns.

### *4.3 Data Integration Layer*

The Data Integration Layer is the foundation of ACCOUNTGUARD AI. It collects, aligns, and consolidates transaction data from various sources into a single central repository in the form of an accounting data lake. In digital companies, revenue cycle data are usually spread across different systems, such as ERP, POS, CRM, payment gateways, mobile applications, online marketplaces, and banking and digital wallet systems. Integration is carried out through Extract, Transform, and Load (ETL) processes and Application Programming Interfaces (APIs) that allow data to be updated in real time. Each transaction is assigned a unique identifier, called a transaction fingerprint, so that customer

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co | DOI:10.52909/corelytics.v1i4.468 

activity can be traced from ordering, payment, and service use to the completion of the transaction. In addition to the main transaction data, the system collects metadata such as Internet Protocol (IP) addresses, devices used, geographic location, transaction time, and user activity logs.

This layer addresses the data fragmentation problem that has been identified as a major barrier to continuous auditing. Big data audit research emphasizes that auditors need integrated access to data from multiple sources to analyze full populations of transactions (Appelbaum et al., 2017). Tamper resistant records, such as those provided by distributed ledger technologies, can further strengthen the reliability of integrated data for continuous assurance (Dai & Vasarhelyi, 2017). By linking transactions across systems through a common fingerprint, the Data Integration Layer enables the end to end tracing that is required to detect schemes such as fictitious sales and refund fraud, which often involve inconsistencies between systems.

### *4.4 Feature Engineering Layer*

After the data are consolidated, ACCOUNTGUARD AI performs feature engineering to transform raw data into indicators with analytical value for fraud detection. This stage is crucial because the quality of the features determines the ability of the model to recognize deviant transaction patterns. The features are grouped into five main categories, which are presented in Table 3.

Table 3. Feature categories in the Feature Engineering Layer

| Feature Category | Examples of Features | Fraud Schemes Addressed |
|---|---|---|
| Behavioral features | Transaction frequency, average transaction value, voucher usage pattern, usual transaction time | Account takeover, voucher abuse |
| Financial features | Ratio of discounts to sales value, gap between revenue recognition and cash receipt, refund frequency | Revenue recognition manipulation, refund fraud |
| Operational features | Order processing time, transaction cancellation rate | Fictitious sales, channel stuffing |
| Network features | Links between accounts, devices, bank accounts, and payment methods | Collusion, multiple accounts, organized refund fraud |
| Temporal features | Changes in transaction patterns over time, period end spikes | Revenue timing manipulation, emerging fraud patterns |

Table 3 shows that each feature category captures a different dimension of fraud risk and corresponds to specific fraud schemes. Behavioral features describe how individual customers normally transact, so deviations such as sudden changes in transaction time or voucher use can indicate account takeover or promotion abuse. Financial features link operational events to accounting outcomes and are therefore essential for detecting revenue recognition manipulation and refund fraud. Operational, network, and temporal features add information about process efficiency, relationships between entities, and changes over time, which together allow the model to detect schemes that would remain invisible when transactions are examined one by one. This multidimensional feature set is consistent with evidence that aggregated and periodic behavioral features substantially improve fraud detection performance (Correa Bahnsen et al., 2016).

### *4.5 Hybrid Fraud Detection Engine*

The Hybrid Fraud Detection Engine is the analytical core of ACCOUNTGUARD AI. Unlike conventional fraud detection systems that rely only on predefined rules, this layer combines several approaches simultaneously to increase accuracy and reduce false positives. The first component is a rule based detection engine that applies business rules and internal control policies set by the company. For example, the system issues an alert when a discount exceeds an authorization limit, when a refund occurs without supporting documents, or when customer data change within a very short time before a transaction. The second component is unsupervised anomaly detection. Algorithms

such as Isolation Forest and clustering identify transactions that deviate from normal patterns without requiring labeled fraud data, which makes this approach effective for detecting new fraud schemes that have never been seen before (Pang et al., 2022).

The third component is supervised fraud classification. Algorithms such as Gradient Boosting, Random Forest, and XGBoost classify transactions based on known historical fraud patterns and produce a probability of fraud for each transaction (Ali et al., 2022). The fourth component is a graph analytics engine that maps relationships between customers, bank accounts, devices, IP addresses, and user accounts to identify suspicious transaction networks. Graph based approaches are particularly effective for detecting collusion, multiple accounts, and refund fraud involving many linked accounts. The outputs of all components are combined in a risk scoring engine that produces a score between 0 and 100, where a higher score indicates a greater likelihood that the transaction contains fraud indications.

The hybrid design follows evidence that combining detection techniques produces better results than any single technique. Hybrid ensembles that integrate traditional machine learning with deep learning have been shown to improve detection in large scale card fraud systems (Kim et al., 2019), and combining unsupervised and supervised learning improves the detection of both known and novel fraud patterns (Carcillo et al., 2021). Ensemble methods such as AdaBoost with majority voting further reduce misclassification (Randhawa et al., 2018). At the same time, the inclusion of a rule based component ensures that explicit control policies are always enforced, which is important for compliance and audit documentation.

### *4.6 Mapping to the Revenue Cycle Stages*

The main advantage of ACCOUNTGUARD AI is its ability to monitor every stage of the revenue cycle in an integrated way. At the sales order and credit approval stage, the system examines new customer profiles, unusual transaction patterns, and indications of synthetic accounts. At the order fulfillment stage, the system matches delivery or digital service usage data with sales data to detect fictitious transactions. At the invoicing stage, the system reviews the consistency of invoices with contracts, payment schedules, and revenue recognition requirements under PSAK 72 (Ikatan Akuntan Indonesia, 2018). Differences between the time of service delivery and the time of revenue recognition are flagged as a risk of revenue manipulation.

At the cash collection stage, the system automatically reconciles transactions from QRIS, digital wallets, virtual accounts, credit cards, and bank transfers, and differences that cannot be logically explained are categorized as anomalies. At the returns and refunds stage, the system analyzes refund patterns, return frequency, and links between accounts to identify refund fraud, voucher abuse, and misuse of digital promotions. This stage by stage mapping ensures that the model addresses the red flags identified in Table 2 and that the risk score of each transaction reflects the specific risks of the stage in which it occurs. Linking the detection engine to accounting standards also distinguishes ACCOUNTGUARD AI from generic fraud detection systems that focus only on payment fraud and ignore revenue recognition risk (Bao et al., 2020).

### *4.7 Human in the Loop Reporting and Escalation Layer*

The final layer serves as a bridge between the AI system and human decision makers. All transactions with a risk score above a defined threshold are displayed in a real time monitoring dashboard. The dashboard shows the transaction value, risk score, type of anomaly detected, investigation priority, and the factors that influenced the model's decision. In this way, auditors not only know that a transaction is risky but also understand the reasons behind the assessment, which is the essence of explainable AI (Barredo Arrieta et al., 2020). Local explanation methods for tree based models make it possible to show the contribution of each feature to the risk score of an individual transaction (Lundberg et al., 2020).

The human in the loop approach ensures that final decisions remain with auditors and management. AI acts only as a decision support system and an early warning system. This arrangement reflects the view that AI should augment rather than replace professional judgment in auditing (Issa et al., 2016, Kokina & Davenport, 2017), and it addresses concerns about accountability for automated decisions (Rudin, 2019). The results of investigations are fed back into the model as new labels, which allows the supervised component to be retrained and helps the system cope with concept drift as fraud patterns change (Lu et al., 2019, Dal Pozzolo et al., 2018).

### *4.8 Conceptual Prototype of the Dashboard*

The conceptual dashboard prototype of ACCOUNTGUARD AI functions as the interface through which fraud risk in the revenue cycle is monitored directly. The dashboard provides information on total transactions, high and medium risk transactions, early warnings, risk score trends, risk distribution, and a list of transactions that require the auditor's attention. The prototype is presented in Figure 3.

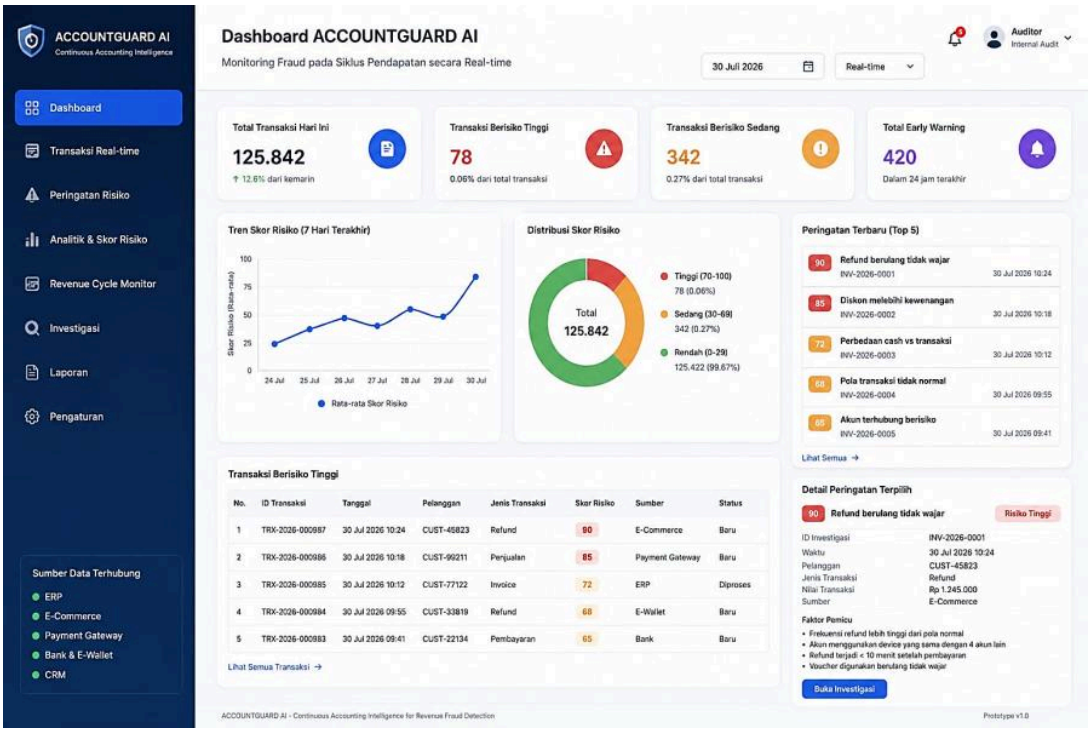



Figure 3. Conceptual prototype of the ACCOUNTGUARD AI dashboard for continuous fraud monitoring

Figure 3 shows the main screen of the ACCOUNTGUARD AI dashboard, which summarizes the daily number of transactions, the number of high and medium risk transactions, and the number of early warnings in tiles at the top of the screen. The central part displays the trend of average risk scores over the last seven days and the distribution of transactions by risk level, which allows auditors to see quickly whether overall risk is rising and how risk is spread across the transaction population. The list of the latest alerts and the table of high risk transactions show the transaction identifier, date, customer, transaction type, risk score, source system, and status, so auditors can set priorities for examination. The panel on the right shows the details of a selected alert together with the risk factors that explain its score and a button to start an investigation, which illustrates how the human in the loop principle is built into the interface.

The prototype integrates the human in the loop concept through the selected alert detail feature. The system provides a risk score together with the underlying causal factors, while auditors continue to investigate and decide on the next steps. The ACCOUNTGUARD AI dashboard therefore functions as

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co | DOI:10.52909/corelytics.v1i4.468 

a tool for continuous monitoring and decision support, not as a replacement for auditors in judging whether a transaction should be classified as fraud. This design responds to findings that explainability increases user trust and acceptance of AI systems (Shin, 2021) and that auditors require transparent outputs to rely on AI in their work (Zhang et al., 2022).

### *4.9 Comparison with Conventional Approaches*

The third research question concerns the effectiveness of the model compared with conventional audit and internal control approaches. The comparison is summarized in Table 4.

Table 4. Comparison of conventional approaches and ACCOUNTGUARD AI

| Aspect | Conventional Audit and Internal Control | ACCOUNTGUARD AI |
|---|---|---|
| Timing | Periodic and retrospective | Continuous and in real time |
| Coverage | Sample of transactions | Entire transaction population |
| Adaptability | Fixed rules and procedures | Learns new fraud patterns through retraining |
| Traceability | Limited across systems | End to end tracing through transaction fingerprints |
| Prioritization | Based on auditor judgment and sampling | Risk scoring that ranks transactions for investigation |
| Decision authority | Auditor and management | Auditor and management supported by explainable AI |

Table 4shows that ACCOUNTGUARD AI differs from conventional approaches in timing, coverage, adaptability, traceability, and prioritization, while keeping decision authority with auditors and management. Real time monitoring allows fraud to be detected before it causes material losses, and full population coverage removes the dependence on sampling that limits traditional audits. The ability to learn from new fraud patterns and to trace transactions across systems from end to end addresses the adaptive and fragmented nature of digital fraud. Risk scoring improves audit efficiency by directing attention to the transactions with the highest risk, and the explicit retention of human decision authority ensures that the model complements rather than replaces professional judgment.

These advantages are consistent with research on the transformation of auditing through technology. Analysis of entire populations and continuous anomaly detection are among the main benefits of AI in auditing (Kokina & Davenport, 2017), and big data analytics enables auditors to move from sampling to more comprehensive testing (Appelbaum et al., 2017). Automation of routine audit tasks frees auditors to focus on complex judgments (Eulerich et al., 2022). At the same time, the effectiveness of the model depends on the quality of its data and features, the calibration of its risk thresholds, and the competence of the people who interpret its outputs.

### *4.10 Implementation Challenges*

Despite its advantages, the implementation of ACCOUNTGUARD AI faces several challenges. The first challenge is data quality and interoperability, which often differ between systems and payment service providers. Without consistent identifiers and formats, the Data Integration Layer cannot link transactions reliably, and errors in the data will propagate to the detection engine. The second challenge is the relatively high investment required for technology, including computing infrastructure, data storage, and the development of AI models. This challenge may be particularly significant for small and medium sized digital companies, which may need to adopt cloud based services or phased implementation.

The third challenge concerns data security and privacy, because the system manages large volumes of sensitive transaction information. Strong access controls, encryption, and compliance with personal data protection regulations are therefore essential. The fourth challenge is the readiness of accounting staff to understand, interpret, and use the results of AI analysis. Research shows that the work of

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co | DOI:10.52909/corelytics.v1i4.468 

accountants is being reshaped by digital technologies, which requires new skills in data analytics and technology (Moll & Yigitbasioglu, 2019). The final challenge is model interpretability, which must be maintained so that fraud detection results can be justified in audits, regulatory examinations, and legal proceedings if necessary (Adadi & Berrada, 2018, Zhang et al., 2022). Models must also be monitored continuously because their performance declines when fraud patterns shift (Lu et al., 2019).

### *4.11 Discussion*

The results of this study show that the early detection of fraud in the revenue cycle of digital companies requires a combination of continuous data integration, rich feature engineering, hybrid detection techniques, and human oversight. ACCOUNTGUARD AI brings these elements together in a single model that is explicitly linked to the stages of the revenue cycle and to revenue recognition requirements. This integration distinguishes the model from many existing fraud detection systems, which focus on payment fraud at the transaction level and pay less attention to the accounting consequences of fraud. By connecting operational events with accounting outcomes, the model can detect not only fraudulent payments but also manipulations that affect reported revenue.

The model also contributes to the debate on the role of AI in auditing. Rather than viewing AI as a replacement for auditors, ACCOUNTGUARD AI positions it as an early warning and decision support system within a human in the loop framework. This view is consistent with research on human and AI symbiosis in organizational decision making (Jarrahi, 2018) and with the argument that organizations should combine automation and augmentation (Raisch & Krakowski, 2021). It also reflects the importance of trust, since auditors who do not understand how an AI system reaches its conclusions may either rely on it too much or ignore its alerts (Glikson & Woolley, 2020). Explainability is therefore not an optional feature but a core requirement of the model.

For Indonesian digital companies, the model is particularly relevant given the rapid growth of QRIS, digital wallets, and other cashless payment instruments. The expansion of digital finance supports inclusion and economic growth (Ozili, 2018, Mhlanga, 2020), but it also increases the volume and complexity of transactions that must be monitored. Adopting a model such as ACCOUNTGUARD AI could help companies maintain the reliability of their financial statements and the trust of investors and consumers as the digital economy continues to expand. The model also provides a basis for regulators and professional associations to develop guidance on the governance and explainability of AI in accounting and auditing.

## 5. Conclusions

The digitalization of the revenue cycle in digital companies operating in the cashless society increases transaction efficiency but also expands the space for various fraud schemes, from fictitious sales and revenue recognition manipulation to refund fraud, which are difficult to detect through periodic audits and conventional internal control. This study shows that fraud red flags appear at every stage of the digital revenue cycle and that they can be translated into observable indicators related to customer identity, sales and delivery consistency, revenue recognition timing, cash reconciliation, and refund patterns.

ACCOUNTGUARD AI, which combines continuous accounting with a hybrid detection engine based on AI, offers comprehensive and continuous monitoring of every stage of the revenue cycle, from ordering to cash collection and returns, while keeping human judgment as the final decision maker. Its four layers integrate data from multiple systems, transform them into behavioral, financial, operational, network, and temporal features, combine rule based, unsupervised, supervised, and graph based detection into a risk score, and present the results through an explainable dashboard with escalation to auditors and management. The model therefore has the potential to increase the speed and accuracy of early fraud detection and to strengthen confidence in the reliability of the financial statements of digital companies.

This study has several limitations. The model is conceptual and has not been tested empirically with real or simulated transaction data, so its detection accuracy, false positive rate, and cost efficiency have not been measured. The dashboard is a conceptual prototype rather than a working system. The study also relies on literature that is largely drawn from card fraud and financial statement fraud research, which may not capture all characteristics of revenue cycle fraud in Indonesian digital companies.

Based on these findings, several recommendations are proposed. Digital companies are advised to begin integrating data across ERP, POS, and payment gateway systems into a single accounting platform as a prerequisite for continuous accounting intelligence such as ACCOUNTGUARD AI. Regulators and professional accounting associations are advised to develop governance guidelines and explainability standards for the use of AI in accounting and auditing to maintain accountability and compliance with financial reporting standards. Future researchers are advised to test ACCOUNTGUARD AI empirically using real or simulated transaction data and to measure its accuracy, sensitivity, and cost efficiency compared with conventional fraud detection methods.

## Acknowledgement

The authors thank the Faculty of Economics, Universitas Katolik Darma Cendika, for its support, and the organizers of the National Accounting Paper Competition for the opportunity to develop this study.

## Author Contributions

DW contributed to the conceptualization of the study, the literature review, the design of the ACCOUNTGUARD AI model and dashboard prototype, and the writing and revision of the manuscript. GNC contributed to the conceptualization of the study, the literature review, the design of the ACCOUNTGUARD AI model and dashboard prototype, and the writing and revision of the manuscript. JRS contributed to the conceptualization of the study, the literature review, the design of the ACCOUNTGUARD AI model and dashboard prototype, and the writing and revision of the manuscript. All authors read and approved the final manuscript.

## Conflict of Interest

The authors declare no conflict of interest.

## References

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications, 68, 90–113*. https://doi.org/10.1016/j.jnca.2016.04.007

Adadi, A., & Berrada, M. (2018). Peeking inside the black-box: A survey on explainable artificial intelligence (XAI). *IEEE Access, 6, 52138–52160*. https://doi.org/10.1109/ACCESS.2018.2870052

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, *12*(19). https://doi.org/10.3390/app12199637

Appelbaum, D., Kogan, A., & Vasarhelyi, M. A. (2017). Big data and analytics in the modern audit engagement: Research needs. *Auditing: A Journal of Practice & Theory*, *36*(4), 1-27. https://doi.org/10.2308/ajpt-51684

Asrul, Suryawan, I. K. D., Jana, P., & Mandias, G. F. (2025). Machine learning. *Yash Media*.

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co | 

Bao, Y., Ke, B., Li, B., Yu, Y. J., & Zhang, J. (2020). Detecting accounting fraud in publicly traded U.S. *firms using a machine learning approach. Journal of Accounting Research*, *58*(1), 199-235. https://doi.org/10.1111/1475-679X.12292

Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58, 82–115*. https://doi.org/10.1016/j.inffus.2019.12.012

Bussmann, N., Giudici, P., Marinelli, D., & Papenbrock, J. (2021). Explainable machine learning in credit risk management. *Computational Economics*, *57*(1), 203-216. https://doi.org/10.1007/s10614-020-10042-0

Carcillo, F., Le Borgne, Y.-A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2021). Combining unsupervised and supervised learning in credit card fraud detection. *Information Sciences, 557, 317–331*. https://doi.org/10.1016/j.ins.2019.05.042

Correa Bahnsen, A., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications, 51, 134–142*. https://doi.org/10.1016/j.eswa.2015.12.030

Dai, J., & Vasarhelyi, M. A. (2017). Toward blockchain-based accounting and assurance. *Journal of Information Systems*, *31*(3), 5-21. https://doi.org/10.2308/isys-51804

Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: A realistic modeling and a novel learning strategy. *IEEE Transactions on Neural Networks and Learning Systems*, *29*(8), 3784-3797. https://doi.org/10.1109/TNNLS.2017.2736643

Eulerich, M., Pawlowski, J., Waddoups, N. J., & Wood, D. A. (2022). A framework for using robotic process automation for audit tasks. *Contemporary Accounting Research*, *39*(1), 691-720. https://doi.org/10.1111/1911-3846.12723

Fahmi, M., Zulkarnain, Muda, I., & Kesuma, S. A. (2022). Implementation of internal control procedures that enable cost savings in dealing with threats in the revenue cycle: Traditional vs digital accounting information system era in pharmaceutical sector. *Journal of Pharmaceutical Negative Results*, *13*(7), 3566-3571.

Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals*, *14*(2), 627-660. https://doi.org/10.5465/annals.2018.0057

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems*, *35*(1), 220-265. https://doi.org/10.1080/07421222.2018.1440766

Hidayati, M., Anggraeni, A. F., Evi, T., Rahmadi, Z. T., & Asri, M. (2023). Teori akuntansi [Accounting theory]. *PT Sonpedia Publishing Indonesia*.

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications, 193, Article 116429*. https://doi.org/10.1016/j.eswa.2021.116429

Ikatan Akuntan Indonesia. (2018). PSAK 72 Pendapatan dari kontrak dengan pelanggan [Revenue from contracts with customers]. *Ikatan Akuntan Indonesia*.

Issa, H., Sun, T., & Vasarhelyi, M. A. (2016). Research ideas for artificial intelligence in auditing: The formalization of audit and workforce supplementation. *Journal of Emerging Technologies in Accounting*, *13*(2), 1-20. https://doi.org/10.2308/jeta-10511

Jarrahi, M. H. (2018). Artificial intelligence and the future of work: Human-AI symbiosis in organizational decision making. *Business Horizons*, *61*(4), 577-586. https://doi.org/10.1016/j.bushor.2018.03.007

Kim, E., Lee, J., Shin, H., Yang, H., Cho, S., Nam, S., Song, Y., Yoon, J., & Kim, J. (2019). Champion-challenger analysis for credit card fraud detection: Hybrid ensemble and deep learning. *Expert Systems with Applications, 128, 214–224*. https://doi.org/10.1016/j.eswa.2019.03.042

Kokina, J., & Davenport, T. H. (2017). The emergence of artificial intelligence: How automation is changing auditing. *Journal of Emerging Technologies in Accounting*, *14*(1), 115-122. https://doi.org/10.2308/jeta-51730

Lu, J., Liu, A., Dong, F., Gu, F., Gama, J., & Zhang, G. (2019). Learning under concept drift: A review. *IEEE Transactions on Knowledge and Data Engineering*, *31*(12), 2346-2363. https://doi.org/10.1109/TKDE.2018.2876857

Lundberg, S. M., Erion, G., Chen, H., DeGrave, A., Prutkin, J. M., Nair, B., Katz, R., Himmelfarb, J., Bansal, N., & Lee, S. I. (2020). From local explanations to global understanding with explainable AI for trees. *Nature Machine Intelligence*, *2*(1), 56-67. https://doi.org/10.1038/s42256-019-0138-9

Mhlanga, D. (2020). Industry 4.0 in finance: The impact of artificial intelligence (AI) on digital financial inclusion. *International Journal of Financial Studies*, *8*(3). https://doi.org/10.3390/ijfs8030045

Moll, J., & Yigitbasioglu, O. (2019). The role of internet-related technologies in shaping the work of accountants: New directions for accounting research. *The British Accounting Review*, *51*(6). https://doi.org/10.1016/j.bar.2019.04.002

Moon, I. T., Shamsuzzaman, M., Mridha, M. M. R., & Rahaman, A. S. M. M. (2022). Towards the advancement of cashless transaction: A security analysis of electronic payment systems. *Journal of Computer and Communications*, *10*(7), 103-129. https://doi.org/10.4236/jcc.2022.107007

Narendrar, N. A., Suseno, J. E., & Nugraheni, D. M. K. (2023). Factors influencing interest in continuing use of e-wallet using the technology acceptance model and task-technology fit. *Mimbar Ilmu*, *28*(2), 221-230.

Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, *18*(4), 329-340. https://doi.org/10.1016/j.bir.2017.12.003

Pang, G., Shen, C., Cao, L., & van den Hengel, A. (2022). Deep learning for anomaly detection: A review. *ACM Computing Surveys*, *54*(2). https://doi.org/10.1145/3439950

Patil, P., Tamilmani, K., Rana, N. P., & Raghavan, V. (2020). Understanding consumer adoption of mobile payment in India: Extending Meta-UTAUT model with personal innovativeness, anxiety, trust, and grievance redressal. *International Journal of Information Management, 54, Article 102144*. https://doi.org/10.1016/j.ijinfomgt.2020.102144

Petcu, M. A., David, M. I. S., & Curea, S. C. (2024). Integrating digital technologies in sustainability accounting and reporting: Perceptions of professional cloud computing users. *Electronics*, *13*(14). https://doi.org/10.3390/electronics13142684

Raisch, S., & Krakowski, S. (2021). Artificial intelligence and management: The automation–augmentation paradox. *Academy of Management Review*, *46*(1), 192-210. https://doi.org/10.5465/amr.2018.0072

Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit card fraud detection using AdaBoost and majority voting. *IEEE Access, 6, 14277–14284*. https://doi.org/10.1109/ACCESS.2018.2806420

Rifky, S., Kharisma, L. P. I., & Afendi, A. R. (2024). Artificial intelligence. *PT Sonpedia Publishing Indonesia*.

Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, *1*(5), 206-215. https://doi.org/10.1038/s42256-019-0048-x

Shin, D. (2021). The effects of explainability and causability on perception, trust, and acceptance: Implications for explainable AI. *International Journal of Human-Computer Studies, 146, Article 102551*. https://doi.org/10.1016/j.ijhcs.2020.102551

Trischler, M. F. G., & Li-Ying, J. (2023). Digital business model innovation: Toward construct clarity and future research directions. *Review of Managerial Science*, *17*(1), 3-32. https://doi.org/10.1007/s11846-021-00508-2

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118-144. https://doi.org/10.1016/j.jsis.2019.01.003

Vousinas, G. L. (2019). Advancing theory of fraud: The S.C.O.R.E. *model. Journal of Financial Crime*, *26*(1), 372-381. https://doi.org/10.1108/JFC-12-2017-0128

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security, 57, 47–66*. https://doi.org/10.1016/j.cose.2015.09.005

Yang, H., Shukur, Z., & Sahran, S. (2026). A review of artificial intelligence for financial fraud detection. *Applied Sciences*, *16*(4). https://doi.org/10.3390/app16041931

Zahirah, F. R., Melenia, F., & Aminy, A. R. (2021). Continuous audit: Penerapan dan pengendalian pelaksanaan fungsi audit berbasis teknologi informasi. *Balance: Jurnal Akuntansi, Auditing dan Keuangan*, *18*(2), 200-216. https://doi.org/10.25170/balance.v18i2.3136

Zhang, C. A., Cho, S., & Vasarhelyi, M. (2022). Explainable artificial intelligence (XAI) in auditing. *International Journal of Accounting Information Systems, 46, Article 100572*. https://doi.org/10.1016/j.accinf.2022.100572

© 2026 Abnus | Open Access — CC BY 4.0 | abnus.co | DOI:10.52909/corelytics.v1i4.468 