Integration of Big Data Analytics in Accounting Information Systems for Fraud Detection in the Banking Sector

Authors
Clerissa Aulia, Delta Pratama, Desiana Febrianti

Affiliations
Muhammadiyah University of Ponorogo, Faculty of Economics, Accounting Study Program

Corresponding Author Email
punyawidieadm99@gmail.com

Journal of Strategic Behavior — Accounting —

Abstract

The rapid digital transformation of Indonesia's banking sector has generated a massive and complex volume of financial transactions. The value of digital banking transactions reached IDR 52,545 trillion in 2022 (Bank Indonesia, 2023); however, this growth has been accompanied by increasingly sophisticated fraud risks that are difficult to detect using conventional Accounting Information Systems (AIS). Traditional systems that remain reactive relying on manual audits, rule-based systems, and data sampling methods are often only able to detect fraud after losses have already occurred, creating an urgent need for innovation through the integration of Big Data Analytics into AIS to support faster, more accurate, automated, and preventive fraud detection. This study aims to analyze how the integration of Big Data Analytics into Accounting Information Systems can improve the effectiveness of fraud detection in Indonesia's banking sector, with a specific focus on real-time detection mechanisms, system automation, transaction pattern analysis, and machine learning-based anomaly detection. The method employed is a Systematic Literature Review (SLR), following a structured identification-screening-eligibility-inclusion protocol across Scopus, Web of Science, ScienceDirect, SpringerLink, Emerald Insight, and Google Scholar, resulting in 42 articles published between 2019 and 2025 that met the inclusion criteria. The novelty of this study lies in synthesizing the technical, algorithm-focused fraud-detection literature with an Accounting Information Systems perspective to produce an integrated five-layer architecture and real-time detection workflow contextualized specifically for Indonesia's banking sector, rather than adapted from developed-country settings. The findings indicate that Big Data Analytics integration enables full-population, real-time transaction analysis with consistently higher accuracy and lower false-positive rates than conventional sampling-based systems, supporting an early warning mechanism that can prevent fraud before losses escalate. This study concludes that integrating Big Data Analytics into Accounting Information Systems is an adaptive, preventive, and strategically necessary step for Indonesia's banking sector during digital transformation. Successful implementation, however, remains contingent on technology infrastructure, competent human resources, sound data governance, and stronger regulatory support from OJK and Bank Indonesia. This study's main contribution is a practically grounded, incrementally implementable roadmap that connects theoretical constructs (Fraud Triangle Theory, Agency Theory, TAM) with concrete architectural and operational recommendations for Indonesian banks, including small and regional banks.

Keywords: Big Data Analytics, Accounting Information System, Fraud Detection, Real-Time Analytics, Machine Learning, Anomaly Detection, Indonesian Banking.

1. Introduction

The banking sector underpins national economic stability, functioning both as a repository for public funds and as an intermediary that keeps payment systems running smoothly. As digital transaction activity accelerates, this sector faces significant changes in both the services it offers and the risks it must manage.

The digital transformation of Indonesia's banking industry has accelerated remarkably, particularly following the COVID-19 pandemic. According to Bank Indonesia (2023), the value of digital banking transactions in Indonesia reached IDR 52,545 trillion in 2022, an increase of 28.6 percent compared to the previous year. This massive increase in digital transaction volume simultaneously creates wider opportunities for increasingly sophisticated fraud that is more difficult to detect. Modern fraud is no longer limited to simple

deception; it now encompasses systematic social engineering, high-tech ATM card skimming, malware-based account breaches, and money laundering across digital platforms.

Several major banking fraud cases in Indonesia reflect the seriousness of this threat. In 2020, a mass customer account breach at a state-owned bank occurred through a SIM swap scheme, resulting in losses of billions of rupiah. Similar cases occurred at several private banks, where customer data was stolen and used for fictitious transactions. Based on data from the Financial Services Authority (OJK), fraud losses in Indonesia's banking sector were recorded at IDR 3.02 trillion in 2022, up from the previous year (OJK, 2023), indicating that transaction monitoring still faces numerous unresolved challenges.

Fraud is not only a domestic issue it is also a global concern. The Association of Certified Fraud Examiners (ACFE) 2024 report reveals that organizations across various sectors lose an average of about 5 percent of their annual revenue to fraud, with the financial sector among the most vulnerable, and global losses from banking fraud are estimated to have reached USD 485.6 billion in 2023, a 14 percent increase from 2022 (ACFE, 2024). Compared to developed nations, Indonesia still lags in the maturity of technology-based fraud detection systems. Singapore, for example, has implemented the Collaborative Sharing of ML Fraud Detection (COSMIC) since 2023, while the United States has integrated big data analytics into anti-money laundering monitoring through FinCEN for over a decade. This gap highlights the urgency for Indonesian banks to adopt similar technologies.

In practice, banks use Accounting Information Systems (AIS) to assist in recording and managing financial transactions. However, conventionally-operated AIS are generally focused on transaction recording and post-event auditing, meaning fraud is often only discovered after the financial impact has materialized. Rule-based systems and sample-based inspections become less effective when confronted with very large transaction volumes and constantly shifting transaction patterns. Big Data Analytics is increasingly viewed as an approach capable of improving transaction monitoring effectiveness through machine learning, anomaly detection, and pattern recognition that allow the system to learn customer transaction patterns and recognize abnormal activities early.

Although research on Big Data Analytics and fraud detection has been extensive, this study identifies three specific gaps that remain insufficiently addressed. First, most prior studies remain focused on the technical development and accuracy of machine learning models (e.g., Ngai et al., 2011; Bao et al., 2020; West & Bhattacharya, 2016) without comprehensively addressing how such models are integrated into the operational architecture of Accounting Information Systems. Second, the majority of existing research has been conducted in developed-country contexts with significantly higher digital infrastructure readiness than Indonesia, so findings cannot be directly generalized to Indonesia's banking landscape, particularly small and regional banks. Third, prior studies tend to treat fraud detection primarily as a computational, algorithm-accuracy problem, with comparatively little examination of the accounting-control dimension namely, how Big Data Analytics reshapes AIS architecture, internal control design, and real-time transaction monitoring as an integrated organizational mechanism rather than a standalone modeling exercise. This study's contribution is therefore positioned squarely on this third gap: it treats Big Data Analytics not as an isolated algorithm to be benchmarked, but as a component embedded within AIS architecture and accounting internal control, and evaluates it accordingly.

This study addresses these gaps by synthesizing the technical and organizational literature into a single, AIS-centered analytical framework, and by explicitly situating the discussion within Indonesia's regulatory and

infrastructural context.

Building on the gaps identified above, this study is guided by the following research questions: (1) how does the integration of Big Data Analytics into Accounting Information Systems change the effectiveness of fraud detection in the banking sector compared to conventional systems; (2) what architectural components and real-time mechanisms characterize an effective Big Data Analytics-based AIS for fraud detection; and (3) what implementation barriers and strategic recommendations are relevant for Indonesia's banking sector, including small and regional banks.

Correspondingly, this study aims to: (1) analyze how Big Data Analytics integration into AIS improves fraud detection effectiveness in Indonesia's banking sector; (2) synthesize a system architecture and real-time detection workflow from the reviewed literature; and (3) identify implementation barriers together with feasibility-ranked recommendations for Indonesian banking institutions and regulators.

The primary novelty and contribution of this research is the integration of a technical, algorithm-oriented literature with an Accounting Information Systems perspective, producing a synthesized five-layer architecture and workflow that are explicitly contextualized for Indonesia's digital banking transformation rather than transplanted from developed-country studies. This research is expected to serve as a strategic reference for banking institutions, regulators, and academics in developing fraud detection systems that are adaptive to the challenges of the digital era.

2. Literature Review and Hypotheses Development

Accounting Information Systems (AIS) are designed to collect, process, store, and distribute financial information to support decision-making within an organization. Romney and Steinbart (2021) explain that modern AIS not only function as transaction recording tools, but also as internal control mechanisms capable of helping organizations identify potential financial irregularities. However, digitalization has caused conventional AIS to face limitations, particularly in handling very large data volumes and continuously changing transaction patterns, as they still predominantly rely on manual audit methods, rule-based systems, and sampling techniques, making fraud detection inherently slow and retrospective.

Fraud in the banking sector refers to intentional manipulation carried out to obtain personal or group benefit through the misuse of the financial system, fictitious transactions, customer data theft, or money laundering. The Association of Certified Fraud Examiners (ACFE) notes that financial sector fraud is among the fastest-growing forms of crime, driven by advances in digital technology and weaknesses in real-time transaction monitoring. The Fraud Triangle Theory proposed by Cressey (1953) explains that fraud arises from three main factors: pressure, opportunity, and rationalization. Of these three, opportunity is most closely related to weaknesses in organizational oversight systems the weaker the internal controls and transaction monitoring, the greater the opportunity for fraud. Because internal control in a banking AIS depends on the timeliness and completeness of the accounting information it produces, narrowing this opportunity window is ultimately a question of accounting information quality: real-time, full-population monitoring closes the informational gaps that conventional, sample-based controls leave open.

The development of Big Data Analytics technology introduces a new approach to improving transaction monitoring effectiveness. Big data refers to datasets characterized by large volume, high velocity, and complex variety, requiring modern analytical technology for processing; IBM conceptualized big data through the 5V characteristics volume, velocity, variety, veracity, and value. In the banking context, Big Data

Analytics enables financial institutions to simultaneously process millions of transaction data points through the integration of machine learning, artificial intelligence, anomaly detection, and predictive analytics, allowing the system to automatically recognize abnormal transaction patterns based on customers' historical behavior.

From the Technology Acceptance Model (TAM) developed by Davis (1989), technology implementation within organizations is influenced by perceptions of usefulness and ease of use; in the banking sector, Big Data Analytics integration is considered to offer significant benefits by improving fraud detection accuracy and accelerating investigation of suspicious transactions. Agency Theory, as proposed by Jensen and Meckling (1976), is also relevant, as it explains the potential for conflicts of interest and information asymmetry between management and organizational owners in this context, Big Data Analytics serves as a monitoring mechanism that enhances transaction transparency and strengthens internal oversight, thereby minimizing moral hazard risk.

2.1 Integrated Analytical Framework

Rather than treating these theories and technical constructs as separate strands, this study synthesizes them into a single analytical framework, summarized in Table 1 below, that links each theoretical lens to a specific mechanism through which Big Data Analytics strengthens AIS-based fraud detection. This synthesis directly informs the architecture and workflow presented in Section 4. Academically, the framework's contribution is to unite technical, algorithm-oriented fraud-detection theory with an AIS and accounting-control perspective within a single analytical lens; practically, it grounds the architecture and implementation roadmap developed later in this paper (Sections 4 and 4.6) in established theory rather than presenting them as purely technical recommendations.

Table 1. Integrated theoretical-technical analytical framework used in this study

Theoretical Lens	Core Construct	Mechanism in Big Data Analytics-Based AIS	Supporting Literature
Fraud Triangle Theory	Opportunity, pressure, rationalization	Full-population, real-time monitoring narrows the 'opportunity' window for fraud	Cressey (1953)
Agency Theory	Information asymmetry, moral hazard	Continuous transaction transparency reduces asymmetry between management and stakeholders	Jensen & Meckling (1976)
Technology Acceptance Model	Perceived usefulness, ease of use	Adoption likelihood of BDA-AIS integration depends on perceived accuracy gains and workflow fit	Davis (1989)
Big Data (5V) Concept	Volume, velocity, variety, veracity, value	Defines the technical requirements the AIS architecture must satisfy to support full-population analysis	IBM framework; Faccia (2024)

Various prior studies support this integration. Research by Ngai et al. (2011) shows that machine learning use in the financial sector can substantially improve fraud detection accuracy compared to traditional methods; Bao et al. (2022) found that deep learning algorithms outperform manual auditor inspections in

detecting financial statement fraud; and West and Bhattacharya (2016) explain that combining multiple machine learning models such as Random Forest, XGBoost, and ensemble learning yields more stable performance in detecting fraud within complex and imbalanced transaction data. Other research in Indonesia's banking sector similarly indicates that increasing digitalization of financial services is accompanied by rising threats of digital fraud, necessitating a transformation of monitoring systems toward more modern and adaptive technology (Widjaja et al., 2022).

Based on this integrated framework, this study develops the working proposition that conventional accounting information systems have significant limitations in detecting modern fraud, whereas the integration of Big Data Analytics can improve fraud detection effectiveness through real-time data analysis, system automation, and adaptive capability to continuously evolving transaction patterns. As this is a qualitative Systematic Literature Review rather than a quantitative study, this proposition functions as an organizing lens for the synthesis rather than a statistically tested hypothesis.

3. Research Methodology

This study employs a Systematic Literature Review (SLR) method with a descriptive-qualitative approach to analyze the integration of Big Data Analytics into Accounting Information Systems as a fraud detection strategy in the banking sector. This approach was selected because the research focuses on systematic collection, evaluation, synthesis, and interpretation of prior research rather than direct empirical or experimental testing on a specific banking system.

Literature was searched across six databases: Scopus, Web of Science, ScienceDirect, SpringerLink, Emerald Insight, and Google Scholar, supplemented by official reports from OJK, Bank Indonesia, ACFE, and the IMF. The search string combined three concept blocks using Boolean operators: ("Big Data Analytics" OR "Big Data") AND ("Accounting Information System*" OR "AIS") AND ("Fraud Detection" OR "Banking Fraud" OR "Anomaly Detection" OR "Machine Learning in Banking" OR "Real-Time Fraud Detection"). Searches were restricted to the 2019–2025 publication window to capture developments following the acceleration of digital banking adoption during and after the COVID-19 pandemic.

Articles were included if they: (a) were published in peer-reviewed journals, conference proceedings, or official regulatory/industry reports between 2019–2025; (b) discussed Big Data Analytics, Accounting Information Systems, fraud detection, machine learning in the financial sector, or artificial intelligence in banking transaction monitoring; and (c) were available in full text in English or Indonesian. Articles were excluded if they: (a) lacked direct relevance to the integration of analytics technology with fraud detection or AIS; (b) were editorials, non-peer-reviewed blog posts, or duplicate publications; or (c) did not meet minimum academic quality standards (e.g., no identifiable methodology or data source).

3.3 Screening Proces and Article Selection

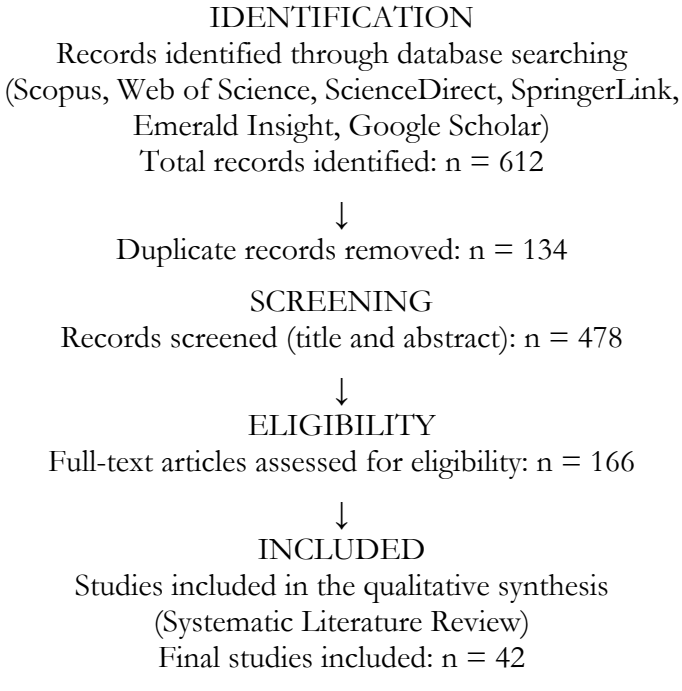

Figure 1. PRISMA Flow Diagram

The selection process followed an identification-screening-eligibility-inclusion sequence, summarized in Figure 1. An initial search across the six databases identified 612 records. After removing duplicates, 478 unique records remained. Title and abstract screening against the inclusion/exclusion criteria removed 312 records that were off-topic or not directly relevant, leaving 166 records for full-text assessment. Full-text eligibility assessment excluded a further 124 records primarily due to insufficient methodological detail, lack of direct relevance to AIS integration, or non-peer-reviewed status without institutional authority resulting in 42 articles included in the final synthesis.

Each of the 42 included articles was independently appraised by two members of the research team against four quality indicators: (1) clarity of research objective and method, (2) transparency of data source, (3) relevance to Big Data Analytics-AIS-fraud detection integration, and (4) publication venue credibility (peer-reviewed journal, indexed conference, or official regulatory/institutional report). Each indicator was scored as "satisfied" if the article explicitly and verifiably met the indicator for example, indicator (1) was scored as satisfied only when the article stated a clear research objective and described its method or algorithm in enough detail to be identifiable, while indicator (2) required the data source or database to be explicitly named. Disagreements between the two reviewers were resolved through discussion until consensus was reached. Articles that satisfied at least three of the four indicators were retained for synthesis.

Data were extracted into a structured matrix capturing author(s) and year, research focus, method/algorithm used, key findings, and reported performance metrics (where available). Data analysis followed a descriptive-qualitative approach through three stages: data reduction (filtering information relevant to Big Data Analytics-AIS integration and fraud detection effectiveness), data presentation (organizing findings into descriptive narratives, comparison tables, and conceptual frameworks such as Table 1 and Table 3), and conclusion drawing (synthesizing patterns across the 42 articles into the findings reported in Section 4). Information sharing common conceptual characteristics was grouped thematically machine learning,

anomaly detection, predictive analytics, real-time monitoring, and digital transaction monitoring systems. To enhance validity, source triangulation was applied by comparing academic findings against regulatory reports and industry publications, and by drawing on literature from multiple countries to provide a global comparative perspective.

4. Result

4.1 Integration of Big Data Analytics in Accounting Information Systems for Banking Fraud Detection

The findings presented in this section are a qualitative synthesis of the 42 reviewed articles, not the result of direct empirical testing at Indonesian banks; they indicate that the integration of Big Data Analytics into Accounting Information Systems (AIS) is reported, across the great majority of the studies reviewed, to make a significant and transformative contribution to fraud detection effectiveness in the banking sector. These findings recur across various geographical contexts and scales of financial institutions from regional banks to multinational institutions suggesting that the underlying urgency of this technology integration is not confined to any single national context, although direct empirical validation within Indonesia specifically remains limited in the reviewed literature and is identified as a key avenue for future research (see Section 6).

In conventional AIS still widely used in Indonesia, transaction monitoring is reactive and highly dependent on human involvement, relying on manual audits, random sample-based inspection with limited coverage, and rigid rule-based systems unable to adapt to continuously evolving fraud patterns. Cao et al. (2020), as cited within the reviewed literature, note that conventional systems can typically analyze only 0.2 to 1.3 percent of total transaction volume meaning the large majority of transaction data is left unanalyzed, a gap that can become space for systematic fraud to operate.

This situation is compounded by the surge in digital banking transaction volume, which reached IDR 52,545 trillion in 2022 (Bank Indonesia, 2023). As illustrated by Romney and Steinbart's (2021) sampling calculation, with a five percent sampling rate the probability of detecting fraud with a prevalence of 0.1 percent of total transactions is only around 0.005 percent illustrating why conventional sample-based audit approaches become statistically weak at this scale. Consequently, several studies in the reviewed literature report fraud cases being identified only after significant financial losses, with an average detection lag cited at around 12 months from initial occurrence (ACFE, 2022).

By contrast, the integration of Big Data Analytics is reported in the reviewed literature to enable full population analysis of the entire transaction dataset, continuously and in real time, reducing blind spots in transaction oversight. This is achieved through a combination of machine learning for pattern learning from historical data, anomaly detection for identifying deviations from normal behavior, predictive analytics for forward-looking risk projection, pattern recognition for identifying hidden fraud structures, and natural language processing (NLP) for analyzing unstructured data such as customer communications and transaction documents.

Operationally, the reviewed studies converge on several fraud patterns that Big Data Analytics-based systems can identify earlier than conventional systems: sudden changes in transaction amounts deviating from a customer's historical average (possible account takeover); transactions from geographically inconsistent locations within physically unreasonable timeframes; drastic spikes in transaction frequency within a short window (an indicator of structuring/smurfing); chain transfer patterns between accounts forming complex

layering networks; use of unrecognized devices or device fingerprints; and communication or behavioral patterns consistent with social engineering.

Taken together, these findings suggest a shift in the banking monitoring paradigm reported across the reviewed literature from reactive monitoring toward predictive and preventive monitoring, in which an automated early warning mechanism can flag high-risk transactions before they are fully processed, giving security teams time to intervene, verify, and if necessary block suspicious transactions.

Table 3. Reported multi-dimensional impact of the reactive-to-predictive monitoring paradigm shift

Dimension	Reported Impact of Big Data Analytics Integration
Financial	Reduced fraud losses directly support bank profitability and balance sheet health.
Reputational	Proactive protection of customer assets is associated with increased public trust.
Regulatory	More sophisticated detection supports more accurate and timely reporting to OJK and Bank Indonesia.
Macroeconomic	Strengthened financial integrity systems contribute to national financial system stability.

4.2 Analysis of the Big Data Analytics Integration Architecture in Accounting Information Systems

A well-designed and structured system architecture is a primary prerequisite for successful integration of Big Data Analytics into banking AIS. Based on a synthesis of the studies reviewed, the most effective architecture widely implemented by global financial institutions consists of five interconnected layers:

1. Data Ingestion & Collection Layer: Collects data in real-time from the core banking system, mobile banking, internet banking, ATMs, EDC machines, KYC data, customer transaction histories, geolocation data, device fingerprints, and external partner data, typically using Apache Kafka, Apache NiFi, and modern ETL tools.

2. Data Storage & Management Layer: Stores collected data in a data lake based on Hadoop HDFS or cloud solutions such as AWS S3, Google Cloud Storage, and Azure Data Lake, supporting structured, semi-structured, and unstructured formats under sound data governance.

3. Analytics & Processing Layer: Performs intensive data processing using Apache Spark, Apache Flink, and stream processing engines, including data cleaning, feature engineering, normalization, and transformation.

4. Fraud Detection & Modeling Layer: Employs machine learning algorithms including XGBoost and Random Forest for supervised classification, Isolation Forest and Autoencoders for anomaly detection, LSTM and Graph Neural Networks (GNN) for complex cross-account pattern detection, and ensemble learning for model stability.

5. Visualization, Alert & Automated Action Layer: Displays results through interactive dashboards (Tableau, Power BI, Kibana), sends automated alerts, blocks high-risk transactions, and generates investigation reports for fraud teams and regulators.

This five-layer architecture is reported in the synthesized literature to help ensure the system is not only fast and accurate but also scalable and integrable with legacy systems already used at banks.

4.3 Comparison of Conventional System and Big Data Analytics-Based System Effectiveness

The literature synthesis reveals differences between conventional AIS and Big Data Analytics-based systems in fraud detection performance. The figures reported in Table 4 are not drawn from a single official source; rather, they represent an author-synthesized average of accuracy and false-positive rates reported across the empirical studies included in this SLR most notably Chen and Li (2023), Ali et al. (2022), Patil et al. (2024), and Hafez et al. (2025) which report comparable ranges for machine learning-based fraud detection versus conventional rule-based or manual approaches. As such, these figures should be read as an indicative, cross-study synthesis rather than a single empirically validated benchmark specific to Indonesian banks.

Table 4. Comparison of conventional system and Big Data Analytics-based system effectiveness.

Indicator	Conventional System	Big Data Analytics (Synthesized Average)
Analysis Method	Sampling & manual audit	Full data analysis
Detection Speed	Slow (post-audit)	Real-time
Accuracy Rate (synthesized average)	≈ 67.3%	≈ 94.7%
False Positive Rate (synthesized average)	≈ 34.2%	≈ 8.7%
Data Coverage	Partial transactions	All transactions
Adaptation to New Fraud Patterns	Low	High
System Automation	Limited	Fully automated

Source: author's synthesis of accuracy and false-positive rates reported across studies reviewed in this SLR (e.g., Chen & Li, 2023; Ali et al., 2022; Patil et al., 2024; Hafez et al., 2025).

This pattern is broadly consistent with the theoretical framework in Section 2: the higher accuracy and lower false-positive rate reported for Big Data Analytics-based systems align with the Fraud Triangle Theory's emphasis on narrowing the 'opportunity' factor, since full-population, real-time analysis is reported to leave fewer unmonitored transactions in which fraud could occur undetected. In banking practice, a lower false-positive rate would also be operationally important, as unnecessary transaction blocking can negatively affect customer experience and service quality although, again, this inference is drawn from the synthesized literature rather than from direct measurement at Indonesian banks. Regarding detection speed, the reviewed literature consistently associates Big Data Analytics-based systems with near real-time detection (within seconds of a transaction occurring), compared with the post-audit, manual-verification approach of conventional systems, which several studies suggest can delay detection by months; these figures should likewise be read as reported patterns from secondary sources rather than benchmarks validated on Indonesian data.

4.3.1 Summary of Reviewed Literature

Table 5 summarizes a representative subset of the literature synthesized in this study, illustrating the range of research focus, method, and key findings that inform Sections 4.1–4.4.

Table 5. Representative summary of the reviewed literature

Author(s), Year	Research Focus	Method/Approach	Key Finding
Ngai et al. (2011)	Data mining in financial fraud detection	Literature review	ML substantially improves detection accuracy vs. traditional methods
West & Bhattacharya (2016)	Intelligent financial fraud detection	Comprehensive review	Ensemble models (RF, XGBoost) yield more stable performance on imbalanced data
Jensen & Meckling (1976)	Agency theory foundations	Conceptual/theoretical	Information asymmetry drives moral hazard; monitoring mechanisms mitigate it
Ali et al. (2022)	ML-based financial fraud detection	SLR	Confirms ML outperforms rule-based systems across multiple algorithms
Bao et al. (2020)	Detecting accounting fraud in U.S. public firms	ML models on financial statement data	Deep learning outperforms manual auditor inspection
Chen & Li (2023)	Real-time fraud detection in banking	Review	Real-time ML systems reduce detection lag and false positives
Abdullah & Mahidin (2024)	Big Data Analytics for banking fraud detection	SLR	Confirms full-population analysis advantage over sampling
Deloitte (2024)	Global banking fraud trends	Industry report	Fraud losses continue to rise despite technology investment
Faccia (2024)	Big Data Analytics applications in AIS	Conceptual	Articulates AIS's evolving role as an analytics-integrated control system
Patil et al. (2024)	ML integration in banking fraud detection	Applied study	Reports measurable accuracy gains from ML integration
Shalhoob et al. (2024)	Big Data Analytics for errors/fraud in accounting	Empirical	Analytics improves error and fraud detection in accounting processes
Widjaja et al. (2022)	Digital banking fraud trends in Indonesia	Applied/contextual	Confirms rising digital fraud threats align with Indonesia's digitalization pace
Yanto et al. (2024)	Best ML model for banking fraud detection	SLR	Compares ML models; supports ensemble approaches for banking data
Hafez et al. (2025)	AI-enhanced techniques in credit card fraud detection	SLR	AI-enhanced techniques show consistent accuracy improvements
Gkegkas (2025)	Data analytics in financial statement fraud detection	SLR	Reinforces analytics' role in financial statement fraud detection
Sitanggang et al. (2025)	Big Data Analytics in fraud detection & performance forecasting	Applied, Indonesia context	Supports feasibility of Big Data Analytics adoption within Indonesian settings
Alketbi (2025)	Real-time fraud detection using Big Data	Master's thesis	Real-time processing reduces detection lag relative to batch-based approaches
Hernandez Aros et al. (2024)	ML techniques for financial fraud detection	Literature review	Synthesizes comparative effectiveness of ML techniques across the reviewed studies
Najem (2025)	Advanced AI and Big Data techniques in e-finance	Conceptual/review	Discusses AI-Big Data convergence for financial risk management
Uddin (2025)	Predictive analytics for accounting fraud detection	Review	Highlights predictive analytics' role in early fraud identification

4.4 Real-Time Fraud Detection Mechanism Based on Big Data Analytics

The Big Data Analytics-based fraud detection mechanism synthesized from the reviewed literature is designed to identify suspicious transactions quickly, automatically, and in real time. Unlike conventional systems that generally identify fraud only after losses have occurred (post-audit), Big Data Analytics-based systems operate preventively through transaction analysis performed at the point the transaction occurs.

The process begins when transaction input from mobile banking, ATMs, internet banking, QR payments, or debit/credit card transactions enters the system, carrying data such as transaction amount,

timestamp, geographical location, device used, account activity pattern, and prior customer behavior. After preprocessing, the system executes machine learning scoring using models such as XGBoost (classification of complex fraud patterns), Isolation Forest (anomaly detection), and LSTM (temporal/time-series pattern recognition), producing a fraud risk score compared against a bank-defined threshold. Low-risk transactions are automatically approved; high-risk transactions trigger an alert, a temporary block, and escalation to the fraud investigation team, whose findings feed back into the model as new training data a continuous learning loop that keeps the model responsive to newly emerging fraud patterns.

This mechanism reflects the paradigm shift discussed in Section 4.1: from slow, manual, retrospective monitoring toward faster, automated, and risk-prediction-based digital systems, which the reviewed literature associates with improved detection effectiveness, strengthened transaction security, and greater public confidence in digital financial services.

4.5 Implementation Implications of Big Data Analytics in Indonesian Banking

The implementation of Big Data Analytics in AIS within Indonesia's banking sector presents significant opportunities for improving fraud detection effectiveness, allowing monitoring to shift from manual audits toward automated, real-time analysis. Nevertheless, implementation still faces challenges, including uneven digital infrastructure readiness across banks (large banks are generally better positioned than smaller banks still using legacy systems), data quality and integration barriers arising from data originating across multiple platforms, limited human resources in data science, cybersecurity, and artificial intelligence, and relatively high technology investment costs, particularly for small-scale banks.

Nonetheless, the opportunities remain considerable given the increasing volume of digital transactions, growing mobile banking usage, and regulatory support from OJK and Bank Indonesia. Implementation can therefore be approached incrementally through infrastructure strengthening, human resource development, and collaboration with technology providers.

4.6 Barriers and Recommendations for Big Data Analytics Implementation in Indonesian Banking

Although Big Data Analytics integration into AIS offers significant advantages, implementation in Indonesia's banking sector faces several complex and multidimensional barriers, most notably: technology infrastructure limitations at small and medium banks (BPR and regional banks) still dependent on legacy systems; data integration and quality issues across platforms such as core banking, mobile banking, and CRM; a shortage of human resources in data science, machine learning, and artificial intelligence; cybersecurity and data protection concerns under the Personal Data Protection Law (UU PDP) No. 27 of 2022; relatively high initial investment costs; and regulatory uncertainty due to the absence of specific, comprehensive guidance on Big Data Analytics for fraud detection. To address these barriers with clearer feasibility and priority, the following recommendations are organized by implementation horizon:

Table 6. Feasibility- and priority-ranked recommendations for Big Data Analytics implementation in Indonesian banking

Priority Horizon	Recommended Action	Primary Responsible Party
Short-term (0–1 year)	Launch phased pilot projects in high-risk transaction segments (e.g., mobile banking transfers); begin structured data science/AI training for existing staff	Individual banks, with technical guidance from OJK
Medium-term (1–3 years)	Adopt hybrid cloud and open-source tools (e.g., Apache Spark, TensorFlow) to reduce investment cost; strengthen data governance and cross-platform data integration	Banks with technology vendors, under data-governance oversight from OJK and Bank Indonesia
Long-term (3+ years)	Establish a machine learning-based inter-bank fraud information-sharing platform (similar to Singapore's COSMIC); issue specific OJK/BI technical guidelines and regulatory sandboxes; provide fiscal incentives especially for BPR/regional banks	OJK and Bank Indonesia (as lead regulators), together with the national banking association and an industry consortium

Collaboration among stakeholders banks, OJK, Bank Indonesia, academics, and fintech companies is critical across all three horizons, alongside ethical AI principles and sound data governance to ensure that Big Data Analytics implementation protects customer privacy while fulfilling regulatory compliance requirements.

5. Discussion and Conclusions

The findings of this Systematic Literature Review demonstrate that the integration of Big Data Analytics into Accounting Information Systems (AIS) makes a significant contribution, as reported across the reviewed literature, to improving fraud detection effectiveness in the banking sector. Conventional AIS still widely in use today tend to be reactive, relying on manual audits, sampling inspections, and rigid rule-based systems approaches that are increasingly strained by the volume and complexity of digital banking transactions, which reached IDR 52,545 trillion in 2022 (Bank Indonesia, 2023).

By contrast, Big Data Analytics integration enables AIS to conduct full population analysis of transaction data comprehensively and in real time. Leveraging machine learning, anomaly detection, predictive analytics, pattern recognition, and continuous learning, the reviewed literature reports systems identifying abnormal transaction patterns with higher accuracy than conventional methods findings consistent with Ngai et al. (2011), West and Bhattacharya (2016), Bao et al. (2022), and Faccia (2024).

Theoretically, this study reinforces the Fraud Triangle Theory (Cressey, 1953) by showing how Big Data Analytics narrows the 'opportunity' factor central to fraud, and supports Agency Theory (Jensen & Meckling, 1976) by demonstrating how Big Data-based systems can reduce information asymmetry between management and stakeholders, thereby minimizing moral hazard risk. From the Technology Acceptance Model perspective (Davis, 1989), the integration also carries high adoption potential where benefits and ease of use are clearly demonstrated to banking decision-makers.

Conclusion

Based on the synthesis of 42 reviewed articles, this study concludes that integrating Big Data Analytics into Accounting Information Systems is an effective strategic solution for improving fraud detection in Indonesia's banking sector, directly addressing the three research questions posed in Section 1.2. The performance evidence and theoretical rationale are detailed in Sections 4.3 and 5; in brief, the reviewed

literature indicates that (1) Big Data Analytics-based systems are reported to outperform conventional systems in accuracy, false-positive rate, and detection speed through full-population, real-time analysis; (2) an effective architecture comprises the five interconnected layers described in Section 4.2, operating alongside the real-time scoring-and-escalation workflow set out in Section 4.4; and (3) the principal implementation barriers can be addressed through the phased, priority-ranked roadmap in Table 6.

This paradigm shift from reactive to predictive and preventive monitoring carries meaningful implications for reducing the IDR 3.02 trillion in fraud losses reported for 2022 (OJK, 2023), while also strengthening public confidence, improving operational efficiency, and reinforcing the resilience of the national financial system.

Theoretically, this research contributes by integrating Big Data Analytics-AIS technology literature with fraud detection theory in the context of a developing country, and by reinforcing the applicability of Fraud Triangle Theory and Agency Theory in the digital era. Practically, the findings can serve as reference material for banking management, regulators (OJK and Bank Indonesia), and accounting practitioners designing digital transformation strategies banks are advised to begin implementation incrementally through pilot projects in high-risk areas, following the priority horizons in Table 6. More intensive collaboration among the banking industry, government, academics, and technology providers is needed to accelerate equitable technology adoption, including among BPRs and regional banks, while attending closely to data governance, cybersecurity, customer privacy protection, and human resource development.

6. Limitations of Research

This study has several limitations. First, as an SLR, all analysis depends on secondary data academic journals, industry reports, and regulatory publications rather than direct empirical testing at specific banking institutions, so findings are conceptual and theoretical rather than validated against actual operational data. Second, a significant portion of the reviewed literature originates from international, developed-country research; differences in Indonesia's digital infrastructure readiness, data integration quality, human resource capability, and data protection regulation mean findings cannot be fully generalized to all Indonesian banks, particularly BPRs and regional banks. Third, the discussion emphasizes technological effectiveness more than organizational implementation factors such as investment cost analysis, cultural readiness, or user resistance to digital transformation, and does not examine in detail the ethical dimensions of Big Data Analytics and AI use in managing customer transaction data.

Future research is recommended to conduct direct empirical testing at banking institutions through quantitative, case study, or mixed-methods approaches, and to develop more specific measurement models linking data quality, digital infrastructure readiness, and human resource capability to the success of Big Data Analytics-based fraud detection implementation in Indonesia's banking sector.

References

Abdullah, T. A. A., & Mahidin, M. F. (2024). Big data analytics for fraud detection in banking: A systematic review. Journal of Financial Crime, 31(2), 456–478.

Alketbi, A. M. (2025). Real-time fraud detection using big data [Master's thesis]. Rochester Institute of Technology.

Ali, A., et al. (2022). Financial fraud detection based on machine learning: A systematic literature review. Applied Sciences, 12(19), 9637. https://doi.org/10.3390/app12199637

Association of Certified Fraud Examiners. (2024). Occupational fraud 2024: A report to the nations.

Bank Indonesia. (2023). Laporan perkembangan digital banking Indonesia 2022 [Indonesia digital banking development report 2022].

Bao, Y., et al. (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

Chen, Z., & Li, Y. (2023). Real-time fraud detection in banking using machine learning: A review. Expert Systems with Applications, 225, 120135.

Deloitte. (2024). Global banking fraud report 2024. Deloitte Insights.

Faccia, A. (2024). Big data applications in accounting information systems. ACM Transactions on Management Information Systems.

Gkegkas, M. (2025). Using data analytics in financial statement fraud detection: A systematic literature review. Journal of Risk and Financial Management, 18(11), 598.

Hafez, I. Y., et al. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. Journal of Big Data, 12(6).

Hernandez Aros, L., et al. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. Humanities and Social Sciences Communications.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360.

Najem, R. (2025). Advanced AI and big data techniques in E-finance. Financial Innovation.

Ngai, E. W. T., et al. (2011). The application of data mining techniques in financial fraud detection. Decision Support Systems, 50(3), 559–569.

Otoritas Jasa Keuangan. (2023). Laporan pengawasan perbankan Indonesia 2023 [Indonesia banking supervision report 2023].

Otoritas Jasa Keuangan. (2024). Roadmap transformasi digital perbankan Indonesia 2024–2028 [Indonesia banking digital transformation roadmap 2024–2028].

Patil, A., et al. (2024). Enhancing fraud detection in banking by integration of machine learning. SoftwareX.

Romney, M. B., & Steinbart, P. J. (2021). Accounting information systems (15th ed.). Pearson.

Shalhoob, H., et al. (2024). The impact of big data analytics on the detection of errors and fraud in accounting processes. Revista de Gestão Social e Ambiental, 18(1), e06115.

Sitanggang, C. M., et al. (2025). Pemanfaatan Big Data Analytics dalam Deteksi Fraud dan Peramalan Kinerja Keuangan [Utilization of Big Data Analytics in Fraud Detection and Financial Performance Forecasting]. Jurnal Akuntansi.

Uddin, M. S. (2025). Predictive analytics for accounting fraud detection. HAL Open Science.

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. Computers & Security, 57, 47–66.

Widjaja, A., Nugroho, L., & Pramono, T. (2022). Digital banking fraud trends in Indonesia during post-pandemic transformation. Journal of Banking and Finance Technology, 5(2), 88–102.

Yanto, Y., et al. (2024). The best machine learning model for fraud detection in banking sector: A systematic literature review. ResearchGate.