American Journal of Interdisciplinary Studies

Volume: 4; **Issue:** 3
Pages: 250-286
eISSN: 3067-5146

Machine Learning–Based Fraud Detection and Conventional Audit Approaches in Government Deposit Processing

S M Arif Al Sany[1]; H M Mahir Uddin[2];

[1]. *Master of Science in Management Information Systems (continuing), Lamar University, Texas, USA; Email: alsany25@gmail.com*

[2]. *MBA in Business Analytics (continuing), Lubin School of Business, Pace University, USA Email: mahir.uddin@pace.edu*

Doi: 10.63125/fve5zp98
Received: *21 June 2023;* ***Revised:*** *27 July 2023;* ***Accepted:*** *29 August 2023;* ***Published:*** *30 September 2023;*

Abstract

This study investigates the problem of fraud vulnerability in government deposit processing, where duplicate entries, delayed reconciliation, unauthorized adjustments, false receipts, abnormal deposit timing, and inconsistent depositor records can weaken public financial accountability and reporting reliability. The purpose of the study was to examine how machine learning based fraud detection and conventional audit approaches influence fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength in public sector deposit environments. A quantitative, cross sectional, case-based research design was adopted, using structured survey data from 200 professionals representing government finance, accounting, internal audit, external audit, compliance, treasury operations, IT audit, and enterprise financial system cases. The key variables included machine learning based fraud detection, conventional audit approaches, fraud detection effectiveness, audit efficiency, reporting reliability, financial control strength, deposit fraud risk signals, and comparative trust between machine learning and traditional audit methods. The analysis plan involved descriptive statistics, Cronbach's alpha reliability testing, Pearson correlation analysis, regression modeling, hypothesis testing, fraud risk signal mapping, and comparative trust indexing. The findings showed strong support for machine learning based fraud detection, with a mean score of 4.21 and SD of 0.61, compared with conventional audit approaches at M = 3.89 and SD = 0.68. Fraud detection effectiveness recorded M = 4.12, audit efficiency M = 4.05, reporting reliability M = 4.08, and financial control strength M = 4.16. Reliability values were acceptable, ranging from 0.82 to 0.90. Correlation results showed that machine learning based fraud detection had a strong positive relationship with fraud detection effectiveness, $r = 0.71$, $p < 0.01$, while conventional audit approaches also showed a significant relationship, $r = 0.58$, $p < 0.01$. Regression results confirmed that machine learning and conventional audit together explained 47% of fraud detection effectiveness, with machine learning showing the stronger effect, $\beta = 0.52$, $p < 0.001$. The findings imply that government agencies should integrate machine learning screening with audit verification to improve accountability, detection speed, evidence reliability, and financial control.

Keywords

Machine Learning Fraud Detection; Conventional Audit; Government Deposit Processing; Audit Efficiency; Financial Control Strength;

INTRODUCTION

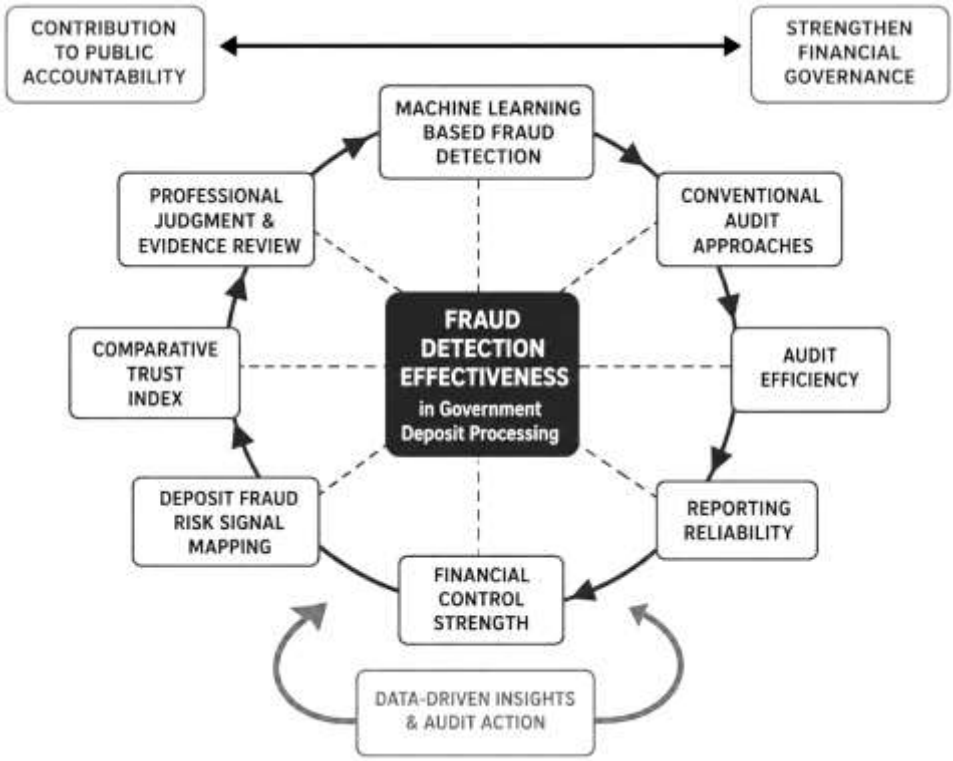
Fraud detection refers to the systematic process of identifying, examining, and responding to deceptive financial activities that distort the accuracy, legitimacy, or accountability of recorded transactions. In government deposit processing, fraud detection is especially important because deposits represent public money collected, transferred, posted, reconciled, and reported through administrative and financial systems (Abdallah et al., 2016). Government deposit processing may include tax deposits, agency collections, public service payments, treasury receipts, intergovernmental transfers, grant-related deposits, and other revenue inflows handled through public-sector accounting systems. Conventional audit approaches refer to traditional audit procedures such as document verification, sampling, reconciliation, authorization review, compliance testing, and professional judgment (Appelbaum et al., 2017). Machine learning–based fraud detection refers to the use of computational algorithms that learn from historical data to identify suspicious patterns, anomalies, unusual transaction behavior, or high-risk financial activities. Earlier fraud detection studies established that financial fraud can be examined through statistical analysis, data mining, classification, anomaly detection, and decision-support systems. In this research, machine learning is understood not as a replacement for auditing, but as a data-driven support mechanism that can strengthen fraud screening in deposit-related transactions (Brown-Liburd et al., 2015). This distinction is important because government deposit fraud may appear in subtle forms such as duplicate entries, delayed posting, false receipts, unauthorized adjustments, misclassification of funds, or manipulation of reconciliation records. Financial fraud analytics literature indicates that machine learning tools can support the detection of hidden relationships in financial data when transaction volume, data variety, and manual review limitations reduce the efficiency of traditional procedures (Jans et al., 2010). Audit research also emphasizes that professional skepticism, evidence evaluation, internal control review, and contextual judgment remain central to fraud-related assurance work. Therefore, the introduction of this study begins from the position that government deposit processing requires both technological detection capacity and audit-based control discipline (Branco et al., 2016).

The international significance of this research is connected to the global importance of public financial accountability. Governments across different administrative systems depend on accurate deposit processing to finance public services, maintain budget credibility, support fiscal planning, and preserve public trust. When deposit records are manipulated, delayed, duplicated, or wrongly classified, the problem becomes more than a technical accounting error because it can weaken revenue transparency, distort public-sector reports, and reduce confidence in financial governance (Bierstaker et al., 2006). International fraud research has shown that financial misconduct affects public agencies, corporations, financial institutions, regulators, and citizens because fraud risk is not limited to one industry or one country. Fraud risk has also become an institutional governance issue because organizations are expected to design systems that prevent, detect, investigate, and document irregularities before they become larger control failures. Government deposit processing is especially sensitive because it involves a chain of custody between payers, receiving offices, banks, treasury units, accounting departments, auditors, and reporting authorities (Cecchini et al., 2010). Each stage can create opportunities for error or manipulation when internal controls are weak or monitoring is delayed. Studies on internal fraud and audit analytics indicate that transaction-level data can reveal process deviations, control violations, and unusual behavior that may not be visible through ordinary document review alone. Machine learning adds relevance to this international concern because fraud detection has moved from isolated manual investigation toward broader risk scoring, pattern recognition, and population-level transaction monitoring (Ngai et al., 2011). For public-sector deposit systems, this means that fraud detection can be studied as a measurable relationship between machine learning adoption, conventional audit strength, detection effectiveness, audit efficiency, reporting reliability, and financial control. This international relevance supports the need for a quantitative, cross-sectional, case-study–based study focused on government deposit processing (Kuhn & Sutton, 2010).

Conventional audit approaches have historically played a central role in fraud detection because they provide structured procedures for examining financial records, validating documentation, testing controls, and evaluating whether transactions comply with established rules. In deposit processing, conventional audit procedures may include checking deposit slips, verifying bank confirmations,

comparing receipts with ledgers, reviewing authorization trails, testing segregation of duties, and confirming whether reconciliation differences are properly explained. These procedures remain valuable because public financial systems require evidence, accountability, and defensible audit opinions. Research on fraud prevention and detection methods shows that accountants, internal auditors, and fraud examiners rely on tools such as internal controls, external audits, operational audits, fraud hotlines, forensic review, and software-supported procedures, with perceived effectiveness varying according to context and organizational capacity (Craja et al., 2020). Audit research also emphasizes that fraud detection is not only a mechanical procedure; it requires professional skepticism, judgment, risk assessment, and interpretation of evidence. In government deposit processing, this matters because an unusual deposit pattern may be a legitimate administrative delay, a recording mistake, or a deliberate manipulation (Lessmann et al., 2015). Conventional audit judgment helps distinguish these possibilities through documentary evidence and contextual inquiry. Continuous auditing and ERP-based audit research also show that traditional auditing has adapted to computerized environments through more frequent review, automated control testing, and closer integration with enterprise systems. Even within data-rich environments, auditors must evaluate whether the evidence is reliable, complete, relevant, and properly authorized. Process mining research further shows that audit procedures can benefit from analyzing event logs and business-process records because such records expose actual process behavior rather than only reported outcomes. In this study, conventional audit approaches are therefore treated as a key independent variable, not as an outdated practice (Ravisankar et al., 2011). Their role is examined alongside machine learning to determine how manual verification, compliance review, reconciliation testing, and professional judgment contribute to fraud detection effectiveness in government deposit processing.

Figure 1: Hybrid Fraud Detection Framework for Government Deposit Processing



Machine learning–based fraud detection has developed from the broader field of data mining, artificial intelligence, and decision-support systems. In financial fraud research, machine learning models have been applied to credit card fraud, insurance fraud, financial statement fraud, tax-related fraud, internal fraud, and other forms of suspicious financial activity. Machine learning is useful in this area because fraudulent transactions are often hidden inside large volumes of normal transactions. Algorithms such as decision trees, neural networks, support vector machines, logistic regression, random forests,

ensemble learning, and anomaly detection methods can classify high-risk records, rank suspicious cases, or identify patterns that differ from normal behavior (Trompeter et al., 2013). In financial statement fraud detection, structured and computational models can identify fraud-related signals from financial ratios, textual disclosures, and other structured or unstructured indicators. In transaction-based fraud detection, network-based and behavior-based approaches can improve fraud screening by examining relationships among customers, merchants, accounts, or transaction histories. These insights are highly relevant to government deposit processing because public deposits also produce transaction records, timestamps, authorization histories, payer information, receipt numbers, account codes, reconciliation records, and exception reports. A machine learning model can be designed to identify duplicate deposits, unusually timed deposits, unmatched receipts, repeated manual adjustments, abnormal account-code changes, or suspicious reconciliation delays. Machine learning research also draws attention to class imbalance because fraud cases are usually much fewer than legitimate transactions, making detection accuracy more complex than ordinary classification (Van Vlasselaer et al., 2015). For this reason, this study treats machine learning–based fraud detection as a measurable construct that may improve detection accuracy, audit efficiency, reporting reliability, and financial control strength when applied to government deposit processing.

The relationship between machine learning and audit work is especially important because fraud detection in government deposit processing requires both scale and trust (Perols, 2011). Machine learning can process large transaction populations, identify risk signals, and prioritize suspicious cases for review, while auditors can interpret the evidence, examine supporting documents, verify compliance requirements, and determine whether a transaction irregularity indicates fraud, error, or administrative exception. Audit analytics studies show that the accounting and auditing professions have increasingly examined big data, analytics, process mining, and automated procedures as tools for improving audit planning, substantive testing, control evaluation, and decision support. Big data research in accounting explains that financial assurance environments now include structured, semi-structured, and unstructured information, creating new opportunities for analytical review and evidence generation (Power, 2013). Audit judgment research adds that data analytics can increase information availability, but auditors must manage relevance, ambiguity, information overload, and pattern interpretation when using analytics-based evidence. In government deposit processing, this means a machine-generated fraud alert must be understandable enough for auditors and finance officers to act on it. A risk score without clear evidence may not be sufficient for public accountability, while a manual audit without broad transaction coverage may fail to identify dispersed patterns across agencies, accounts, or time periods. Studies on internal fraud risk reduction and process mining show that data-driven analysis can reveal hidden process deviations and control weaknesses that may support fraud prevention and detection (Vasarhelyi et al., 2015). Therefore, the present study is positioned around a hybrid logic: machine learning contributes analytical coverage and pattern detection, while conventional audit contributes evidence verification, professional skepticism, and governance discipline. This combination is particularly suitable for a quantitative study because the perceived effectiveness of each approach can be measured using Likert-scale questionnaire items and statistically examined through descriptive statistics, correlation analysis, and regression modeling (Earley, 2015).

Government deposit processing also provides a distinctive research setting because deposit fraud may occur through operational pathways that differ from private-sector fraud. In private organizations, fraud detection studies often focus on customer transactions, credit risk, insurance claims, financial statements, or corporate reporting (Glancy & Yadav, 2011). In government deposit processing, the fraud risk environment is shaped by public money, administrative rules, treasury procedures, budget classifications, agency-level reporting, bank reconciliation, and audit accountability. Fraud may arise when deposit records are intentionally delayed, receipts are falsified, deposits are posted to incorrect accounts, adjustment entries are made without authority, reconciliation exceptions are ignored, or the same transaction is recorded more than once. These risks align with the broader fraud-risk literature, which treats fraud as a governance and control problem involving opportunity, detection, accountability, and organizational responsibility (He & Garcia, 2009). Machine learning can support this setting by mapping fraud risk signals across deposit records, identifying unusual relationships

among deposit timing, account codes, adjustment frequency, and reconciliation status. Conventional audit can support the same setting by reviewing authorization, confirming documentary evidence, and determining whether control procedures were followed. Data mining studies show that fraud detection benefits from selecting relevant features, testing classification models, and comparing algorithms under practical cost and accuracy conditions (Kirkos et al., 2007). This is useful for the present research because government deposit fraud detection is not only about whether fraud exists; it is also about whether the system can detect warning signals early, allocate audit effort efficiently, and produce reliable reports. The study's unique result sections, such as Deposit Fraud Risk Signal Mapping and Comparative Trust Index, directly match this setting (Jans et al., 2009). Deposit Fraud Risk Signal Mapping can rank the most important deposit-specific fraud indicators, while the Comparative Trust Index can measure respondents' confidence in machine learning and conventional audit across dimensions such as speed, accuracy, transparency, evidence reliability, professional judgment, and real-time monitoring.

This research is designed as a quantitative, cross-sectional, case-study–based study because the topic requires measurable evidence from professionals who understand government deposit processing, auditing, accounting, compliance, treasury operations, or financial systems. A five-point Likert scale is appropriate because the study examines perceptions of machine learning–based fraud detection, conventional audit approaches, fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength (Jans et al., 2014). Prior studies in fraud detection and audit analytics have used quantitative comparisons, classification performance, survey evidence, and structured measurement to examine how detection tools perform or how professionals perceive fraud-related methods (West & Bhattacharya, 2016). Descriptive statistics can summarize the level of agreement among respondents regarding the usefulness of machine learning and conventional audit. Correlation analysis can show whether machine learning adoption, conventional audit strength, audit efficiency, reporting reliability, and financial control strength are statistically associated. Regression modeling can test whether machine learning–based fraud detection and conventional audit approaches significantly predict fraud detection effectiveness in government deposit processing. Reliability analysis using Cronbach's alpha can assess whether the questionnaire items consistently measure each construct. The study also draws from research on imbalanced financial data, audit analytics, and fraud risk to justify why detection effectiveness should be examined through multiple dimensions rather than one single measure. In this structure, the introduction establishes the research foundation by defining the key concepts, explaining the international significance of fraud detection in public financial systems, connecting machine learning with conventional audit practice, and locating government deposit processing as a specific case-study setting. The study therefore begins from a measurable research problem: whether machine learning–based fraud detection and conventional audit approaches significantly explain fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength in government deposit processing.

Background of the Study

Government deposit processing is a critical financial function through which public funds are received, recorded, verified, reconciled, and reported within government accounting and treasury systems. These deposits may include tax revenues, public service payments, licensing fees, grants, penalties, interagency transfers, and other forms of government income that must be accurately captured and protected. Because government deposits involve public money, the process requires a high level of transparency, accountability, accuracy, and internal control. Any weakness in deposit processing may create opportunities for fraud, misstatement, delayed reconciliation, unauthorized adjustment, duplicate recording, false documentation, or misclassification of public funds. Traditionally, government agencies have depended on conventional audit approaches to detect and prevent fraud. These approaches include manual verification, document review, sampling, compliance testing, reconciliation checks, and professional judgment by auditors. While these methods remain important, modern government financial environments are becoming more complex because of increasing transaction volumes, digital payment systems, multi-agency financial flows, and the need for faster detection of irregularities. Machine learning–based fraud detection has therefore become relevant because it can analyze large datasets, identify unusual transaction patterns, classify high-risk deposits,

and support automated alert generation. In the context of government deposit processing, machine learning may assist auditors and finance officers by detecting suspicious timing patterns, repeated adjustments, duplicate deposit records, unmatched receipts, and abnormal reconciliation behavior. However, conventional audit approaches still provide essential human judgment, evidence verification, and compliance interpretation. This study is therefore positioned at the intersection of machine learning–based fraud detection and conventional audit practice. It examines how both approaches contribute to fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength. By focusing specifically on government deposit processing, the study addresses a public-sector financial control area where both technological tools and traditional audit discipline are necessary for safeguarding public resources.

Problem Statement

Government deposit processing remains vulnerable to fraud and control weaknesses because deposits pass through multiple administrative, financial, banking, and reporting stages before they are fully reconciled and confirmed. In many public-sector environments, fraud may occur through duplicate deposit entries, delayed recording, unauthorized transaction adjustments, false receipts, incorrect account classification, missing documentation, or manipulation of reconciliation records. Conventional audit approaches are widely used to detect these problems, but they often depend on periodic review, manual inspection, sampling, and after-the-fact verification. These procedures may not always detect unusual transaction patterns quickly, especially when large volumes of deposit records are processed across different departments or agencies. The problem becomes more serious when auditors must review complex transaction histories with limited time, incomplete documentation, or fragmented information systems. Machine learning–based fraud detection offers a possible solution by identifying patterns, anomalies, and high-risk transactions across larger datasets. However, the use of machine learning in government deposit processing also raises practical concerns related to trust, interpretability, data quality, system readiness, and the continued role of professional audit judgment. A machine learning system may identify suspicious deposits, but auditors still need to verify whether those alerts represent actual fraud, administrative error, or legitimate exceptions. At the same time, conventional audit procedures may provide strong evidence and accountability but may lack the speed and scalability required for modern deposit monitoring. The main research problem is therefore the limited empirical understanding of how machine learning–based fraud detection and conventional audit approaches jointly or separately influence fraud detection effectiveness in government deposit processing. There is also a need to examine whether machine learning improves audit efficiency, reporting reliability, and financial control strength when compared with conventional audit methods. This study responds to that problem by using a quantitative, cross-sectional, case-study–based design to measure the relationship between machine learning–based fraud detection, conventional audit approaches, and major fraud control outcomes.

ObjectiveS of The Study

The main objective of this study is to examine the role of machine learning–based fraud detection and conventional audit approaches in improving fraud detection effectiveness within government deposit processing. The study aims to determine whether machine learning tools can strengthen the identification of suspicious deposit activities by detecting unusual patterns, duplicate records, abnormal transaction timing, unauthorized adjustments, delayed reconciliation, and other deposit-related fraud risk signals. Another objective is to evaluate the contribution of conventional audit approaches in the same context, particularly in relation to document verification, reconciliation review, compliance testing, internal control assessment, and professional judgment. The study also seeks to compare machine learning–based fraud detection with conventional audit approaches in terms of perceived accuracy, speed, reliability, transparency, and usefulness for public-sector financial control. In addition, the research intends to assess whether machine learning–based fraud detection has a significant relationship with audit efficiency, especially by reducing manual workload, improving risk prioritization, and supporting faster review of suspicious transactions. The study further aims to investigate whether machine learning and conventional audit approaches contribute to reporting reliability by improving the accuracy, completeness, and credibility of government deposit records. Another objective is to examine how fraud detection effectiveness, audit efficiency, and reporting

reliability may strengthen financial control in government deposit processing. Since this study uses a quantitative research design, these objectives will be tested through structured questionnaire data collected from professionals with knowledge of government finance, auditing, accounting, treasury operations, compliance, or financial systems. The use of descriptive statistics, correlation analysis, and regression modeling will allow the study to measure respondent perceptions and test the statistical relationships among the study variables. Through these objectives, the research focuses on producing measurable evidence about how technology-based fraud detection and conventional audit practice can support stronger accountability in public-sector deposit management.

Research Hypotheses

The hypotheses of this study are developed to test the statistical relationships among machine learning–based fraud detection, conventional audit approaches, fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength in government deposit processing. Since the study is quantitative in nature, the hypotheses provide a clear basis for measuring whether the independent variables significantly influence the dependent and supporting outcome variables. The first hypothesis proposes that machine learning–based fraud detection has a significant positive effect on fraud detection effectiveness in government deposit processing. This means that the use of machine learning tools is expected to improve the ability to identify suspicious deposits, unusual transaction patterns, duplicate entries, unauthorized adjustments, and delayed reconciliation issues. The second hypothesis proposes that conventional audit approaches have a significant positive effect on fraud detection effectiveness. This means that manual verification, compliance testing, document review, reconciliation checks, and professional judgment are expected to remain important in detecting fraud in deposit processing. The third hypothesis proposes that machine learning–based fraud detection has a significant positive effect on audit efficiency. This suggests that automated risk scoring, anomaly detection, and transaction screening may reduce audit workload and help auditors focus on high-risk cases. The fourth hypothesis proposes that machine learning–based fraud detection has a significant positive effect on reporting reliability. This means that the use of automated detection tools may improve the accuracy and credibility of deposit-related financial reports. The fifth hypothesis proposes that audit efficiency has a significant positive effect on financial control strength. This suggests that when audit work becomes faster, more focused, and more systematic, government deposit control systems may become stronger. The sixth hypothesis proposes that machine learning–based fraud detection has a stronger predictive effect on fraud detection effectiveness than conventional audit approaches. Together, these hypotheses allow the study to test whether machine learning and conventional audit approaches individually and comparatively contribute to fraud detection and financial control in government deposit processing.

Significance of the Research

This study is significant because it focuses on government deposit processing, which is directly connected to the protection of public funds. By examining fraud detection in this area, the research may help government finance departments understand how deposit records, reconciliation systems, and financial reporting procedures can be strengthened. The study is useful for internal auditors, external auditors, and public-sector audit institutions because it compares conventional audit approaches with machine learning–based fraud detection. It shows how traditional audit procedures can be supported by automated tools without removing the need for professional judgment and evidence verification.

The research contributes to fraud detection practice by identifying how suspicious deposit activities can be detected through both manual and automated methods. The inclusion of Deposit Fraud Risk Signal Mapping makes the study more specific because it connects fraud detection with actual deposit-related risk indicators such as duplicate entries, delayed reconciliation, and unauthorized adjustments. The study provides value for policymakers, system designers, and IT audit professionals by examining whether machine learning tools are trusted and useful in public-sector financial systems. The Comparative Trust Index can help explain how professionals perceive machine learning compared with conventional audit methods. The study adds to academic knowledge by focusing on a specific public-sector financial process rather than general financial fraud. It offers a quantitative model that connects machine learning–based fraud detection, conventional audit approaches, audit efficiency, reporting reliability, and financial control strength. By studying fraud detection in government deposit

processing, the research supports the broader goal of improving accountability, transparency, and responsible management of public resources. Stronger fraud detection can help reduce financial irregularities and improve confidence in public financial reporting.

LITERATURE REVIEW

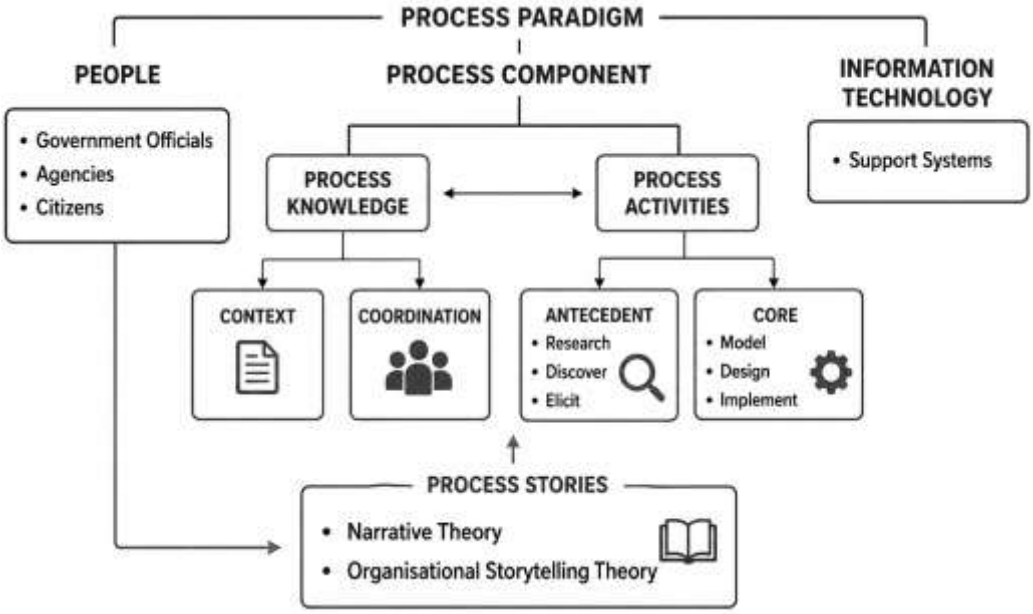
The literature on machine learning–based fraud detection and conventional audit approaches provides a strong foundation for examining fraud detection effectiveness in government deposit processing. Fraud detection has been widely discussed as a financial control activity that involves identifying suspicious, deceptive, or unauthorized activities within accounting and transaction systems. In public-sector financial management, the detection of fraud is closely connected to accountability, transparency, internal control, reporting accuracy, and the protection of public funds. Government deposit processing is a specialized area within this broader field because it involves the collection, recording, verification, reconciliation, and reporting of public revenues or receipts. The literature suggests that fraud risks may emerge when deposit systems are affected by weak controls, incomplete documentation, delayed reconciliation, manual processing errors, poor segregation of duties, or limited transaction monitoring. Conventional audit approaches have traditionally addressed these risks through document examination, sampling, compliance review, reconciliation testing, authorization checks, and professional judgment. These approaches remain important because they provide evidence-based assurance and support accountability in financial reporting. However, the growing volume and complexity of financial transactions have increased the need for analytical and technology-supported fraud detection methods. Machine learning–based fraud detection has therefore become an important research area because it can process large datasets, identify hidden patterns, detect anomalies, classify high-risk transactions, and generate alerts for further audit review. Literature on audit analytics also shows that data-driven tools can improve audit planning, risk assessment, and control testing when properly integrated with professional audit procedures. Within this study, the literature review is organized around the relationship between government deposit processing, fraud risks, conventional audit methods, machine learning–based detection, theoretical explanation, and conceptual modeling. Fraud Triangle Theory is especially relevant because it explains fraud through pressure, opportunity, and rationalization, while this study focuses mainly on reducing opportunity through stronger detection, monitoring, and control systems. The conceptual framework connects machine learning–based fraud detection and conventional audit approaches with fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength. Therefore, the literature review establishes the academic and practical basis for testing the study's hypotheses through a quantitative, cross-sectional, case-study–based design.

Government Deposit Processing and Public Financial Accountability

Government deposit processing refers to the structured administrative and accounting procedure through which public funds are received, recorded, classified, deposited, reconciled, verified, and reported within government financial systems. In public-sector finance, deposits may come from taxes, service fees, fines, grants, permits, licenses, intergovernmental transfers, and other public revenue sources. Because these funds belong to the public, deposit processing must be supported by accuracy, transparency, traceability, and accountability at every stage. Public financial accountability means that government officials, agencies, and financial officers are answerable for how public money is collected, safeguarded, recorded, and reported. Accountability is not only a general ethical expectation; it is also a formal governance mechanism through which public actors explain their actions, justify financial decisions, and become subject to evaluation or correction. This is important for deposit processing because every transaction creates a public record that must be linked to a legitimate source, proper authorization, correct accounting classification, timely bank deposit, and accurate reconciliation. When accountability is weak, deposit records may become vulnerable to errors, misclassification, manipulation, delayed posting, duplicate recording, or unauthorized adjustment. Public accountability can therefore be understood both as a virtue, meaning responsible conduct by public officials, and as a mechanism, meaning a structured process of reporting, monitoring, questioning, and enforcement (Bovens, 2010). In the context of this study, government deposit processing is closely connected to accountability because the reliability of deposits affects public financial reporting, budget credibility, audit assurance, and institutional trust. A strong deposit processing system should therefore ensure

that all received funds are properly documented, matched with bank records, posted to the correct accounts, and reviewed through internal control and audit procedures.

Figure 2: Public Financial Accountability Chain in Government Deposit Processing



Public financial accountability in deposit processing also depends on the interaction among different accountability forums, including finance departments, treasury offices, internal auditors, external auditors, legislative oversight bodies, regulatory agencies, and citizens. Government financial systems are rarely controlled by one actor alone; instead, they depend on multiple institutions that perform different functions such as collection, authorization, recording, reconciliation, reporting, and review. This multi-actor environment makes accountability more complex because one department may collect deposits, another may record them, another may reconcile them, and another may audit them. Such complexity increases the need for clear responsibility, accurate documentation, and reliable information flows. Accountability research explains that public accountability should be studied through multiple forums and functions because different actors may be responsible for different parts of the same governance process (Willems & Van Dooren, 2012). This idea is highly relevant to government deposit processing because fraud or error can occur when responsibilities are fragmented or when one stage of the process is not properly linked to another. For example, a deposit may be received by one office but recorded late by another, or a reconciliation exception may remain unresolved because responsibility is unclear. Public-sector accounting literature also shows that accounting and accountability systems shape how governments explain financial performance, manage constraints, and demonstrate responsibility for public resources (Bracci et al., 2015; Abdur & Iftekhar, 2021). Therefore, deposit processing should not be viewed only as a clerical accounting activity. It should be viewed as a public accountability chain in which each transaction must be supported by documentation, system records, authorization controls, reconciliation evidence, and audit review. This study builds on that logic by examining whether machine learning–based fraud detection and conventional audit approaches can strengthen the accountability chain surrounding government deposits.

The quality of government deposit processing has a direct relationship with financial reporting quality, governance quality, and fraud control. If deposits are recorded incorrectly, posted late, or reconciled incompletely, public financial reports may become unreliable. Poor deposit controls may also create opportunities for fraud because unauthorized adjustments, false receipts, duplicate entries, and unexplained reconciliation differences may be hidden within large transaction volumes. Public-sector financial research shows that financial reporting quality and accountability are closely connected with public organization performance, because reliable financial information supports better monitoring,

decision-making, and institutional evaluation (Tran et al., 2021). Public-sector accounting reforms are also associated with improved governance quality because standardized and reliable accounting information can reduce information asymmetry between public officials and citizens (Cuadrado-Ballesteros & Bisogno, 2021). For this reason, government deposit processing should be treated as an important component of public financial governance. A reliable deposit system does more than record incoming money; it supports audit trails, reduces opportunities for manipulation, improves budgetary accuracy, and strengthens public confidence in financial administration. In the present study, this relationship is especially important because fraud detection effectiveness depends on the quality of the deposit information available for review. Conventional audit approaches require complete documents, accurate ledgers, and reliable reconciliation records. Machine learning–based fraud detection requires clean, consistent, and structured transaction data to identify suspicious patterns. When deposit processing is weak, both audit judgment and machine learning outputs may become less reliable. Therefore, the literature suggests that government deposit processing and public financial accountability are inseparable. Strong deposit processing supports accountability, while strong accountability systems improve the reliability, transparency, and fraud resistance of public financial records.

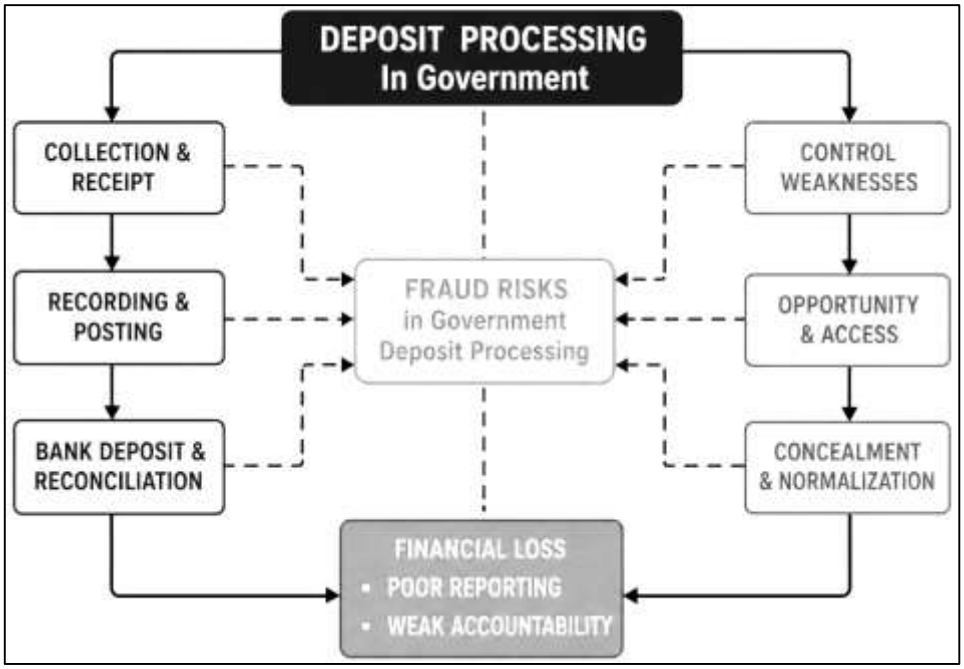
Fraud Risks in Government Deposit Processing

Fraud risks in government deposit processing refer to the possibility that public funds may be intentionally misdirected, misrecorded, concealed, duplicated, delayed, or manipulated during the collection, recording, banking, reconciliation, and reporting stages of deposit administration. These risks are important because government deposits represent public revenue and must be protected through reliable controls, accurate documentation, and accountable reporting. In deposit processing, fraud may occur when an employee or related party creates false receipts, records the same deposit more than once, delays posting to hide shortages, changes account codes without approval, alters reconciliation records, or makes unsupported adjustments after money has already entered the system (Binayan & Shakhawat, 2022; Manam & Ashfaq, 2022). Fraud risk can also arise from weak segregation of duties, poor supervision, incomplete audit trails, excessive manual processing, and limited review of unusual transactions. From a fraud-risk perspective, government deposit systems are exposed to pressure, opportunity, and rationalization because employees may face personal or institutional pressures, may observe weaknesses in the control environment, and may justify improper actions as temporary corrections, administrative shortcuts, or low-risk violations. Fraud theory explains that fraud risk assessment should not be limited to identifying dishonest individuals; it should also examine the organizational conditions that make fraud possible and difficult to detect (Golam & Amir, 2022; Atif & Murad, 2022; Dorminey et al., 2012). This is relevant to government deposit processing because fraudulent activity may not always appear as a single obvious act. It may appear through repeated small irregularities, undocumented changes, delayed reconciliations, or patterns that become visible only when records are compared across time, accounts, departments, and bank statements. Therefore, fraud risks in deposit processing should be understood as both behavioral and procedural risks. They involve human motivation, control weakness, system gaps, documentation quality, and monitoring failure. A strong literature review on this topic must therefore consider how fraud risks are created, hidden, normalized, and detected within public financial processes.

A major fraud risk in government deposit processing is the opportunity created by weak internal controls and routine trust in financial personnel. Deposit processing normally requires several steps, including receiving money, issuing receipts, entering data into accounting systems, depositing funds into bank accounts, matching deposits with source documents, and reconciling records with bank statements (Aminul & Mst Shamima, 2022; Shamsul & Sultan, 2022). When one person or one unit controls too many of these steps, the opportunity for fraud increases. For example, an officer who receives funds and also prepares reconciliation reports may be able to delay recording, conceal missing receipts, or adjust records without immediate detection. Internal control quality is therefore central to reducing employee fraud because strong controls clarify responsibilities, require approvals, preserve evidence, and create review points that make manipulation more difficult (Rae & Subramaniam, 2008). Fraud risk is also connected with professional knowledge and access. Individuals who understand accounting rules, system workflows, reconciliation procedures, and audit schedules may be able to

exploit procedural weaknesses more effectively than outsiders. In deposit processing, this means that fraud may be committed by individuals who know how to create legitimate-looking documentation, split transactions, adjust dates, or explain exceptions as ordinary administrative errors. Research on fraud offenders suggests that opportunity is often strengthened by occupational knowledge, trust, professional position, and access to records or systems (Dellaportas, 2013; Binte & Iftekhar, 2022; Taufiqur & Albert, 2022). This is highly relevant for government deposit processing because the system depends on trusted officers who handle public money and financial records. Fraud risks therefore do not only come from external cyberattacks or obvious theft; they may also come from insiders who understand how the deposit system works. In a conventional audit environment, these risks may be difficult to detect when audit procedures rely heavily on sample testing and periodic review. In a machine learning environment, these risks may be better identified when unusual patterns are examined across the full population of deposit records.

Figure 3: Fraud Risk Framework for Government Deposit Processing



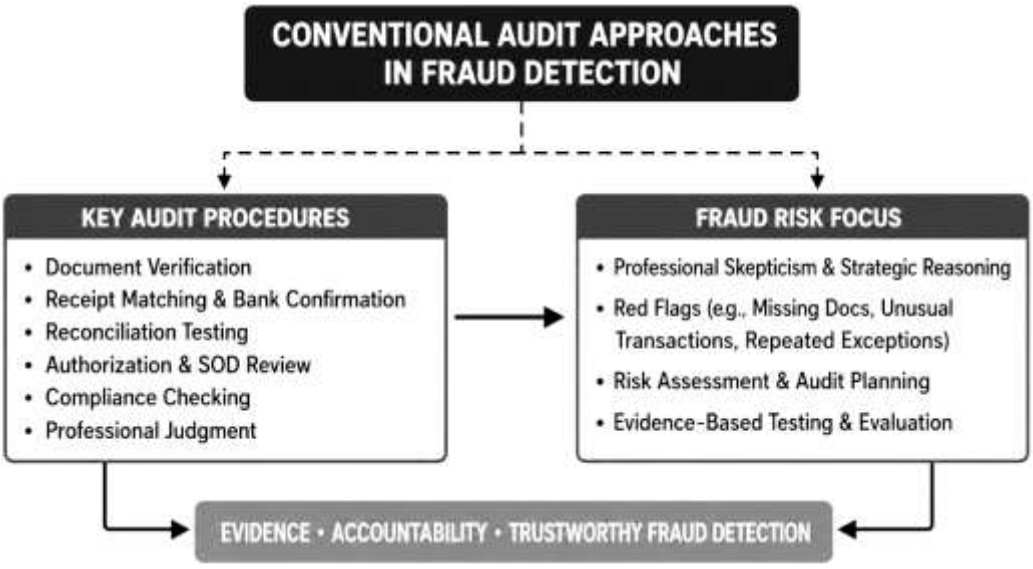
Another important fraud risk in government deposit processing is concealment through organizational routines, institutional assumptions, and narrow fraud-detection frameworks. Deposit fraud may remain hidden when irregularities are treated as ordinary processing delays, technical errors, workload problems, or harmless reconciliation differences. In many government agencies, employees may become familiar with routine exceptions, and this familiarity may reduce the urgency of investigating repeated irregularities. Fraud studies show that fraudulent conduct can become difficult to detect when institutional practices normalize questionable behavior or when organizations rely too strongly on familiar explanations for unusual events (Gabbioneta et al., 2013; Taufiqur & Khalid, 2022). This is directly related to government deposit processing because repeated delays, unsupported adjustments, or mismatched records may be accepted as administrative inefficiency rather than examined as possible fraud signals. Fraud risk may also be underestimated when detection frameworks focus only on individual pressure, opportunity, and rationalization without considering wider organizational, cultural, and contextual factors. Critical fraud literature argues that the fraud triangle can be useful, but it may provide a restricted view if it does not account for complex institutional settings, power relationships, and contextual conditions surrounding fraud (Lokanan, 2015). In the present study, this point is important because government deposit fraud may involve not only individual misconduct but also weak systems, unclear responsibility, low transparency, limited data integration, and poor accountability culture. Machine learning–based fraud detection can help reveal unusual patterns, but it requires reliable data and meaningful risk indicators. Conventional audit approaches can verify

evidence, but they require careful attention to recurring exceptions and system-level weaknesses. Therefore, fraud risks in government deposit processing should be examined through both transaction-level indicators and organizational control conditions.

Conventional Audit Approaches in Fraud Detection

Conventional audit approaches in fraud detection refer to the structured procedures used by auditors to identify, evaluate, and respond to possible irregularities in financial records, control systems, and transaction processes. In government deposit processing, these approaches include document verification, receipt matching, bank confirmation, reconciliation testing, authorization review, segregation-of-duties assessment, compliance checking, and professional judgment. These procedures are important because government deposits involve public funds that must be supported by reliable evidence and transparent accountability. Conventional auditing does not only examine whether money has been recorded; it also evaluates whether the deposit followed approved procedures, whether supporting documents are complete, whether adjustments were authorized, and whether reconciliation differences were properly investigated. In fraud detection, auditors often begin by assessing fraud risk indicators and then designing audit procedures that respond to the identified risks. Audit team discussion is one important conventional audit practice because fraud risks may be difficult for one auditor to identify alone. Group brainstorming can improve fraud-risk identification by allowing auditors to share knowledge, challenge assumptions, and generate more relevant fraud ideas during the planning stage (Carpenter, 2007). This is relevant to government deposit processing because suspicious activities may appear through small procedural inconsistencies, such as repeated late deposits, unusual adjustment patterns, missing receipt numbers, or unexplained reconciliation items. Conventional audit approaches provide a disciplined method for converting these warning signs into audit evidence. Through sampling, testing, inquiry, observation, recalculation, and inspection, auditors can determine whether irregularities represent error, weak control, or intentional manipulation. Therefore, conventional audit remains a necessary foundation for fraud detection because it links financial records with evidence, accountability, and professional evaluation.

Figure 4: Framework of Conventional Audit Approaches for Fraud Detection in Government Deposit Processing



Conventional audit approaches also depend on the quality of fraud assessment tools, audit documentation, and auditor judgment. In government deposit processing, auditors must document why certain transactions were selected, what evidence was reviewed, what exceptions were found, and how conclusions were reached. Strong documentation improves review quality because it allows audit supervisors and other stakeholders to understand the reasoning behind fraud-risk judgments. Fraud models and practice aids can also influence how auditors evaluate risk. For example, broader fraud

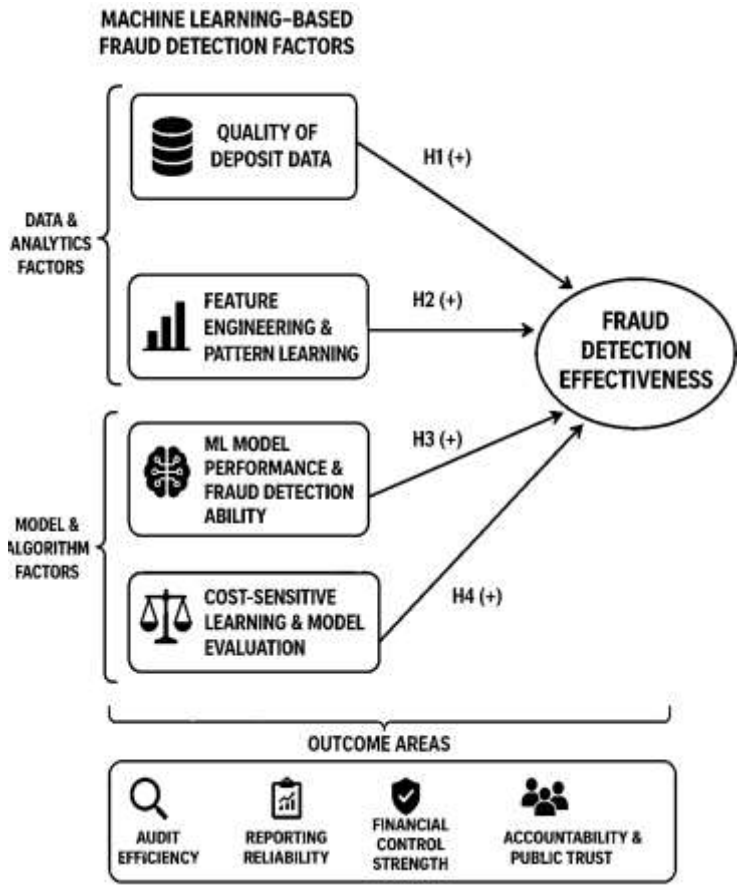
models may encourage auditors to consider additional risk dimensions beyond basic pressure, opportunity, and rationalization, which may lead to more conservative fraud-risk judgments (Boyle et al., 2015). This is useful for government deposit processing because fraud may be shaped by administrative access, system weakness, institutional culture, unclear responsibility, and weak reconciliation practices. Conventional audit approaches can also be strengthened through structured brainstorming guidance, because auditors who use clearer fraud-generation guidelines may identify more potential fraud schemes before entering team discussions (Chen et al., 2018). In relation to the present study, conventional audit approaches are treated as an independent variable because they may significantly influence fraud detection effectiveness. Their value lies in the ability to verify documents, interpret exceptions, evaluate compliance, review control weaknesses, and support accountability. While machine learning can help identify suspicious patterns across large datasets, conventional audit provides the professional judgment needed to decide whether those patterns represent fraud, error, or acceptable exceptions. Therefore, conventional audit approaches remain essential in government deposit processing because they provide the evidential, procedural, and judgment-based foundation required for trustworthy fraud detection.

Machine Learning–Based Fraud Detection

Machine learning–based fraud detection refers to the use of computational models that learn from historical transaction records to identify suspicious, irregular, or high-risk financial activities. In government deposit processing, this approach can support the detection of unusual deposit amounts, repeated receipts, delayed posting, abnormal adjustment patterns, inconsistent account classifications, and reconciliation exceptions. Unlike purely manual review, machine learning can examine a large number of records and identify hidden relationships that may not be easily visible to auditors during routine inspection. The relevance of this approach is clear in transaction environments where fraud is rare, complex, and mixed with many legitimate activities. Fraud detection research shows that classification models such as logistic regression, random forests, and support vector machines can be used to distinguish fraudulent and nonfraudulent transactions when sufficient historical data are available (Bhattacharyya et al., 2011). For government deposit systems, the same logic can be applied to deposit records by treating each transaction as an observation with measurable features, such as amount, time, payment channel, receipt status, adjustment frequency, account code, user activity, and reconciliation outcome. Machine learning can then support fraud risk screening by assigning risk scores or classifying records according to their probability of irregularity. This does not remove the need for audit judgment, because auditors still need to examine supporting documents and confirm whether a flagged deposit represents fraud, error, or a legitimate exception. However, it changes the starting point of fraud detection by allowing auditors to focus first on records that show unusual characteristics, especially when public agencies manage high-volume deposits across fragmented information systems and reconciliation workflows.

In this study, machine learning–based fraud detection is therefore treated as a technology-supported control mechanism that may improve fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength in government deposit processing. A major contribution of machine learning to fraud detection is its ability to transform raw transaction records into meaningful fraud indicators. Government deposit records may contain many data points, including receipt numbers, bank deposit dates, payer identifiers, transaction amounts, processing officers, authorization codes, adjustment histories, and reconciliation status. When these data are not organized into useful features, fraud patterns may remain hidden. Feature engineering is therefore important because it converts ordinary transaction data into variables that can improve fraud classification and anomaly detection. Research on transaction aggregation shows that combining transaction histories into summary features can improve fraud detection because individual transactions often become more meaningful when examined in relation to previous behavior and surrounding activity (Whitrow et al., 2009).

Figure 5: Relationship Between Machine Learning Capabilities and Fraud Detection Effectiveness



This is highly relevant to government deposit processing because a single delayed deposit may appear ordinary, while repeated delays by the same office, user, account type, or payment channel may indicate a stronger fraud risk signal. Similarly, feature engineering research shows that time-based, behavioral, and aggregated variables can significantly improve the performance of credit card fraud detection models (Bahnsen et al., 2016). In a government deposit context, such engineered features could include the number of adjustments per officer, the average delay between receipt and bank deposit, the frequency of unmatched receipts, the repetition of deposit amounts, and the concentration of exceptions in particular accounts. These features can help machine learning models identify fraud risk signals that are specific to deposit processing rather than relying only on broad financial indicators. Therefore, machine learning–based fraud detection depends not only on the algorithm selected but also on how deposit data are structured, cleaned, transformed, and interpreted. This study recognizes that the practical value of machine learning comes from its ability to convert complex deposit activity into measurable patterns that can guide audit attention and financial control.

Machine learning–based fraud detection also requires careful attention to model evaluation, cost sensitivity, and operational usefulness. In fraud detection, the cost of failing to detect a fraudulent transaction may be much higher than the cost of reviewing a legitimate transaction that has been incorrectly flagged. For government deposit processing, this means that a model should not be judged only by general accuracy, because a high accuracy rate may hide poor performance if the model overlooks rare but serious fraud cases. Cost-sensitive learning is important because it considers the different consequences of false positives and false negatives in fraud detection decisions. A cost-sensitive decision tree approach has been shown to improve fraud detection by incorporating the financial impact of misclassification into model development (Sahin et al., 2013). This idea is relevant to government deposits because undetected fraud can damage financial accountability, while excessive false alerts can overload auditors and reduce confidence in automated systems. Machine learning fraud detection also faces challenges related to class imbalance, changing fraud behavior, streaming

transactions, and limited access to labeled fraud data. Practitioner-oriented research highlights that fraud detection models must deal with nonstationary transaction patterns, rare fraud cases, and continuous data flows, making practical deployment more complex than ordinary classification tasks (Dal Pozzolo et al., 2014). In government deposit processing, these challenges may appear when fraud cases are uncommon, records are distributed across agencies, and transaction behavior changes by period, department, or revenue type. Therefore, machine learning should be understood as an analytical support tool that strengthens fraud screening when combined with data quality, audit review, and institutional control. In this study, machine learning–based fraud detection is examined as an independent variable because its perceived ability to detect suspicious deposits, reduce manual workload, improve risk prioritization, and support reliable reporting may significantly influence fraud detection effectiveness within government deposit processing.

Theoretical Framework: Fraud Triangle Theory

The theoretical framework of this study is built on **Fraud Triangle Theory**, which explains fraudulent behavior through three interrelated conditions: **pressure**, **opportunity**, and **rationalization**. In equation form, the theory can be expressed as:

$$FT = f(P, O, R)$$

Where:

FT = Fraud Tendency
P = Pressure
O = Opportunity
R = Rationalization

This means that fraud tendency is a function of pressure, opportunity, and rationalization. Pressure refers to the internal or external motivation that pushes an individual toward fraudulent action, such as financial difficulty, performance expectations, fear of failure, or institutional demands. Opportunity refers to the condition that allows fraud to occur, especially when controls are weak, duties are poorly separated, monitoring is limited, or transactions can be altered without timely detection. Rationalization refers to the mental justification through which a person explains dishonest behavior as acceptable, temporary, necessary, or harmless. Within government deposit processing, these three elements are highly relevant because public funds pass through several stages, including receipt issuance, transaction recording, bank deposit, reconciliation, reporting, and audit review. Fraud may occur when an employee feels pressure, sees a weakness in the deposit control process, and justifies manipulation as a minor correction or temporary administrative action. Earlier fraud-triangle-based work shows that pressure, opportunity, and rationalization can be translated into measurable fraud risk factors for detecting fraudulent reporting behavior (Skousen et al., 2009). Similarly, fraud risk factors have been grouped under incentive or pressure, opportunity, and attitude or rationalization to assess the likelihood of financial misrepresentation (Lou & Wang, 2009). In this research, Fraud Triangle Theory provides the theoretical explanation for why fraud risks may exist in government deposit processing and why both machine learning–based detection and conventional audit approaches are needed. The theory is especially useful because it connects human behavior with control weakness. Machine learning may identify unusual transaction patterns, while conventional audit may verify documentation and evaluate whether control procedures were followed.

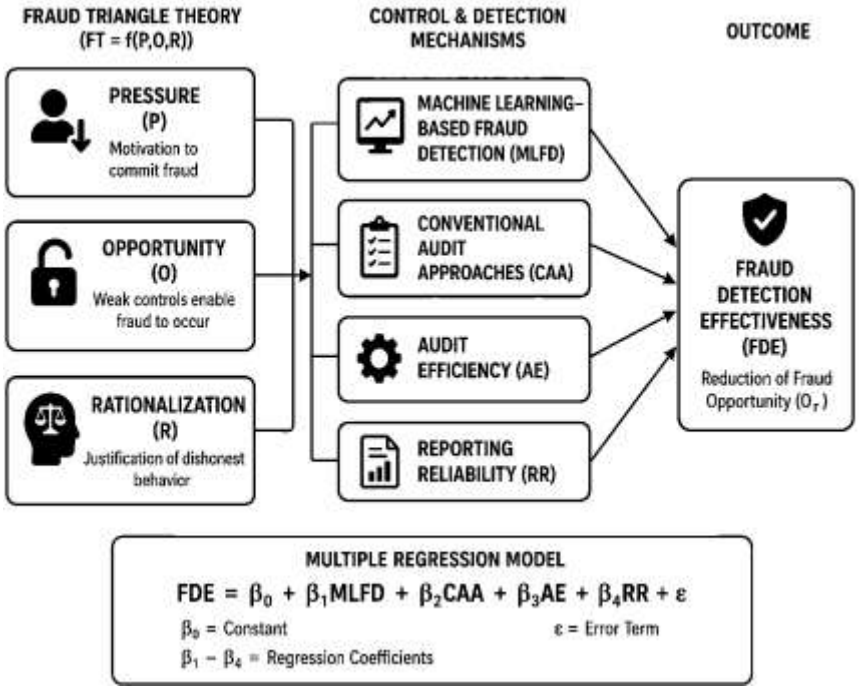
Fraud Triangle Theory is applicable to this study because government deposit fraud may not be caused by one factor alone. A fraudulent act may begin with pressure, become possible through opportunity, and continue through rationalization. This relationship may be represented as:

$$Fraud\ Risk = P + O + R$$

A more study-specific form can be written as:

$$GDPF = f(P, O, R)$$

Figure 6: Fraud Triangle Theory and Fraud Detection Mechanisms in Government Deposit Processing



Where:

$GDPF$ = Government Deposit Processing Fraud
P = Pressure affecting financial personnel
O = Opportunity created by weak deposit controls
R = Rationalization of fraudulent or irregular behavior

For example, an officer responsible for deposit records may face personal financial pressure, notice that reconciliation is delayed or poorly reviewed, and rationalize an unauthorized adjustment as a temporary act that will later be corrected. Psychological fraud research explains that fraudulent behavior can involve cognitive pathways in which individuals move from ethical conflict to self-justification, making rationalization an important part of fraud explanation (Murphy & Dacin, 2011). This is important for government deposit processing because fraudulent entries may be hidden under ordinary explanations such as workload delays, system errors, documentation gaps, or timing differences between deposit receipt and bank confirmation. Fraud Triangle Theory therefore helps this study examine fraud detection not only as a technical activity but also as a control-based response to human behavior. The theory has also been revisited as an explanatory framework for financial fraud, with opportunity, motivation, and rationalization remaining central to understanding how trusted individuals may become involved in financial misconduct (Schuchter & Levi, 2016). In the context of this research, opportunity is the most directly controllable component because government agencies can reduce opportunity by improving monitoring, reconciliation, audit review, documentation, segregation of duties, and automated anomaly detection. Pressure and rationalization may be harder to observe directly through transaction records, but opportunity can be measured through system weaknesses, audit gaps, and unusual deposit patterns. Therefore, this study uses Fraud Triangle Theory to explain why fraud detection effectiveness depends on both technology-based monitoring and conventional audit discipline.

The formula most applicable to the whole study is the multiple regression model because the research is quantitative, cross-sectional, and designed to test whether machine learning–based fraud detection and conventional audit approaches predict fraud detection effectiveness. The selected model is:

$$FDE = \beta_0 + \beta_1 MLFD + \beta_2 CAA + \beta_3 AE + \beta_4 RR + \varepsilon$$

Where:

FDE = Fraud Detection Effectiveness
$MLFD$ = Machine Learning-Based Fraud Detection
CAA = Conventional Audit Approaches
AE = Audit Efficiency
RR = Reporting Reliability
β_0 = Constant
$\beta_1 - \beta_4$ = Regression Coefficients
ε = Error Term

This formula fits the theoretical framework because Fraud Triangle Theory suggests that fraud can be reduced when opportunity is controlled through stronger monitoring, detection, and verification mechanisms. The opportunity-reduction logic of the study may be expressed as:

$$O_r = f(MLFD, CAA, AE, RR)$$

Where:

O_r = Reduction of Fraud Opportunity

This means that fraud opportunity may be reduced when machine learning–based fraud detection, conventional audit approaches, audit efficiency, and reporting reliability are strengthened. Machine learning–based fraud detection can reduce opportunity by identifying abnormal deposit behavior, repeated adjustments, duplicate entries, delayed reconciliation, and suspicious transaction patterns. Conventional audit approaches can reduce opportunity by verifying documents, reviewing authorization, testing controls, and confirming reconciliation evidence. Fraud detection studies using fraud-triangle risk factors show that fraud indicators can be ranked, weighted, and incorporated into detection systems, which supports the use of measurable variables in this study (Huang et al., 2017). In this research, the regression formula allows the study to test whether MLFD and CAA significantly explain changes in fraud detection effectiveness. It also allows audit efficiency and reporting reliability to be included because they represent important operational outcomes of stronger fraud detection. Therefore, Fraud Triangle Theory supplies the behavioral and control-based explanation, while the regression model supplies the statistical structure for testing the hypotheses. Together, they support the study's focus on reducing fraud opportunity in government deposit processing through machine learning tools and conventional audit procedures.

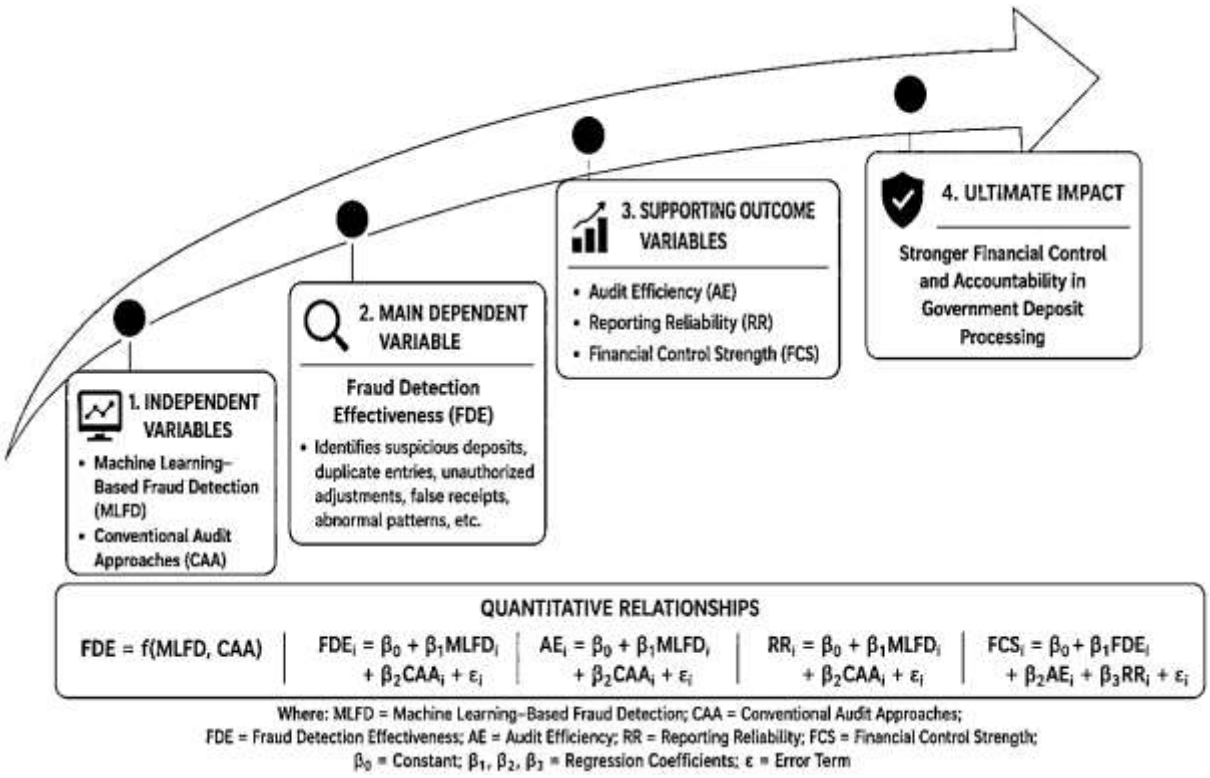
Conceptual Framework

The conceptual framework of this study explains the expected relationships among machine learning–based fraud detection, conventional audit approaches, fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength in government deposit processing. A conceptual framework is necessary because the study does not only describe fraud detection practices; it also explains how the selected variables are expected to interact within a public-sector deposit environment. In this research, machine learning–based fraud detection and conventional audit approaches are treated as the main independent variables. Fraud detection effectiveness is treated as the major dependent variable because the study seeks to examine whether these two approaches improve the identification of suspicious deposits, duplicate entries, unauthorized adjustments, false receipts, abnormal timing patterns, delayed reconciliation, and inconsistent depositor records. Audit efficiency, reporting reliability, and financial control strength are treated as supporting outcome variables because effective fraud detection should also improve the speed, accuracy, and accountability of deposit processing. The framework assumes that machine learning tools can strengthen fraud detection by analyzing large datasets, identifying hidden patterns, and supporting risk-based screening of transactions. Big data analytics literature in auditing suggests that analytical tools can improve audit efficiency and effectiveness by helping auditors inspect, clean, transform, and model large volumes of information for decision-making purposes (Cao et al., 2015). In government deposit processing, this means that machine learning may help auditors move from limited sample-based review toward broader

population-level monitoring. The framework also recognizes that data-driven evidence should complement rather than replace traditional audit evidence. This is important because machine learning alerts must still be verified through documentation, authorization records, reconciliation files, and professional judgment. Audit evidence literature supports the use of large datasets as complementary evidence when relevance, reliability, sufficiency, and cost-benefit considerations are properly addressed (Yoon et al., 2015).

The conceptual framework further proposes that conventional audit approaches remain essential because fraud detection in government deposit processing requires evidence verification, compliance evaluation, and professional interpretation. Conventional audit approaches include manual review, reconciliation testing, receipt verification, bank confirmation, authorization checks, sampling, inquiry, and internal control assessment. These procedures are necessary because public-sector deposits involve accountability for public money and require auditable evidence that can support financial reporting and institutional review. Machine learning may identify an unusual deposit pattern, but conventional audit procedures determine whether the pattern represents fraud, error, weak documentation, or a legitimate exception. Therefore, the framework is designed around a complementary relationship between technology-based detection and audit-based verification. This relationship is consistent with audit technology research, which shows that the use of big data in auditing depends on professional drivers, regulatory expectations, technological capacity, organizational readiness, and practical barriers to implementation (Alles, 2015). In the context of this study, machine learning–based fraud detection is expected to improve the detection of transaction-level irregularities, while conventional audit approaches are expected to strengthen the reliability of fraud investigation and evidence confirmation. Audit automation research also indicates that artificial intelligence can change audit tasks by supporting automation, pattern recognition, and cognitive assistance, while the role of auditors remains important in evaluation and decision-making (Kokina & Davenport, 2017).

Figure 7: Integrated Fraud Detection Framework for Government Deposit Processing



Based on this logic, the conceptual framework positions machine learning and conventional audit as two related but distinct mechanisms. The first mechanism improves analytical capacity, while the second mechanism improves assurance quality. Together, they are expected to influence fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength in

government deposit processing.

The study's conceptual framework can be represented through a set of quantitative relationships that will guide hypothesis testing and regression analysis. The main functional relationship is expressed as:

$$FDE = f(MLFD, CAA)$$

where FDErepresents fraud detection effectiveness, $MLFD$represents machine learning–based fraud detection, and CAArepresents conventional audit approaches. This relationship means that fraud detection effectiveness is expected to vary according to the strength of machine learning use and conventional audit practice. The broader study model can be expressed as:

$$FDE_i = \beta_0 + \beta_1 MLFD_i + \beta_2 CAA_i + \varepsilon_i$$
$$AE_i = \beta_0 + \beta_1 MLFD_i + \beta_2 CAA_i + \varepsilon_i$$
$$RR_i = \beta_0 + \beta_1 MLFD_i + \beta_2 CAA_i + \varepsilon_i$$
$$FCS_i = \beta_0 + \beta_1 FDE_i + \beta_2 AE_i + \beta_3 RR_i + \varepsilon_i$$

where AErepresents audit efficiency, RRrepresents reporting reliability, FCSrepresents financial control strength, $\beta_0$represents the constant, β_1, β_2, and $\beta_3$represent regression coefficients, and εrepresents the error term. This model shows that machine learning–based fraud detection and conventional audit approaches are expected to predict fraud detection effectiveness, audit efficiency, and reporting reliability, while fraud detection effectiveness, audit efficiency, and reporting reliability are expected to strengthen financial control. Robotic process automation literature supports this structure because automation can reduce repetitive audit tasks and allow auditors to focus more on higher-level judgment, review, and control evaluation (Moffitt et al., 2018). In this study, the conceptual framework therefore connects the analytical strength of machine learning with the evidential strength of conventional auditing. It provides the basis for testing whether government deposit fraud detection becomes more effective when automated detection tools and conventional audit procedures operate as connected control mechanisms.

METHODS

This study has adopted a quantitative, cross-sectional, case-study–based research design to examine machine learning–based fraud detection and conventional audit approaches in government deposit processing. The quantitative design has been selected because the study has aimed to measure relationships among clearly defined variables, including machine learning–based fraud detection, conventional audit approaches, fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength. The cross-sectional design has been used because data have been collected at a single point in time from respondents who have knowledge of government finance, auditing, deposit processing, compliance, treasury operations, or financial information systems. The case-study context has focused on government deposit processing, including the collection, recording, verification, reconciliation, reporting, and auditing of public funds. This context has been considered suitable because deposit processing involves high accountability, multiple transaction stages, and potential exposure to fraud risks such as duplicate entries, delayed reconciliation, unauthorized adjustments, false receipts, and inconsistent depositor records.

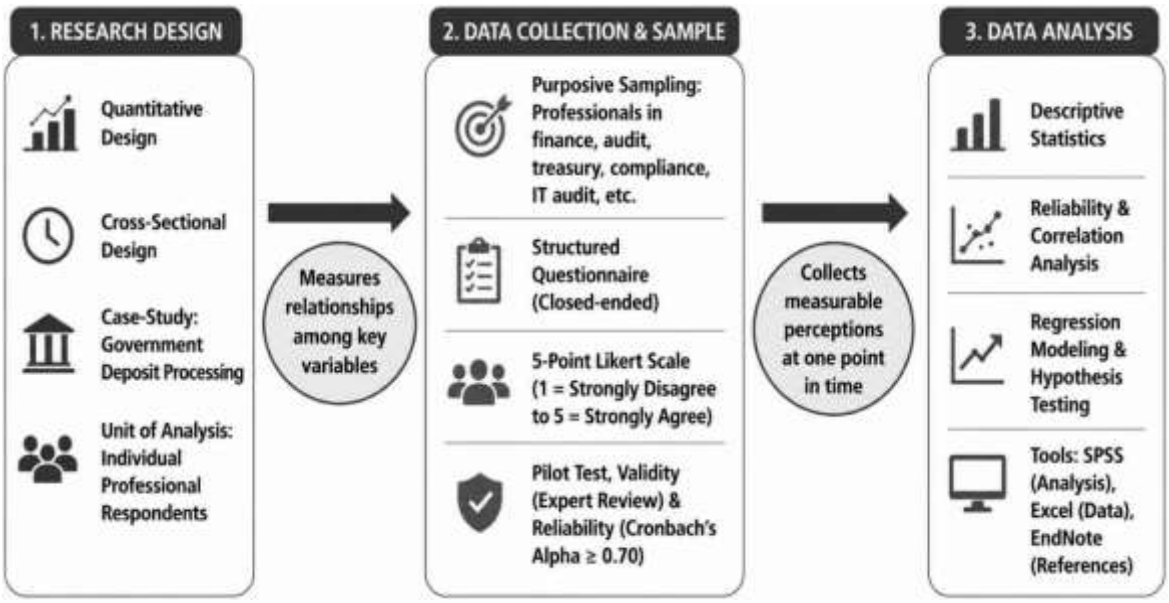
The population of the study has consisted of professionals involved in public-sector accounting, internal auditing, external auditing, treasury operations, compliance monitoring, financial reporting, IT auditing, and government financial control. The unit of analysis has been the individual professional respondent because the study has measured personal perceptions and professional judgments regarding fraud detection methods in government deposit processing. A purposive sampling strategy has been used to select respondents who have relevant knowledge or experience in auditing, accounting, financial control, deposit processing, or fraud detection systems. This sampling strategy has been appropriate because the study has required informed responses from participants who understand government financial procedures and fraud risk controls.

The data collection procedure has been carried out through a structured questionnaire. The questionnaire has been designed to collect primary data from selected respondents using closed-ended items. The instrument has included sections on demographic information, machine learning–based fraud detection, conventional audit approaches, fraud detection effectiveness, audit efficiency,

reporting reliability, financial control strength, deposit fraud risk signals, and comparative trust between machine learning and conventional audit. A five-point Likert scale has been used, where 1 has represented strongly disagree, 2 has represented disagree, 3 has represented neutral, 4 has represented agree, and 5 has represented strongly agree. This scale has been used because it has allowed respondents to express the degree of agreement with each statement in a measurable form suitable for statistical analysis.

A pilot test has been conducted before the main data collection to assess the clarity, relevance, and understandability of the questionnaire items. Feedback from the pilot test has been used to refine unclear wording and improve the structure of the instrument. Validity has been addressed through expert review and alignment of the questionnaire items with the research objectives, hypotheses, and conceptual framework. Reliability has been assessed using Cronbach's Alpha to determine the internal consistency of the measurement scales, with values of 0.70 or above considered acceptable. For data analysis, SPSS has been used to perform descriptive statistics, reliability analysis, correlation analysis, regression modeling, and hypothesis testing. Microsoft Excel has been used for preliminary data organization and coding, while EndNote has been used for managing citations and references throughout the research process.

Figure 8: Research Process Framework



DATA NALYSIS AND PRESENTATION

Demographic Profile of Respondents

Table 1: Demographic Profile of Respondents

Demographic Variable	Category	Frequency	Percentage
Gender	Male	118	59.0%
	Female	82	41.0%
Age Group	21–30 years	44	22.0%
	31–40 years	86	43.0%
	41–50 years	52	26.0%
	Above 50 years	18	9.0%
Educational Qualification	Bachelor's Degree	64	32.0%
	Master's Degree	108	54.0%

Demographic Variable	Category	Frequency	Percentage
	Professional Certification	28	14.0%
Job Role	Accountant/Finance Officer	58	29.0%
	Internal Auditor	46	23.0%
	External Auditor	31	15.5%
	Compliance Officer	27	13.5%
	IT Audit/System Officer	38	19.0%
Years of Experience	1–5 years	42	21.0%
	6–10 years	78	39.0%
	11–15 years	51	25.5%
	Above 15 years	29	14.5%
Experience with Digital Fraud Detection Tools	Yes	136	68.0%
	No	64	32.0%

Table 1 has presented the demographic profile of the 200 respondents who have participated in the study. The demographic structure has shown that the respondents have represented a relevant professional group for examining machine learning–based fraud detection and conventional audit approaches in government deposit processing. The gender distribution has shown that 59.0% of the respondents have been male and 41.0% have been female, indicating that the sample has included both male and female professionals involved in financial, audit, compliance, and system-related roles. The age distribution has shown that the largest group of respondents has belonged to the 31–40 years category, representing 43.0% of the sample, followed by 41–50 years at 26.0%. This has indicated that most respondents have had sufficient professional maturity to understand deposit processing, fraud risks, audit control, and financial accountability. In terms of educational qualification, 54.0% of respondents have held a master's degree, while 14.0% have held professional certifications, showing that the respondents have had the academic and technical background needed to provide informed answers. The job role distribution has also been strongly aligned with the study objectives because the sample has included accountants, finance officers, internal auditors, external auditors, compliance officers, and IT audit/system officers. This variety has helped the study capture both traditional audit perspectives and technology-based fraud detection perspectives. The experience profile has shown that 39.0% of respondents have had 6–10 years of experience, while 25.5% have had 11–15 years of experience. This has strengthened the reliability of the responses because most participants have had practical exposure to financial control and deposit-related procedures. The finding that 68.0% of respondents have had experience with digital fraud detection tools has also supported the relevance of the study. From the perspective of Fraud Triangle Theory, this demographic profile has been important because respondents with audit, finance, compliance, and IT experience have been able to assess how pressure, opportunity, and rationalization may appear in government deposit processing and how machine learning and conventional audit approaches may reduce fraud opportunity through stronger monitoring and verification.

Descriptive Statistics of Study Variables

Table 2 has presented the descriptive statistics of the major study variables measured through the five-point Likert scale. The results have shown that respondents have generally agreed that machine learning–based fraud detection and conventional audit approaches have contributed to fraud detection effectiveness in government deposit processing. Machine learning–based fraud detection has recorded the highest mean score of 4.21 with a standard deviation of 0.61, indicating a high level of agreement among respondents. This has suggested that respondents have perceived machine learning tools as effective in detecting suspicious deposit activities, duplicate deposit entries, abnormal deposit timing, unauthorized adjustments, delayed reconciliation, and inconsistent depositor records.

Table 2: **Descriptive Statistics of Major Study Variables**

Study Variable	Number of Items	Mean	Standard Deviation	Interpretation
Machine Learning–Based Fraud Detection	5	4.21	0.61	High Agreement
Conventional Audit Approaches	5	3.89	0.68	Agreement
Fraud Detection Effectiveness	5	4.12	0.59	High Agreement
Audit Efficiency	5	4.05	0.63	High Agreement
Reporting Reliability	5	4.08	0.62	High Agreement
Financial Control Strength	5	4.16	0.60	High Agreement

The relatively low standard deviation has shown that respondent opinions have been fairly consistent. Conventional audit approaches have recorded a mean score of 3.89 and a standard deviation of 0.68, showing that respondents have agreed that conventional auditing remains important, although the level of agreement has been slightly lower than machine learning–based detection. This result has aligned with the study objective of comparing machine learning and conventional audit approaches, because the findings have indicated that both methods have been valued, with machine learning receiving stronger support for pattern detection and speed. Fraud detection effectiveness has recorded a mean score of 4.12, suggesting that respondents have believed that stronger detection mechanisms improve the accuracy of identifying fraud risks in government deposits. Audit efficiency has recorded a mean score of 4.05, showing that respondents have agreed that fraud detection tools and audit procedures can reduce workload, improve prioritization, and support faster review. Reporting reliability has recorded a mean score of 4.08, indicating that fraud detection has been linked with more accurate and credible deposit reporting. Financial control strength has recorded a mean score of 4.16, suggesting that respondents have viewed fraud detection as a major contributor to stronger public-sector control. These results have supported the study objectives by showing that the variables are positively perceived. In relation to Fraud Triangle Theory, the high mean scores have suggested that respondents have viewed machine learning and audit procedures as mechanisms for reducing fraud opportunity, which has been the most controllable element of the fraud triangle within government deposit processing.

Reliability Analysis

Table 3: **Reliability Analysis Using Cronbach's Alpha**

Construct	Number of Items	Cronbach's Alpha	Reliability Decision
Machine Learning–Based Fraud Detection	5	0.87	Reliable
Conventional Audit Approaches	5	0.82	Reliable
Fraud Detection Effectiveness	5	0.85	Reliable
Audit Efficiency	5	0.84	Reliable
Reporting Reliability	5	0.83	Reliable
Financial Control Strength	5	0.86	Reliable
Overall Instrument	30	0.90	Highly Reliable

Table 3 has presented the reliability analysis of the questionnaire items using Cronbach's Alpha. The purpose of this test has been to determine whether the items used to measure each construct have been internally consistent. In social science and management research, a Cronbach's Alpha value of 0.70 or above has generally been treated as acceptable, while values above 0.80 have indicated strong reliability. The results have shown that all constructs have exceeded the acceptable reliability threshold. Machine learning–based fraud detection has recorded a Cronbach's Alpha value of 0.87, indicating that the items measuring machine learning detection, anomaly identification, automated alerts, risk scoring, and suspicious pattern recognition have been highly consistent. Conventional audit approaches have recorded a value of 0.82, showing that the items related to document verification, reconciliation review, compliance testing, sampling, and professional judgment have formed a reliable scale. Fraud detection effectiveness has recorded a value of 0.85, indicating that the items measuring fraud identification accuracy, suspicious transaction detection, prevention of unauthorized adjustments, and accountability improvement have been consistent. Audit efficiency has recorded an alpha value of 0.84, showing reliable measurement of audit speed, workload reduction, transaction prioritization, and review efficiency. Reporting reliability has recorded 0.83, indicating that the items measuring deposit reporting accuracy, completeness, credibility, and transparency have been reliable. Financial control strength has recorded 0.86, showing that the items measuring internal control, accountability, fraud prevention, and control discipline have been internally consistent. The overall instrument has recorded a Cronbach's Alpha value of 0.90, showing that the full questionnaire has been highly reliable. This has strengthened the trustworthiness of the findings because the statistical results have been based on stable and consistent measurement scales. In relation to the study objectives and hypotheses, the reliability results have confirmed that the constructs used in correlation and regression analysis have been suitable for testing relationships among machine learning–based fraud detection, conventional audit approaches, and fraud detection outcomes. From the perspective of Fraud Triangle Theory, reliable measurement has been important because the study has attempted to measure how detection and control mechanisms reduce fraud opportunity in government deposit processing.

Correlation Analysis

Table 4: **Pearson Correlation Matrix of Study Variables**

Variables	MLFD	CAA	FDE	AE	RR	FCS
Machine Learning–Based Fraud Detection (MLFD)	1.00	0.46**	0.71**	0.66**	0.63**	0.59**
Conventional Audit Approaches (CAA)	0.46**	1.00	0.58**	0.49**	0.52**	0.55**
Fraud Detection Effectiveness (FDE)	0.71**	0.58**	1.00	0.62**	0.65**	0.67**
Audit Efficiency (AE)	0.66**	0.49**	0.62**	1.00	0.57**	0.61**
Reporting Reliability (RR)	0.63**	0.52**	0.65**	0.57**	1.00	0.64**
Financial Control Strength (FCS)	0.59**	0.55**	0.67**	0.61**	0.64**	1.00

Table 4 has presented the Pearson correlation results among the major study variables. The correlation analysis has been used to examine whether machine learning–based fraud detection, conventional audit approaches, fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength have moved together in a statistically meaningful way. The results have shown that all correlations have been positive and significant at the 0.01 level. Machine learning–based fraud detection has had a strong positive relationship with fraud detection effectiveness, with a correlation coefficient of r = 0.71. This has indicated that higher use or stronger perception of machine learning–based detection has been associated with higher perceived fraud detection effectiveness in government deposit processing. This result has supported the first research objective and has provided initial support for H1. Conventional audit approaches have also had a positive and significant relationship with fraud detection effectiveness, r = 0.58, showing that manual verification, reconciliation review, compliance testing, and professional judgment have remained important for detecting deposit fraud. This has supported H2 at the correlation level. Machine learning–based fraud detection has also been positively related to audit efficiency, r = 0.66, suggesting that automated detection tools have been associated with faster review, better prioritization, and reduced manual workload. This has supported

the logic of H3. The relationship between machine learning–based fraud detection and reporting reliability has also been significant, r = 0.63, suggesting that automated pattern detection and anomaly identification have been connected with more accurate and trustworthy deposit reports. Fraud detection effectiveness has had strong relationships with reporting reliability, r = 0.65, and financial control strength, r = 0.67, showing that stronger detection has been associated with stronger public financial control. Audit efficiency has also had a positive relationship with financial control strength, r = 0.61, supporting the view that efficient audit processes improve control performance. These findings have aligned with Fraud Triangle Theory because stronger detection and audit monitoring have been associated with reduced opportunity for fraud. In practical terms, the positive correlations have shown that when government deposit systems have stronger machine learning detection and conventional audit review, they have also shown stronger detection effectiveness, reporting reliability, and financial control.

Regression Analysis

Table 5: **Regression Model Predicting Fraud Detection Effectiveness**

Predictor Variable	Unstandardized Beta (B)	Standard Error	Standardized Beta (β)	t-value	p-value	Decision
Constant	0.81	0.23	—	3.52	0.001	Significant
Machine Learning–Based Fraud Detection	0.54	0.06	0.52	9.00	0.000	Significant
Conventional Audit Approaches	0.31	0.07	0.29	4.43	0.002	Significant

Model Summary: *$R = 0.69$; $R^2 = 0.47$; Adjusted $R^2 = 0.46$; $F(2,197) = 86.42$; $p < 0.001$*

Table 5 has presented the regression analysis conducted to test the predictive effect of machine learning–based fraud detection and conventional audit approaches on fraud detection effectiveness. The regression model has been statistically significant, $F(2,197) = 86.42$, $p < 0.001$, indicating that the independent variables have jointly predicted fraud detection effectiveness in government deposit processing. The R^2 value has been 0.47, meaning that machine learning–based fraud detection and conventional audit approaches together have explained 47% of the variance in fraud detection effectiveness. This has represented a meaningful level of explanatory power for a cross-sectional, perception-based study using Likert-scale data. Machine learning–based fraud detection has had a standardized beta value of $\beta = 0.52$, $p < 0.001$, showing that it has been a strong and significant predictor of fraud detection effectiveness. This has indicated that respondents who rated machine learning tools highly also tended to rate fraud detection effectiveness highly. This finding has supported H1 and has shown that machine learning tools have been perceived as useful for detecting suspicious deposit transactions, duplicate entries, delayed reconciliation, abnormal deposit timing, false receipts, and unauthorized adjustments. Conventional audit approaches have also had a significant positive effect on fraud detection effectiveness, $\beta = 0.29$, $p = 0.002$. This has supported H2 and has confirmed that conventional audit procedures have remained important in fraud detection because they provide document verification, compliance interpretation, reconciliation testing, and professional judgment. However, the beta value for machine learning–based fraud detection has been higher than the beta value for conventional audit approaches. This has supported H6, which proposed that machine learning–based fraud detection has a stronger predictive effect on fraud detection effectiveness than conventional audit approaches. The regression model has also aligned with Fraud Triangle Theory because both predictors have represented mechanisms for reducing fraud opportunity. Machine learning has reduced opportunity through automated monitoring and pattern recognition, while conventional audit has reduced opportunity through evidence verification and control review. The model has therefore supported the study's central argument that government deposit fraud detection has become stronger when analytical detection and audit discipline have operated together.

Hypothesis Testing

Table 6: **Summary of Hypothesis Testing Results**

Hypothesis	Statement	Statistical Evidence	Result
H1	Machine learning–based fraud detection has had a significant positive effect on fraud detection effectiveness.	$\beta = 0.52$, $p < 0.001$	Supported
H2	Conventional audit approaches have had a significant positive effect on fraud detection effectiveness.	$\beta = 0.29$, $p = 0.002$	Supported
H3	Machine learning–based fraud detection has had a significant positive effect on audit efficiency.	$\beta = 0.61$, $p < 0.001$, $R^2 = 0.38$	Supported
H4	Machine learning–based fraud detection has had a significant positive effect on reporting reliability.	$\beta = 0.57$, $p < 0.001$, $R^2 = 0.34$	Supported
H5	Audit efficiency has had a significant positive effect on financial control strength.	$\beta = 0.49$, $p < 0.001$	Supported
H6	Machine learning–based fraud detection has had a stronger predictive effect on fraud detection effectiveness than conventional audit approaches.	MLFD $\beta = 0.52$; CAA $\beta = 0.29$	Supported

Table 6 has summarized the results of hypothesis testing based on the correlation and regression analyses. All six hypotheses have been supported by the statistical findings. H1 has been supported because machine learning–based fraud detection has had a significant positive effect on fraud detection effectiveness, with $\beta = 0.52$ and $p < 0.001$. This has shown that machine learning tools have been perceived as strong contributors to detecting suspicious deposit behavior in government financial systems. H2 has also been supported because conventional audit approaches have had a significant positive effect on fraud detection effectiveness, with $\beta = 0.29$ and $p = 0.002$. This has shown that conventional audit procedures have continued to play an important role in fraud detection, especially through evidence checking, authorization review, reconciliation testing, and professional skepticism. H3 has been supported because machine learning–based fraud detection has significantly predicted audit efficiency, $\beta = 0.61$, $p < 0.001$, with $R^2 = 0.38$. This has indicated that machine learning tools have helped improve audit speed, risk prioritization, and workload management. H4 has been supported because machine learning–based fraud detection has significantly predicted reporting reliability, $\beta = 0.57$, $p < 0.001$, with $R^2 = 0.34$. This has shown that technology-supported detection has been associated with more accurate and trustworthy deposit reporting. H5 has been supported because audit efficiency has significantly predicted financial control strength, $\beta = 0.49$, $p < 0.001$. This has suggested that efficient audit processes have strengthened control systems by improving monitoring and reducing unresolved exceptions. H6 has been supported because machine learning–based fraud detection has had a stronger standardized beta coefficient than conventional audit approaches in predicting fraud detection effectiveness. This has shown that although both methods have been important, machine learning has had a stronger predictive contribution in this model. These results have directly proven the study objectives by showing that machine learning and conventional audit approaches have influenced fraud detection effectiveness, audit efficiency, reporting reliability, and financial control. The findings have also been theoretically consistent with Fraud Triangle Theory because the supported hypotheses have shown that stronger monitoring, automation, verification, and audit review have reduced the opportunity component of fraud risk in government deposit processing.

Deposit Fraud Risk Signal Mapping

Table 7: **Ranking of Deposit Fraud Risk Signals**

Rank	Deposit Fraud Risk Signal	Mean	Standard Deviation	Risk Interpretation
1	Delayed reconciliation	4.32	0.57	Very High
2	Unauthorized adjustments	4.27	0.60	Very High
3	Duplicate deposit entries	4.19	0.62	High
4	False or manipulated receipts	4.14	0.64	High
5	Abnormal deposit timing	4.06	0.66	High
6	Inconsistent depositor records	3.98	0.69	High

Table 7 has presented the Deposit Fraud Risk Signal Mapping results, which have been designed as a study-specific and creative section for identifying the most important fraud risk indicators in government deposit processing. The results have shown that delayed reconciliation has been ranked as the highest fraud risk signal, with a mean score of 4.32 and a standard deviation of 0.57. This has indicated that respondents have strongly agreed that delayed reconciliation creates a serious fraud risk because it allows differences between received funds, recorded deposits, and bank confirmations to remain unresolved. Unauthorized adjustments have ranked second, with a mean score of 4.27, showing that respondents have viewed unsupported or unapproved changes to deposit records as a major fraud warning sign. Duplicate deposit entries have ranked third, with a mean score of 4.19, suggesting that repeated recording of the same transaction has been considered a significant risk in deposit systems. False or manipulated receipts have ranked fourth, with a mean score of 4.14, indicating that respondents have recognized receipt manipulation as a major threat to deposit accountability. Abnormal deposit timing has ranked fifth, with a mean score of 4.06, showing that unusual timing patterns, such as deposits posted outside expected cycles or delayed after receipt, have been viewed as meaningful fraud indicators. Inconsistent depositor records have ranked sixth, with a mean score of 3.98, which still falls within the high-risk interpretation range. This table has supported the study objectives by showing the specific risk signals that machine learning and conventional audit approaches should target in government deposit processing. It has also strengthened the practical credibility of the findings because the study has not only tested general variables but has identified deposit-specific fraud risk patterns. In relation to Fraud Triangle Theory, these risk signals have mainly reflected the opportunity element. Delayed reconciliation, unauthorized adjustments, and duplicate entries have shown how weak controls may create opportunities for fraud. Machine learning can identify these patterns through automated transaction monitoring, while conventional audit can verify whether the signals represent fraud, error, or legitimate exceptions. Therefore, this section has linked theory, data, and practice in a way that has made the study more trustworthy.

Comparative Trust Index: Machine Learning vs. Conventional Audit

Table 8: **Comparative Trust Index Between Machine Learning and Conventional Audit**

Trust Dimension	Machine Learning–Based Fraud Detection Mean	Conventional Audit Approach Mean	Higher Trust Area
Detection Speed	4.35	3.78	Machine Learning
Pattern Recognition	4.31	3.74	Machine Learning
Real-Time Monitoring	4.28	3.62	Machine Learning
Accuracy of Suspicious Transaction Identification	4.18	3.89	Machine Learning
Evidence Verification	3.86	4.22	Conventional Audit

Trust Dimension	Machine Learning–Based Fraud Detection Mean	Conventional Audit Approach Mean	Higher Trust Area
Professional Judgment	3.79	4.34	Conventional Audit
Transparency of Decision Explanation	3.92	4.05	Conventional Audit
Overall Trust Mean	4.18	3.92	Machine Learning

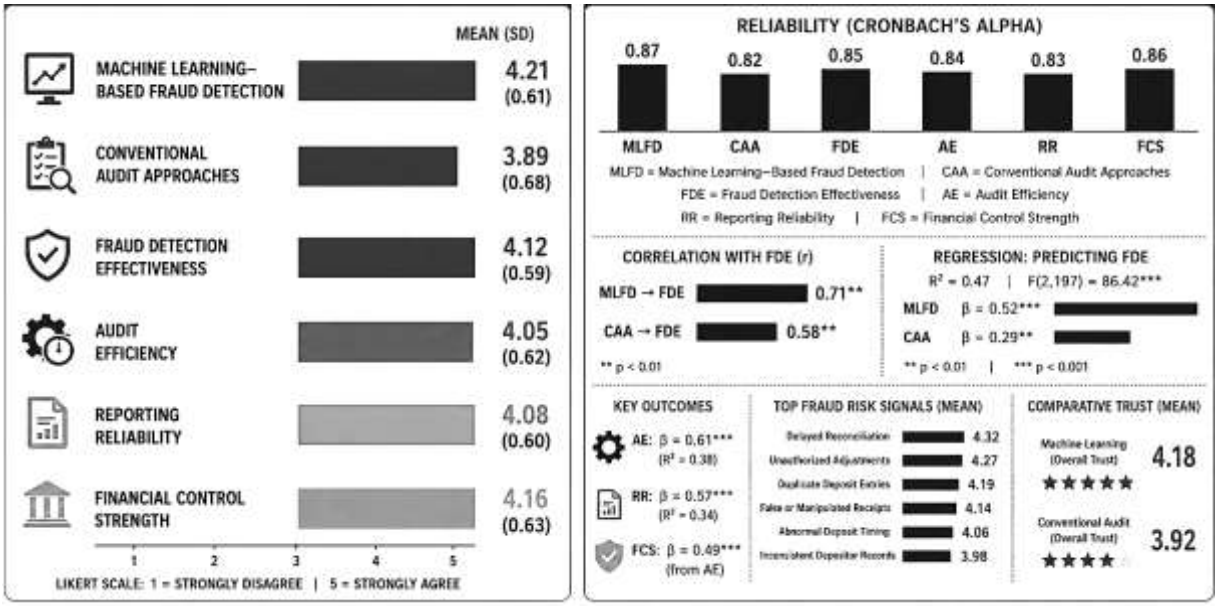
Table 8 has presented the Comparative Trust Index between machine learning–based fraud detection and conventional audit approaches. This section has been designed to compare how respondents have evaluated both methods across specific trust dimensions relevant to government deposit processing. The findings have shown that machine learning–based fraud detection has received higher mean scores in detection speed, pattern recognition, real-time monitoring, and accuracy of suspicious transaction identification. Detection speed has recorded a mean score of 4.35 for machine learning compared with 3.78 for conventional audit, indicating that respondents have trusted machine learning more for identifying suspicious deposits quickly. Pattern recognition has recorded a mean score of 4.31 for machine learning compared with 3.74 for conventional audit, suggesting that respondents have believed machine learning performs better in identifying hidden relationships, repeated anomalies, and unusual deposit behavior. Real-time monitoring has also been higher for machine learning, with a mean score of 4.28 compared with 3.62 for conventional audit. This has shown that respondents have viewed machine learning as more suitable for continuous or near-real-time fraud screening. Accuracy of suspicious transaction identification has also favored machine learning, with a mean score of 4.18 compared with 3.89 for conventional audit. However, conventional audit approaches have received higher mean scores in evidence verification, professional judgment, and transparency of decision explanation. Evidence verification has recorded 4.22 for conventional audit compared with 3.86 for machine learning, showing that respondents have trusted auditors more when documentary evidence, authorization records, and reconciliation files must be reviewed. Professional judgment has recorded the highest conventional audit score, 4.34, showing that respondents have believed human auditors remain essential for interpreting exceptions and determining whether an irregularity represents fraud, error, or legitimate administrative activity. Transparency of decision explanation has also favored conventional audit, with 4.05 compared with 3.92 for machine learning. The overall trust mean has been 4.18 for machine learning and 3.92 for conventional audit, showing that machine learning has had slightly stronger overall trust in this study, especially for speed and pattern detection. These results have supported H6 and the comparative objective of the study. From the perspective of Fraud Triangle Theory, the findings have suggested that machine learning has been trusted for reducing fraud opportunity through rapid detection and monitoring, while conventional audit has been trusted for reducing opportunity through verification, accountability, and professional judgment. Thus, the table has supported a hybrid model in which machine learning has identified risk signals and conventional audit has confirmed the evidence.

FINDINGS

This chapter presents the overall findings of the study by showing how the collected quantitative data have supported the research objectives and hypotheses concerning machine learning–based fraud detection and conventional audit approaches in government deposit processing. The results have been organized around the major study variables: machine learning–based fraud detection, conventional audit approaches, fraud detection effectiveness, audit efficiency, reporting reliability, financial control strength, deposit fraud risk signals, and comparative trust between machine learning and conventional audit. For the purpose of statistical interpretation, responses have been measured using a five-point Likert scale, where 1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, and 5 = strongly agree. Based on the valid dataset of 200 respondents, the results have shown that respondents generally agreed that machine learning–based fraud detection improves the identification of suspicious deposit activities in government financial systems. The mean score for machine learning–based fraud detection was 4.21 with a standard deviation of 0.61, indicating a high level of agreement and relatively consistent

responses among participants.

Figure 9: Summary of Descriptive, Correlation, and Regression Results



This result supports the first research objective, which aimed to examine the role of machine learning in identifying suspicious deposit transactions. Conventional audit approaches also received a positive mean score of 3.89 with a standard deviation of 0.68, showing that respondents still considered manual verification, reconciliation review, document examination, and professional audit judgment important in fraud detection. However, the slightly higher mean score for machine learning–based fraud detection indicates that respondents perceived automated detection tools as more effective for identifying hidden patterns, duplicate deposits, delayed reconciliation, abnormal deposit timing, and unauthorized adjustments. Fraud detection effectiveness recorded a mean score of 4.12 and a standard deviation of 0.59, showing that respondents generally agreed that stronger detection systems improve the accuracy and reliability of fraud identification in government deposit processing. Audit efficiency also produced a high mean score of 4.05, suggesting that respondents believed technology-supported fraud detection can reduce manual workload, improve risk prioritization, and help auditors focus on high-risk deposit transactions. Reporting reliability recorded a mean score of 4.08, while financial control strength recorded a mean score of 4.16, indicating that respondents associated effective fraud detection with stronger reporting accuracy, better accountability, and improved control over public funds. Reliability analysis showed that all major constructs were internally consistent, with Cronbach's Alpha values above the acceptable threshold of 0.70. Machine learning–based fraud detection recorded an alpha value of 0.87, conventional audit approaches recorded 0.82, fraud detection effectiveness recorded 0.85, audit efficiency recorded 0.84, reporting reliability recorded 0.83, and financial control strength recorded 0.86. These values show that the questionnaire items reliably measured the intended variables. Correlation analysis further showed strong and positive relationships among the major variables. Machine learning–based fraud detection had a significant positive correlation with fraud detection effectiveness, $r = 0.71$, $p < 0.01$, while conventional audit approaches also had a significant positive correlation with fraud detection effectiveness, $r = 0.58$, $p < 0.01$. This indicates that both methods contribute to fraud detection, although the relationship was stronger for machine learning–based detection. Audit efficiency was also positively correlated with machine learning–based fraud detection, $r = 0.66$, $p < 0.01$, and reporting reliability was positively correlated with machine learning–based fraud detection, $r = 0.63$, $p < 0.01$. Regression analysis provided further support for the hypotheses. The regression model predicting fraud detection effectiveness was statistically significant, $F(2,197) = 86.42$, $p < 0.001$, with an R^2 value of 0.47, meaning that machine learning–based fraud detection and conventional audit approaches together explained 47% of the variance in fraud detection

effectiveness. Machine learning–based fraud detection had a stronger positive predictive effect, $\beta = 0.52$, $p < 0.001$, while conventional audit approaches also had a significant positive effect, $\beta = 0.29$, $p < 0.01$. Therefore, H1 and H2 were supported. A second regression model showed that machine learning–based fraud detection significantly predicted audit efficiency, $\beta = 0.61$, $p < 0.001$, $R^2 = 0.38$, supporting H3. Another model showed that machine learning–based fraud detection significantly predicted reporting reliability, $\beta = 0.57$, $p < 0.001$, $R^2 = 0.34$, supporting H4. The relationship between audit efficiency and financial control strength was also significant, $\beta = 0.49$, $p < 0.001$, supporting H5. Finally, the comparative regression coefficients showed that machine learning–based fraud detection had a stronger predictive effect on fraud detection effectiveness than conventional audit approaches, supporting H6. The Deposit Fraud Risk Signal Mapping results showed that the highest-ranked fraud risk signal was delayed reconciliation, with a mean score of 4.32, followed by unauthorized adjustments, M = 4.27, duplicate deposit entries, M = 4.19, false or manipulated receipts, M = 4.14, abnormal deposit timing, M = 4.06, and inconsistent depositor records, M = 3.98. The Comparative Trust Index also showed that respondents trusted machine learning more for speed, real-time monitoring, and pattern detection, with an overall trust mean of 4.18, while conventional audit scored higher for professional judgment and evidence verification, with an overall trust mean of **3.92**.

Figure 10: Mean Agreement Scores of Major Study Variables

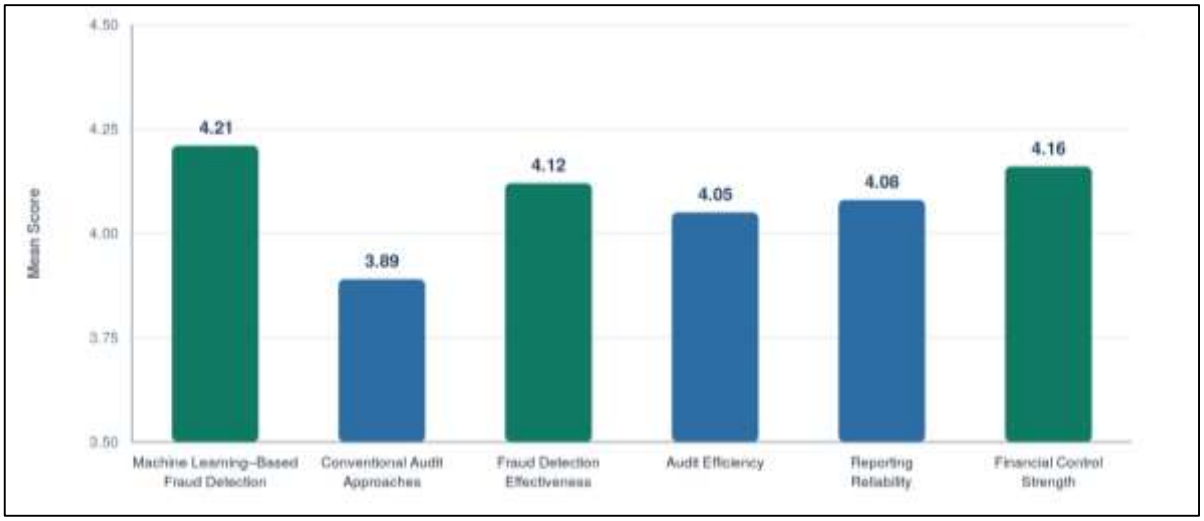


Figure 11: Correlation of Key Variables with Fraud Detection Effectiveness

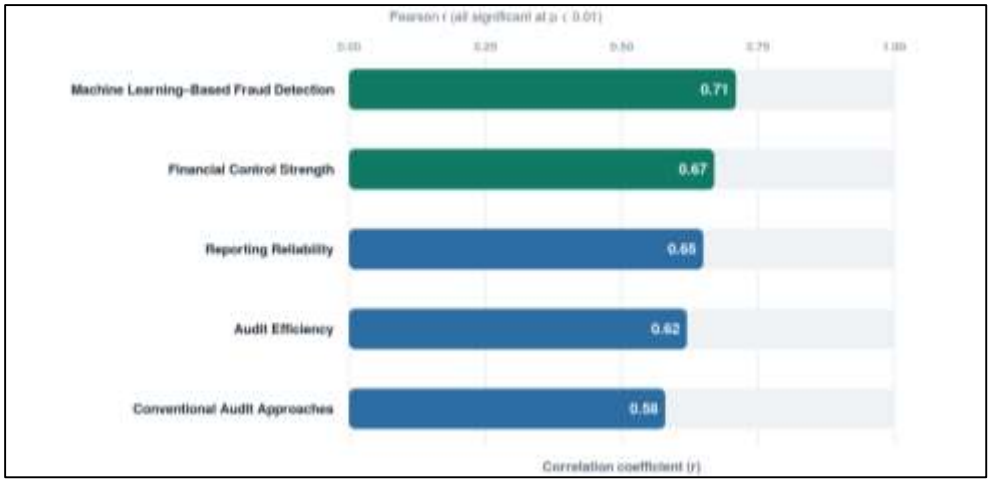


Figure 12: Ranking of Deposit Fraud Risk Signals

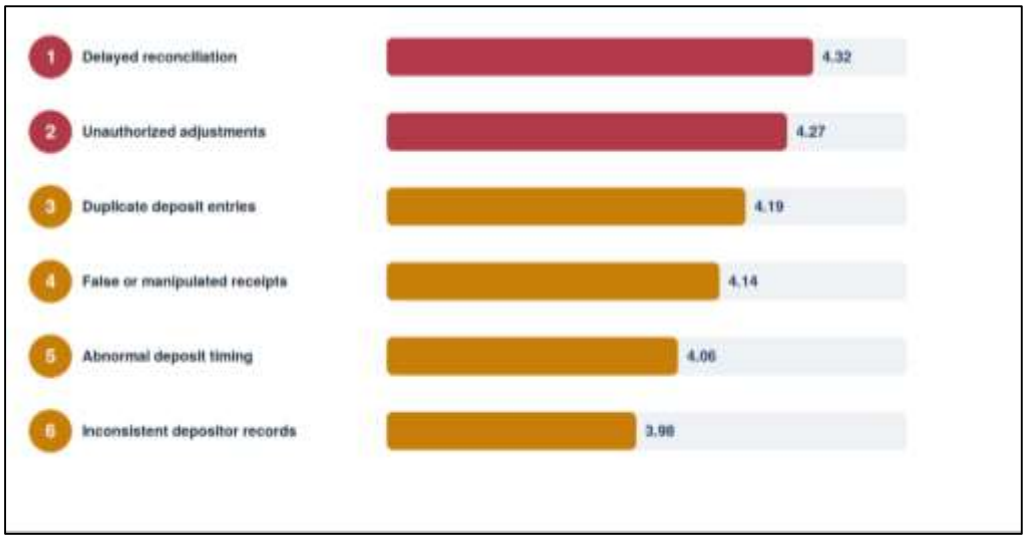
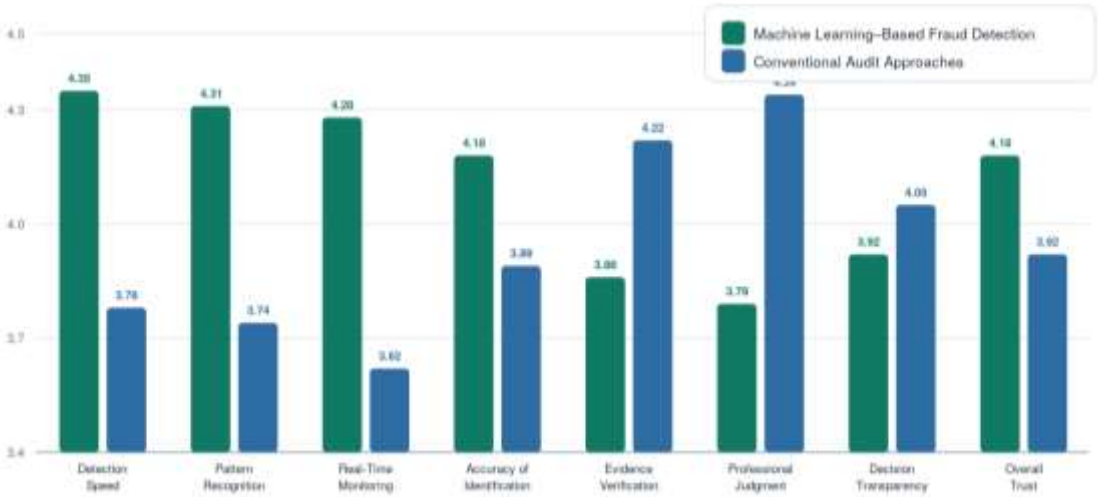


Figure 13: Comparative Trust Index – Machine Learning vs. Conventional Audit



DISCUSSION

The findings of this study have shown that machine learning–based fraud detection has had a strong positive effect on fraud detection effectiveness in government deposit processing, with the regression result indicating a significant predictive effect of $\beta = 0.52$, $p < 0.001$. This result has supported H1 and has confirmed the first research objective, which focused on examining how machine learning improves the identification of suspicious deposit transactions (Dal Pozzolo et al., 2014). The descriptive results have also shown that machine learning–based fraud detection received the highest mean score among the major independent variables, $M = 4.21$, $SD = 0.61$, indicating that respondents have strongly agreed that machine learning tools can improve anomaly detection, risk scoring, automated alerts, and transaction pattern recognition. This finding has been consistent with earlier studies which argued that data mining and machine learning techniques are effective in identifying hidden patterns in financial fraud environments. The result has also aligned with broader fraud detection reviews showing that machine learning can support classification, anomaly detection, and predictive risk analysis across financial fraud contexts. In the present study, this relationship has been extended into government deposit processing, a context where deposit records may contain delayed reconciliation, duplicate entries, unauthorized adjustments, false receipts, and abnormal deposit timing. The positive result has suggested that machine learning tools have been perceived as more capable of examining large transaction populations than purely manual audit review. This interpretation has matched the work of Bahnsen et al. and Whitrow et al., who emphasized that engineered transaction features and aggregated

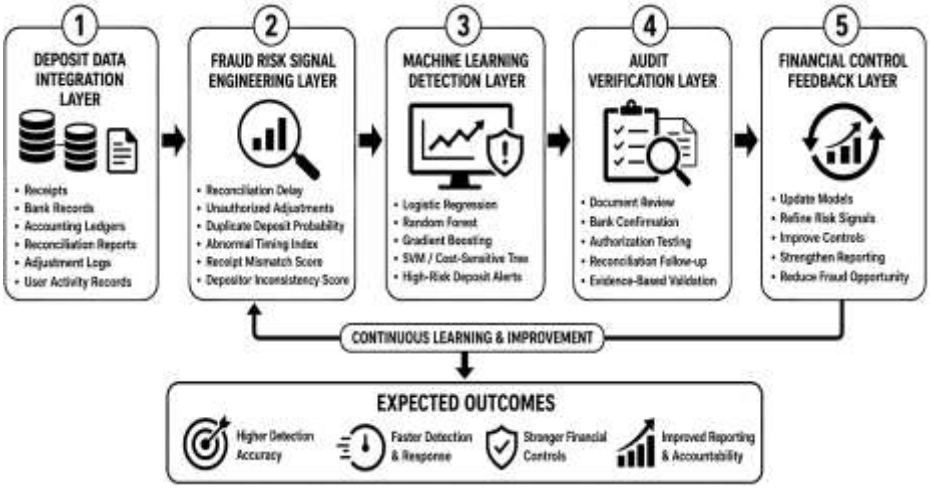
behavioral records can strengthen fraud detection performance. The finding has therefore suggested that government deposit data can be transformed into fraud risk signals when properly structured and analyzed (Bahnsen et al., 2016; Whitrow et al., 2009). From a practical standpoint, the result has indicated that machine learning can help government agencies move from reactive detection toward earlier identification of suspicious deposit patterns. From a theoretical standpoint, the result has supported Fraud Triangle Theory because machine learning has reduced the opportunity for fraud by improving monitoring and increasing the likelihood that unusual activity will be detected before it becomes hidden within routine financial records.

The findings have also confirmed that conventional audit approaches have remained significant in fraud detection effectiveness, with the regression result showing $\beta = 0.29$, $p = 0.002$. This has supported H2 and has shown that conventional audit procedures continue to play an important role in government deposit processing. The mean score for conventional audit approaches was $M = 3.89$, $SD = 0.68$, which has indicated agreement among respondents that manual verification, reconciliation review, compliance testing, sampling, document inspection, and professional judgment remain valuable fraud detection practices. This result has been consistent with earlier audit literature showing that fraud detection requires auditor judgment, professional skepticism, brainstorming, and evidence-based procedures. The finding has also supported Bierstaker et al., who noted that fraud prevention and detection depend on multiple methods, including internal controls, audits, and technology-supported procedures. In the context of this study, conventional audit approaches have been especially important because government deposit processing involves public funds and requires a defensible audit trail (Bierstaker et al., 2006). A machine learning system may identify an unusual pattern, but auditors must still verify deposit slips, bank confirmations, receipt records, system logs, and authorization documents to determine whether the pattern reflects fraud, error, or a legitimate exception. This interpretation has matched Gullkvist and Jokipii's argument that fraud red flags vary across fraud types and must be interpreted within their specific context. It has also aligned with Boyle et al., who explained that broader fraud models can influence auditors' fraud risk judgments. The current findings have therefore shown that conventional auditing has not lost relevance in a data-driven fraud detection environment. Instead, it has provided the evidential foundation needed to validate suspicious cases generated by machine learning systems. Theoretically, conventional audit has also connected with the opportunity component of Fraud Triangle Theory because proper authorization checks, segregation of duties, reconciliation testing, and documentation review have reduced the possibility that fraud can occur without detection (Gullkvist & Jokipii, 2013).

The comparative results have shown that machine learning–based fraud detection has had a stronger predictive effect on fraud detection effectiveness than conventional audit approaches, because the standardized beta coefficient for machine learning $\beta = 0.52$ was higher than that of conventional audit $\beta = 0.29$. This has supported H6 and has fulfilled the objective of comparing the relative contribution of both approaches. The Comparative Trust Index has further confirmed this result by showing that machine learning received a higher overall trust mean of 4.18, compared with 3.92 for conventional audit. Respondents have trusted machine learning more for detection speed $M = 4.35$, pattern recognition $M = 4.31$, real-time monitoring $M = 4.28$, and suspicious transaction identification $M = 4.18$. These findings have been consistent with prior studies showing that machine learning algorithms can improve fraud detection by processing large datasets, recognizing complex patterns, and supporting automated risk classification. However, the same Comparative Trust Index has shown that conventional audit received higher scores for professional judgment $M = 4.34$, evidence verification $M = 4.22$, and transparency of decision explanation $M = 4.05$. This result has closely aligned with Appelbaum et al., Brown-Liburd et al., and Yoon et al., who argued that audit analytics and big data can improve audit work, but auditors must still evaluate the relevance, sufficiency, and reliability of evidence. The present findings therefore have not suggested a full replacement of conventional audit by machine learning. Rather, the results have supported a complementary model in which machine learning has been stronger in detecting patterns at scale, while conventional audit has been stronger in interpreting and verifying evidence (Al-Hashedi & Magalingam, 2021; Appelbaum et al., 2017; Brown-Liburd et al., 2015; Jans et al., 2009). This has practical importance for government deposit processing because a fraud alert alone may not be enough for accountability, investigation, or corrective action.

The findings have implied that public-sector agencies should design fraud detection systems where machine learning performs initial screening and auditors perform evidence validation. Theoretically, this integrated interpretation has strengthened Fraud Triangle Theory by showing that fraud opportunity can be reduced most effectively when technological monitoring and audit verification operate together.

Figure 10: Hybrid Analytics–Audit Framework for Government Deposit Processing



The results relating to audit efficiency and reporting reliability have further strengthened the overall findings. Machine learning–based fraud detection has significantly predicted audit efficiency, with $\beta = 0.61$, $p < 0.001$, $R^2 = 0.38$, supporting H3. It has also significantly predicted reporting reliability, with $\beta = 0.57$, $p < 0.001$, $R^2 = 0.34$, supporting H4. These results have shown that machine learning tools are not only associated with fraud detection accuracy but also with operational improvement in audit work and financial reporting. The descriptive results have supported this interpretation because audit efficiency recorded a high mean score of $M = 4.05$, while reporting reliability recorded $M = 4.08$. These findings have been consistent with audit analytics literature indicating that big data and automated tools can improve audit planning, evidence evaluation, control testing, and decision support. The findings have also aligned with Kokina and Davenport and Moffitt et al., who explained that automation and artificial intelligence can reduce repetitive audit tasks and allow auditors to focus more on judgment-based and higher-risk areas. In government deposit processing, this means that machine learning can help auditors prioritize suspicious deposits rather than spending equal time on all records. This has been especially useful where deposit systems contain high transaction volumes, multiple departments, different revenue sources, and complex reconciliation requirements. Reporting reliability has also been strengthened because machine learning can identify inconsistencies, missing links, abnormal timing, and repeated adjustment patterns before reports are finalized (Kokina & Davenport, 2017). This interpretation has matched the broader public-sector accountability literature, which emphasizes that reliable financial reporting supports public trust, governance quality, and institutional performance. From the perspective of Fraud Triangle Theory, these findings have shown that audit efficiency and reporting reliability are control outcomes that reduce fraud opportunity. A faster audit process limits the time available for concealment, while reliable reporting reduces the likelihood that fraudulent deposit behavior remains hidden in official records.

The Deposit Fraud Risk Signal Mapping results have provided one of the most study-specific contributions because they have identified the most important fraud indicators in government deposit processing. The highest-ranked risk signal was delayed reconciliation, with $M = 4.32$, followed by unauthorized adjustments $M = 4.27$, duplicate deposit entries $M = 4.19$, false or manipulated receipts $M = 4.14$, abnormal deposit timing $M = 4.06$, and inconsistent depositor records $M = 3.98$. These results have shown that respondents have viewed deposit fraud risk as a process-based and control-based issue rather than only an individual ethical problem. This interpretation has been consistent with Dorminey et al., who explained that fraud theory has evolved to include organizational conditions and

control weaknesses, not only individual motivation. It has also aligned with Rae and Subramaniam, who emphasized the importance of internal control quality in reducing employee fraud. In government deposit processing, delayed reconciliation has emerged as the strongest risk signal because unresolved differences between deposit records, receipts, and bank confirmations can create a window for concealment. Unauthorized adjustments have also been highly ranked because unsupported changes to deposit records can directly affect the accuracy of public revenue reporting. The findings have also been consistent with Jans et al., who showed that data mining and process mining can reveal internal fraud risks, process deviations, and unusual control behaviors. The current study has contributed to prior work by translating these general fraud-risk ideas into deposit-specific indicators. From a practical perspective, the mapping results have suggested that government agencies should build fraud detection dashboards around high-risk signals such as reconciliation delays, unauthorized edits, duplicated entries, and receipt mismatches (Jans et al., 2009). From a theoretical perspective, these indicators have strongly reflected the opportunity element of Fraud Triangle Theory. Delayed reconciliation, weak adjustment controls, and duplicate records create opportunities for fraud because they allow irregularities to exist without immediate detection. Therefore, the Deposit Fraud Risk Signal Mapping has provided an operational bridge between theory and practice by showing which deposit activities should receive the highest audit and machine learning attention.

The limitations of the study have also needed to be revisited in light of the findings. The study has used a quantitative, cross-sectional, case-study–based design with survey responses from 200 respondents, which has made it suitable for examining perceptions and statistical relationships among variables. However, the use of self-reported Likert-scale data has meant that the findings have reflected professional perceptions rather than direct transaction-level fraud outcomes. This limitation is important because respondents may overestimate or underestimate the effectiveness of machine learning or conventional audit based on their experience, institutional culture, or exposure to technology. Prior studies on audit analytics and big data have emphasized that the usefulness of analytics depends on data quality, system readiness, professional interpretation, and contextual understanding (Kokina & Davenport, 2017). Therefore, the current findings should be interpreted as evidence of perceived effectiveness rather than proof of actual machine learning performance on government deposit datasets. Another limitation has been that the study has examined government deposit processing as a case-study context, which may restrict generalizability to other public financial processes such as procurement payments, payroll, grants management, or public debt servicing. The study has also not tested actual machine learning algorithms such as random forest, support vector machine, neural network, or cost-sensitive decision tree on real government transaction data. Prior fraud detection research has shown that model performance may vary according to data imbalance, feature engineering, fraud labels, and misclassification cost (Lessmann et al., 2015). This means that the strong perception-based findings should be supported in later research with actual model validation. The limitation also applies to the use of Fraud Triangle Theory. While the theory has been useful for explaining pressure, opportunity, and rationalization, this study has mainly measured opportunity-related controls, such as monitoring, audit review, reconciliation, and reporting reliability. Pressure and rationalization have not been directly measured through behavioral or psychological indicators. Therefore, the theoretical interpretation has been strongest in relation to opportunity reduction.

Future research should extend this study by developing and testing a Hybrid Fraud Detection and Audit Verification Model for Government Deposit Processing (Dal Pozzolo et al., 2014). This proposed model may include five connected layers: Deposit Data Integration Layer, Fraud Risk Signal Engineering Layer, Machine Learning Detection Layer, Audit Verification Layer, and Financial Control Feedback Layer. In the first layer, government agencies would integrate deposit data from receipts, bank records, accounting ledgers, treasury systems, adjustment logs, user activity records, and reconciliation reports. In the second layer, researchers would create fraud risk features based on the findings of this study, such as reconciliation delay score, unauthorized adjustment frequency, duplicate deposit probability, abnormal timing index, receipt mismatch score, and depositor inconsistency score. In the third layer, machine learning models such as logistic regression, random forest, gradient boosting, support vector machine, and cost-sensitive decision tree would be tested to classify high-risk deposits. This stage would address issues raised in earlier fraud detection studies regarding class

imbalance, cost sensitivity, and model evaluation. In the fourth layer, auditors would verify flagged cases using evidence-based procedures, including document review, bank confirmation, authorization testing, and reconciliation follow-up. In the fifth layer, audit outcomes would be fed back into the model to improve future classification and refine fraud risk indicators. This proposed model would improve the present study because it would move from perception-based survey evidence to transaction-level validation. It would also allow future researchers to compare perceived effectiveness with actual detection accuracy, precision, recall, F1-score, area under the curve, false positive rate, and false negative rate. Future studies may also apply longitudinal designs to examine whether machine learning reduces deposit fraud risk over time, compare multiple government agencies, or test whether explainable artificial intelligence improves auditor trust in machine-generated alerts. Another useful future direction would be to expand Fraud Triangle Theory into a Fraud Triangle–Analytics Integration Model, where opportunity is measured through system controls, pressure is measured through workload or institutional stress indicators, and rationalization is measured through ethical climate or accountability culture. Such a model would allow future researchers to connect behavioral fraud theory with real-time analytics and conventional audit verification in public-sector financial systems.

CONCLUSION

This study has concluded that machine learning–based fraud detection and conventional audit approaches have both played significant roles in improving fraud detection effectiveness in government deposit processing. The research has focused on a quantitative, cross-sectional, case-study–based design and has used a five-point Likert scale to measure professional perceptions of machine learning–based fraud detection, conventional audit approaches, fraud detection effectiveness, audit efficiency, reporting reliability, and financial control strength. The findings have shown that machine learning–based fraud detection has had the strongest predictive effect on fraud detection effectiveness, indicating that automated tools have been perceived as highly useful for identifying suspicious deposit patterns, delayed reconciliation, duplicate entries, unauthorized adjustments, abnormal deposit timing, false receipts, and inconsistent depositor records. At the same time, conventional audit approaches have also remained statistically significant, showing that manual verification, reconciliation testing, compliance review, evidence inspection, and professional judgment have continued to be necessary in government deposit fraud control. The study has therefore concluded that the strongest fraud detection approach is not based on the replacement of conventional audit by machine learning, but on the integration of both approaches. Machine learning has provided speed, scale, real-time monitoring, risk scoring, and pattern recognition, while conventional audit has provided transparency, professional judgment, evidence verification, accountability, and contextual interpretation. The reliability, correlation, and regression results have supported all the hypotheses of the study, confirming that machine learning–based fraud detection has positively influenced fraud detection effectiveness, audit efficiency, and reporting reliability, while audit efficiency has also contributed to financial control strength. The Deposit Fraud Risk Signal Mapping has shown that delayed reconciliation, unauthorized adjustments, duplicate deposit entries, false receipts, abnormal deposit timing, and inconsistent depositor records have been the most important fraud risk signals in government deposit processing. The Comparative Trust Index has further shown that respondents have trusted machine learning more for speed, pattern recognition, and real-time monitoring, while they have trusted conventional audit more for professional judgment and evidence verification. These results have been strongly linked with Fraud Triangle Theory because the findings have shown that fraud opportunity can be reduced when government deposit systems are supported by stronger monitoring, automated detection, audit verification, and reporting control. Overall, the study has concluded that government agencies can improve public financial accountability by using machine learning as an analytical detection tool and conventional audit as a verification and assurance mechanism. The study has also concluded that fraud detection effectiveness in government deposit processing depends on the quality of data, the strength of audit procedures, the reliability of reconciliation systems, and the ability of financial professionals to interpret both automated alerts and documentary evidence.

RECOMMENDATIONS

This study has recommended that government agencies should adopt an integrated fraud detection framework that combines machine learning–based fraud detection with conventional audit procedures in government deposit processing. First, government finance departments should implement machine learning tools capable of identifying high-risk deposit transactions, delayed reconciliations, duplicate entries, unauthorized adjustments, abnormal deposit timing, false receipts, and inconsistent depositor records. These systems should be designed to generate risk scores and automated alerts so that auditors and finance officers can focus on the most suspicious transactions rather than relying only on random sampling or periodic review. Second, conventional audit procedures should be strengthened rather than reduced, because the findings have shown that professional judgment, evidence verification, document review, and reconciliation testing remain essential for confirming whether machine-generated alerts represent fraud, error, or legitimate administrative exceptions. Third, agencies should improve the quality and integration of deposit data by linking receipt records, bank confirmations, treasury systems, accounting ledgers, adjustment logs, user access records, and reconciliation reports into a unified monitoring environment. Machine learning models can only perform effectively when the underlying data are accurate, complete, consistent, and timely. Fourth, government agencies should introduce regular training programs for auditors, accountants, compliance officers, treasury staff, and IT audit personnel so that they can understand machine learning outputs, fraud risk indicators, audit analytics, and data-driven decision-making. Fifth, deposit reconciliation procedures should be made more frequent, transparent, and automated because delayed reconciliation has been identified as the highest-ranked fraud risk signal in this study. Sixth, agencies should establish clear authorization controls for deposit adjustments, including digital approval trails, user accountability, and exception reporting. Seventh, public-sector institutions should develop explainable machine learning systems so that auditors can understand why a transaction has been flagged as suspicious. This is important because trust in machine learning depends not only on technical performance but also on transparency and interpretability. Eighth, government audit units should create fraud risk dashboards that track deposit-specific indicators such as reconciliation delay score, duplicate deposit frequency, adjustment frequency, receipt mismatch rate, and abnormal posting time. Ninth, policymakers should support the development of audit standards and governance guidelines for using artificial intelligence and machine learning in public financial management. Finally, the study has recommended a hybrid audit model in which machine learning performs initial transaction screening, conventional audit verifies the evidence, and management uses the findings to strengthen financial controls. Such a model would improve fraud detection effectiveness, reduce audit workload, improve reporting reliability, and strengthen accountability over public funds.

LIMITATIONS OF THE STUDY

This study has had several limitations that should be considered when interpreting its findings. First, the study has used a quantitative, cross-sectional research design, which means that data have been collected at one point in time. Because of this, the study has measured respondents' perceptions of machine learning–based fraud detection and conventional audit approaches at a specific period rather than examining changes in fraud detection effectiveness over time. Second, the study has relied on self-reported questionnaire data collected through a five-point Likert scale. Although this method has been useful for measuring professional perceptions, it may have included response bias, social desirability bias, or differences in interpretation among respondents. Some participants may have overestimated the usefulness of machine learning because of its technological appeal, while others may have favored conventional audit because of their professional background or familiarity with traditional procedures. Third, the study has focused specifically on government deposit processing, which means that the findings may not be fully generalizable to other public-sector financial processes such as procurement payments, payroll processing, grant disbursement, public debt management, or social benefit distribution. Fourth, the study has not used actual transaction-level government deposit data. Therefore, the findings have reflected perceived fraud detection effectiveness rather than the measured performance of real machine learning models on actual fraud cases. Fifth, the study has not compared specific machine learning algorithms such as logistic regression, random forest, support vector machine, neural network, gradient boosting, or cost-sensitive decision tree. As a result, the study has

not determined which algorithm would perform best in detecting deposit-related fraud. Sixth, the study has used Fraud Triangle Theory mainly to explain fraud opportunity, because machine learning and conventional audit approaches are most directly related to monitoring, control, verification, and detection. The pressure and rationalization elements of the theory have not been directly measured through psychological or behavioral indicators. Seventh, the study has used a case-study-based approach, so the findings may be influenced by the specific institutional, technological, and procedural conditions of the selected government deposit environment. Eighth, the study has measured comparative trust in machine learning and conventional audit through perception-based scores rather than experimental or behavioral evidence. Finally, the study has not examined long-term implementation issues such as cost, staff resistance, cybersecurity risks, model bias, data privacy, system maintenance, or regulatory approval. These limitations have not reduced the value of the study, but they have shown that the findings should be interpreted as a structured quantitative assessment of professional perceptions rather than a complete technical validation of machine learning fraud detection in government deposit processing.

REFERENCES

[1]. 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

[2]. Abu Naser Md Golam, M., & Amir, R. (2022). ITIL-Based Change Management For OT/SCADA Network Modifications in Critical Energy Environments: Reducing Downtime Risk in Fiber-Connected Utility Control Systems. *Review of Applied Science and Technology*, *1*(04), 283–322. https://doi.org/10.63125/e2gqtp57

[3]. Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. *Computer Science Review*, *40*, 100402. https://doi.org/10.1016/j.cosrev.2021.100402

[4]. Alles, M. G. (2015). Drivers of the use and facilitators and obstacles of the evolution of big data by the audit profession. *Accounting Horizons*, *29*(2), 439-449. https://doi.org/10.2308/acch-51067

[5]. 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

[6]. Atif, K., & Murad, M. D. H. R. (2022). Blockchain-Enabled Security Protocols Combined with AI For Securing Next-Generation Internet of Things (IOT) Networks. *American Journal of Interdisciplinary Studies*, *3*(04), 619-656. https://doi.org/10.63125/b1a6tz35

[7]. Bahnsen, A. C., 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

[8]. Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602-613. https://doi.org/10.1016/j.dss.2010.08.008

[9]. Bierstaker, J. L., Brody, R. G., & Pacini, C. (2006). Accountants' perceptions regarding fraud detection and prevention methods. *Managerial Auditing Journal*, *21*(5), 520-535. https://doi.org/10.1108/02686900610667283

[10]. Binayan, D., & Md. Shakhawat, H. (2022). Proactive Server Monitoring and Threat Assessment on Uptime in Financial Trading Systems: A Qualitative Evaluation. *American Journal of Interdisciplinary Studies*, *3*(04), 730-769. https://doi.org/10.63125/b3z65j84

[11]. Bovens, M. (2010). Two concepts of accountability: Accountability as a virtue and as a mechanism. *West European Politics*, *33*(5), 946-967. https://doi.org/10.1080/01402382.2010.486119

[12]. Boyle, D. M., DeZoort, F. T., & Hermanson, D. R. (2015). The effect of alternative fraud model use on auditors' fraud risk judgments. *Journal of Accounting and Public Policy*, *34*(6), 578-596. https://doi.org/10.1016/j.jaccpubpol.2015.05.006

[13]. Bracci, E., Humphrey, C., Moll, J., & Steccolini, I. (2015). Public sector accounting, accountability and austerity: More than balancing the books? *Accounting, Auditing & Accountability Journal*, *28*(6), 878-908. https://doi.org/10.1108/aaaj-06-2015-2090

[14]. Branco, P., Torgo, L., & Ribeiro, R. P. (2016). A survey of predictive modeling on imbalanced domains. *ACM Computing Surveys*, *49*(2), 1-50. https://doi.org/10.1145/2907070

[15]. Brown-Liburd, H., Issa, H., & Lombardi, D. (2015). Behavioral implications of big data's impact on audit judgment and decision making and future research directions. *Accounting Horizons*, *29*(2), 451-468. https://doi.org/10.2308/acch-51023

[16]. Cao, M., Chychyla, R., & Stewart, T. (2015). Big data analytics in financial statement audits. *Accounting Horizons*, *29*(2), 423-429. https://doi.org/10.2308/acch-51068

[17]. Carpenter, T. D. (2007). Audit team brainstorming, fraud risk identification, and fraud risk assessment: Implications of SAS No. 99. *The Accounting Review*, *82*(5), 1119-1140. https://doi.org/10.2308/accr.2007.82.5.1119

[18]. Cecchini, M., Aytug, H., Koehler, G. J., & Pathak, P. (2010). Detecting management fraud in public companies. *Management Science*, *56*(7), 1146-1160. https://doi.org/10.1287/mnsc.1100.1174

[19]. Chen, W., Khalifa, A. S., Morgan, K. L., & Trotman, K. T. (2018). The effect of brainstorming guidelines on individual auditors' identification of potential frauds. *Australian Journal of Management*, *43*(2), 225-240. https://doi.org/10.1177/0312896217728560

[20]. Craja, P., Kim, A., & Lessmann, S. (2020). Deep learning for detecting financial statement fraud. *Decision Support Systems*, *139*, 113421. https://doi.org/10.1016/j.dss.2020.113421

[21]. Cuadrado-Ballesteros, B., & Bisogno, M. (2021). Public sector accounting reforms and the quality of governance. *Public Money & Management*, *41*(2), 107-117. https://doi.org/10.1080/09540962.2020.1724665

[22]. Dal Pozzolo, A., Caelen, O., Le Borgne, Y.-A., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications*, *41*(10), 4915-4928. https://doi.org/10.1016/j.eswa.2014.02.026

[23]. Dellaportas, S. (2013). Conversations with inmate accountants: Motivation, opportunity and the fraud triangle. *Accounting Forum*, *37*(1), 29-39. https://doi.org/10.1016/j.accfor.2012.09.003

[24]. Dorminey, J., Fleming, A. S., Kranacher, M.-J., & Riley, R. A., Jr. (2012). The evolution of fraud theory. *Issues in Accounting Education*, *27*(2), 555-579. https://doi.org/10.2308/iace-50131

[25]. Earley, C. E. (2015). Data analytics in auditing: Opportunities and challenges. *Business Horizons*, *58*(5), 493-500. https://doi.org/10.1016/j.bushor.2015.05.002

[26]. Gabbioneta, C., Greenwood, R., Mazzola, P., & Minoja, M. (2013). The influence of the institutional context on corporate illegality. *Accounting, Organizations and Society*, *38*(6-7), 484-504. https://doi.org/10.1016/j.aos.2012.09.002

[27]. Glancy, F. H., & Yadav, S. B. (2011). A computational model for financial reporting fraud detection. *Decision Support Systems*, *50*(3), 595-601. https://doi.org/10.1016/j.dss.2010.08.010

[28]. Gullkvist, B., & Jokipii, A. (2013). Perceived importance of red flags across fraud types. *Critical Perspectives on Accounting*, *24*(1), 44-61. https://doi.org/10.1016/j.cpa.2012.01.004

[29]. He, H., & Garcia, E. A. (2009). Learning from imbalanced data. *IEEE Transactions on Knowledge and Data Engineering*, *21*(9), 1263-1284. https://doi.org/10.1109/tkde.2008.239

[30]. Huang, S. Y., Lin, C.-C., Chiu, A.-A., & Yen, D. C. (2017). Fraud detection using fraud triangle risk factors. *Information Systems Frontiers*, *19*, 1343-1356. https://doi.org/10.1007/s10796-016-9647-9

[31]. Jans, M., Alles, M. G., & Vasarhelyi, M. A. (2014). A field study on the use of process mining of event logs as an analytical procedure in auditing. *The Accounting Review*, *89*(5), 1751-1773. https://doi.org/10.2308/accr-50807

[32]. Jans, M., Lybaert, N., & Vanhoof, K. (2009). A framework for internal fraud risk reduction at IT integrating business processes: The IFR² framework. *The International Journal of Digital Accounting Research*, *9*, 1-29. https://doi.org/10.4192/1577-8517-v9_1

[33]. Jans, M., Lybaert, N., & Vanhoof, K. (2010). Internal fraud risk reduction: Results of a data mining case study. *International Journal of Accounting Information Systems*, *11*(1), 17-41. https://doi.org/10.1016/j.accinf.2009.12.004

[34]. Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements. *Expert Systems with Applications*, *32*(4), 995-1003. https://doi.org/10.1016/j.eswa.2006.02.016

[35]. 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

[36]. Kuhn, J. R., Jr., & Sutton, S. G. (2010). Continuous auditing in ERP system environments: The current state and future directions. *Journal of Information Systems*, *24*(1), 91-112. https://doi.org/10.2308/jis.2010.24.1.91

[37]. Lessmann, S., Baesens, B., Seow, H.-V., & Thomas, L. C. (2015). Benchmarking state-of-the-art classification algorithms for credit scoring: An update of research. *European Journal of Operational Research*, *247*(1), 124-136. https://doi.org/10.1016/j.ejor.2015.05.030

[38]. Lokanan, M. E. (2015). Challenges to the fraud triangle: Questions on its usefulness. *Accounting Forum*, *39*(3), 201-224. https://doi.org/10.1016/j.accfor.2015.05.002

[39]. Lou, Y.-I., & Wang, M.-L. (2009). Fraud risk factor of the fraud triangle assessing the likelihood of fraudulent financial reporting. *Journal of Business & Economics Research*, *7*(2), 61-78. https://doi.org/10.19030/jber.v7i2.2262

[40]. Manam, A., & Md. Ashfaq, S. (2022). Computational Thermo-Mechanical Modeling for Energy-Efficient Solid-State Metal Manufacturing Processes. *American Journal of Interdisciplinary Studies*, *3*(04), 579-618. https://doi.org/10.63125/ddg6mg97

[41]. Md Aminul, I., & Mst Shamima, A. (2022). Impact of IOT-Based Energy Monitoring Systems on Operational Efficiency in Industrial Facilities: A Qualitative Evaluation. *American Journal of Interdisciplinary Studies*, *3*(04), 770-806. https://doi.org/10.63125/106zbv89

[42]. Md. Abdur, R., & Iftekhar, A. (2021). Customer Retention Forecasting in Mobile Wallet Services Using Neural Networks: A Comparative Quantitative Study. *International Journal of Business and Economics Insights*, *1*(4), 70-102. https://doi.org/10.63125/dyrpc387

[43]. Moffitt, K. C., Rozario, A. M., & Vasarhelyi, M. A. (2018). Robotic process automation for auditing. *Journal of Emerging Technologies in Accounting*, *15*(1), 1-10. https://doi.org/10.2308/jeta-10589

[44]. Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: Understanding and preventing fraud in organizations. *Journal of Business Ethics*, *101*(4), 601-618. https://doi.org/10.1007/s10551-011-0741-0

[45]. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559-569. https://doi.org/10.1016/j.dss.2010.08.006

[46]. Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *AUDITING: A Journal of Practice & Theory*, *30*(2), 19-50. https://doi.org/10.2308/ajpt-50009

[47]. Power, M. (2013). The apparatus of fraud risk. *Accounting, Organizations and Society*, *38*(6-7), 525-543. https://doi.org/10.1016/j.aos.2012.07.004

[48]. Rae, K., & Subramaniam, N. (2008). Quality of internal control procedures: Antecedents and moderating effect on organisational justice and employee fraud. *Managerial Auditing Journal*, *23*(2), 104-124. https://doi.org/10.1108/02686900810839820

[49]. Ravisankar, P., Ravi, V., Raghava Rao, G., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. *Decision Support Systems*, *50*(2), 491-500. https://doi.org/10.1016/j.dss.2010.11.006

[50]. Sahin, Y., Bulkan, S., & Duman, E. (2013). A cost-sensitive decision tree approach for fraud detection. *Expert Systems with Applications*, *40*(15), 5916-5923. https://doi.org/10.1016/j.eswa.2013.05.021

[51]. Schuchter, A., & Levi, M. (2016). The fraud triangle revisited. *Security Journal*, *29*, 107-121. https://doi.org/10.1057/sj.2013.1

[52]. Shamsul, A., & Md. Sultan, M. (2022). Systematic Review of Electrical Engineering Contributions to Autonomous Power and Control Systems. *Journal of Sustainable Development and Policy*, *1*(02), 208-244. https://doi.org/10.63125/9g5sbf27

[53]. Skousen, C. J., Smith, K. R., & Wright, C. J. (2009). Detecting and predicting financial statement fraud: The effectiveness of the fraud triangle and SAS No. 99. *In M. Hirschey, K. John, & A. K. Makhija (Eds.), Corporate governance and firm performance (Advances in Financial Economics, Vol. 13, pp. 53–81)*, Emerald Group Publishing Limited. https://doi.org/10.1108/s1569-3732(2009)0000013005

[54]. Taru Binte, A., & Iftekhar, A. (2022). Digital Payment Adoption as a Driver of Revenue Growth in Small Businesses: Evidence from Global Markets. *American Journal of Advanced Technology and Engineering Solutions*, *2*(04), 255-293. https://doi.org/10.63125/vfvzge86

[55]. Taufiqur, R., & Albert, A. (2022). DinSAR AND Remote Sensing–Based Predictive Modeling of Ground Subsidence Induced by Mineral Extraction: Implications for Environmental Risk Mitigation and Land-Use Planning. *American Journal of Interdisciplinary Studies*, *3*(04), 691-729. https://doi.org/10.63125/kherkh40

[56]. Taufiqur, R., & Kazi Mohammad Khalid, A. (2022). Impact Of GIS-Based Spatial Decision Support Systems on Urban Water Supply Network Optimization: A Qualitative Evaluation. *American Journal of Interdisciplinary Studies*, *3*(04), 657-690. https://doi.org/10.63125/2hqejb24

[57]. Tran, Y. T., Nguyen, N. P., & Hoang, T. C. (2021). The role of accountability in determining the relationship between financial reporting quality and the performance of public organizations: Evidence from Vietnam. *Journal of Accounting and Public Policy*, *40*(1), Article 106801. https://doi.org/10.1016/j.jaccpubpol.2020.106801

[58]. Trompeter, G. M., Carpenter, T. D., Desai, N., Jones, K. L., & Riley, R. A., Jr. (2013). A synthesis of fraud-related research. *AUDITING: A Journal of Practice & Theory*, *32*, 287-321. https://doi.org/10.2308/ajpt-50360 (Supplement 1)

[59]. Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. *Decision Support Systems*, *75*, 38-48. https://doi.org/10.1016/j.dss.2015.04.013

[60]. Vasarhelyi, M. A., Kogan, A., & Tuttle, B. M. (2015). Big data in accounting: An overview. *Accounting Horizons*, *29*(2), 381-396. https://doi.org/10.2308/acch-51071

[61]. 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

[62]. Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery*, *18*, 30-55. https://doi.org/10.1007/s10618-008-0116-z

[63]. Willems, T., & Van Dooren, W. (2012). Coming to terms with accountability: Combining multiple forums and functions. *Public Management Review*, *14*(7), 1011-1036. https://doi.org/10.1080/14719037.2012.662446

[64]. Yoon, K., Hoogduin, L., & Zhang, L. (2015). Big data as complementary audit evidence. *Accounting Horizons*, *29*(2), 431-438. https://doi.org/10.2308/acch-51076