World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Conceptual Framework for AI-powered fraud detection in E-commerce: Addressing systemic challenges in public assistance programs

Areeba Farooq [1,*], Anate Benoit Nicaise Abbey [2] and Ekene Cynthia Onukwulu [3]

[1] *Amazon Grocery Logistics, New York, USA.*
[2] *Altice USA, Plano,TX, USA.*
[3] *Independent Researcher, Nigeria.*

World Journal of Advanced Research and Reviews, 2024, 24(03), 2207-2218

Publication history: Received on 16 November 2024; revised on 22 December 2024; accepted on 24 December 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.3.3961

Abstract

Fraud in public assistance programs, such as the Supplemental Nutrition Assistance Program (SNAP) and Electronic Benefit Transfer (EBT), poses significant economic and social challenges, diverting vital resources from vulnerable populations. Traditional fraud detection methods, including manual audits and static rule-based systems, have proven insufficient to address the complexity and adaptability of modern fraudulent schemes. This paper proposes a conceptual framework for AI-powered fraud detection, emphasizing the use of machine learning, anomaly detection, and predictive analytics to combat fraud effectively. The framework addresses systemic challenges, including evolving fraud tactics, sector-specific issues, and technological barriers such as data privacy and scalability. It highlights the core components of AI-driven systems, ensuring interoperability across public assistance programs and e-commerce platforms. Ethical considerations, such as transparency, fairness, and accountability, are integrated into the framework to prevent algorithmic bias and protect beneficiaries' rights. The paper also explores AI adoption's economic and social implications, outlining the potential for cost savings, operational efficiency, and improved equity in benefit distribution. Finally, strategic recommendations are provided to support the ethical design, sector-agnostic deployment, and continuous improvement of AI-based fraud detection systems. By addressing these challenges, this paper aims to contribute to a more efficient, fair, and transparent approach to public resource protection.

Keywords: AI-Powered Fraud Detection; Public Assistance Programs; Machine Learning Models; Ethical AI Frameworks; Resource Optimization

1. Introduction

1.1. Brief Overview

Fraud in public assistance programs like the Supplemental Nutrition Assistance Program (SNAP) and Electronic Benefits Transfer (EBT) systems poses a significant threat to the integrity of public resources. These programs are designed to provide essential support to vulnerable populations, yet they are frequently exploited through a variety of fraudulent activities (Blitstein et al., 2023). Common forms of fraud include identity theft, benefit trafficking, misrepresentation of eligibility, and retailer collusion. Such actions deplete public funds, erode public trust, and undermine the social equity these programs are meant to uphold (Robinson, 2020).

The economic impact of fraud in public assistance programs is substantial. In the United States alone, SNAP fraud has been estimated to cost taxpayers millions annually. While oversight mechanisms exist, traditional detection methods such as manual audits, rule-based checks, and whistleblower reports have proven insufficient due to the growing

* Corresponding author: Areeba Farooq

sophistication of fraud schemes. Detecting fraudulent activity is akin to finding a needle in a haystack, given the sheer volume of daily transactions within public assistance systems. Manual reviews are labor-intensive, time-consuming, and prone to human error, creating enforcement gaps (Bosso, 2023).

The social implications are equally concerning. Fraud not only drains public resources but also exacerbates inequities. When bad actors exploit these systems, deserving beneficiaries may face stricter eligibility criteria and reduced program funding. This threatens the primary objective of public assistance: to support economically disadvantaged households. Thus, there is a pressing need for innovative, efficient, and scalable solutions to detect and prevent fraud while maintaining equitable access to benefits (Davies).

1.2. Relevance of AI

Artificial Intelligence (AI) has emerged as a transformative tool for fraud detection in financial, healthcare, and e-commerce sectors. Given its capacity for real-time analysis, adaptability, and predictive accuracy, AI is well-positioned to revolutionize fraud detection in public assistance programs like SNAP and EBT. Unlike traditional systems that rely on predefined rules, AI-powered models can identify anomalies and patterns that human reviewers might overlook. This ability to "learn" from data makes AI a superior option for combating increasingly sophisticated fraud schemes (Bello & Olufemi, 2024).

AI's relevance lies in its ability to automate fraud detection at scale. Machine learning (ML) algorithms, a subset of AI, can process vast datasets to detect deviations from normal spending behaviors. For instance, if an EBT card is suddenly used in multiple locations in a short period or for unusually large purchases, AI systems can flag it as suspicious for further review. Similarly, anomaly detection models can identify retailer collusion by analyzing transaction patterns, such as unusually high redemptions compared to similar businesses (Shoetan & Familoni, 2024).

Another key advantage of AI is its capacity for continuous improvement. As fraud tactics evolve, traditional systems require manual rule updates, which can be slow and inefficient. In contrast, AI models can learn and adapt over time, updating detection parameters based on new data. This makes AI a proactive tool that anticipates fraudulent behavior rather than merely reacting to it. Furthermore, AI enhances decision-making speed, enabling near-instant identification of potential fraud, and reducing the opportunity window for fraudulent activity to occur (Ismaeil, 2024).

Beyond its technical capabilities, AI can address the operational challenges that public assistance agencies face, such as limited human resources and rising workloads. AI-powered tools free up human analysts by automatically prioritizing high-risk cases for review. This allows human intervention to focus on the most critical cases, thereby optimizing the allocation of limited resources. Additionally, automated fraud detection enhances transparency and accountability, as every decision made by AI models can be traced and audited, ensuring compliance with regulatory requirements (Asolo, Gil-Ozoudeh, & Ejimuda, 2024; Onoja & Ajala, 2023).

1.3. Research Aim

This paper aims to develop a conceptual framework for AI-powered fraud detection in public assistance programs, specifically focusing on SNAP and EBT. While AI-driven fraud detection is well-established in the private sector, its application to public welfare programs is still emerging. By addressing systemic challenges, ethical considerations, and the scalability of AI frameworks, this research seeks to fill a critical gap in the literature.

This paper offers a theoretical exploration of AI's role in identifying, preventing, and mitigating fraud in public assistance systems. The conceptual framework will address how AI models can be designed and adapted for cross-sector application, particularly in e-commerce, where fraud detection systems are already advanced. The rationale for this cross-sectoral approach lies in the overlap of fraud tactics between the e-commerce and public welfare sectors. For instance, fraudulent chargebacks in e-commerce bear similarities to benefit trafficking in SNAP, where users exchange benefits for cash or non-eligible goods. By conceptualizing an adaptable AI framework, this paper seeks to create a versatile model that can be applied to other domains. The research also emphasizes ethical considerations and social equity. Since public assistance programs serve vulnerable populations, it is essential to ensure that AI-driven fraud detection systems do not introduce biases that could unjustly deny benefits to eligible recipients. Ethical AI principles, such as fairness, transparency, and accountability, will be integrated into the proposed framework. Ensuring the ethical deployment of AI is vital in preserving the public's trust and minimizing harm to beneficiaries (Ogunbiyi-Badaru, Alao, Dudu, & Alonge, 2024a).

Furthermore, this paper will examine the broader economic and social implications of using AI to combat fraud in public assistance programs. From an economic perspective, reducing fraud could lead to significant savings for governments

and taxpayers. These savings could be redirected to expand program coverage or improve service delivery (Hassan, Aziz, & Andriansyah, 2023). From a social standpoint, curbing fraud ensures that benefits are allocated to those who genuinely need them, thereby promoting social equity. This paper seeks to contribute to the global discourse on how public assistance programs can leverage advanced technology to ensure efficiency, accountability, and fairness by conceptualizing a scalable, ethical, and cross-sectoral AI framework (Bello & Olufemi, 2024).

This paper presents a comprehensive conceptual framework for applying AI in fraud detection for public assistance programs. By addressing systemic challenges, ethical concerns, and the potential for cross-sector scalability, the proposed framework seeks to offer a holistic approach to fraud prevention. This exploration will highlight how AI's predictive power, adaptability, and ethical design can be harnessed to create fairer, more transparent, and more effective fraud detection systems across public welfare programs and beyond.

2. Systemic Challenges in Fraud Detection

2.1. Fraud Complexity

Fraudulent activities in public assistance programs have become increasingly sophisticated, evolving beyond traditional methods to exploit loopholes in technology and administration. While early fraud attempts in programs like SNAP and EBT often involved simple misrepresentations of eligibility, modern fraud schemes now utilize advanced tactics such as identity theft, synthetic identities, and collusion with third-party retailers. This complexity poses a significant challenge to detection efforts (Mokogwu, Achumie, Gbolahan, Adeleke, & Ewim; I. C. Okeke, Agu, Ejike, Ewim, & Komolafe, 2022).

One of the primary reasons for this shift is the digitalization of benefit distribution. The use of Electronic Benefits Transfer (EBT) cards, which function similarly to debit cards, has made benefits more accessible to recipients but also more susceptible to fraud. For instance, fraudsters now deploy skimming devices to capture card details, allowing them to clone EBT cards and make unauthorized purchases. Similarly, cybercriminals may engage in "phishing" schemes to steal beneficiaries' login credentials for online benefits portals. Once in possession of this information, fraudsters can deplete an individual’s benefits without their knowledge (Kuhn, 2021).

Another layer of complexity arises from benefit trafficking, where recipients sell or exchange their SNAP benefits for cash, often at a reduced value. Trafficking is difficult to detect because it mimics legitimate transactions, and offenders can use mobile payment platforms and encrypted communication channels to avoid detection. Retailer collusion adds to this challenge, as unscrupulous store owners facilitate trafficking by processing false transactions and pocketing the cash difference. Since such activities blend into normal transactional data, traditional rule-based detection systems struggle to identify them (Surak, 2023).

The limitations of traditional detection methods exacerbate this problem. Rule-based detection relies on pre-defined rules and thresholds to flag suspicious activity and is only effective against known fraud patterns. For instance, a rule may flag purchases made outside the recipient's residential area, but fraudsters can easily circumvent this by using online delivery services or making transactions in neighboring regions. Additionally, manual audits and human reviews are slow, costly, and often fail to keep pace with the volume of transactions processed in public assistance programs. This reactive approach means that fraudulent transactions are often detected long after they occur, making recovery of misappropriated funds difficult (Mills, 2022).

More dynamic and adaptive detection systems are required to combat these evolving tactics. Machine learning (ML) and artificial intelligence (AI) offer a way forward, as they can identify hidden patterns in large datasets and detect anomalies that fall outside of established rules. However, AI adoption introduces new challenges, including ethical considerations related to bias and fairness, which must be addressed to avoid harming legitimate beneficiaries (Shah, 2021).

2.2. Sector-Specific Issues

Public assistance programs like SNAP and EBT face unique sector-specific challenges that complicate fraud detection efforts. Unlike e-commerce or banking systems, where clear contractual relationships and financial profit motives exist, public assistance programs operate under principles of equity and inclusivity. This makes the balance between fraud prevention and beneficiary protection especially delicate (Waqas et al., 2022).

One of the most pressing issues is benefit misuse. Misuse occurs when beneficiaries use benefits in ways that violate program rules. For example, SNAP benefits are intended to purchase eligible food items, but some beneficiaries attempt

to buy non-eligible items such as alcohol or household supplies. While point-of-sale (POS) systems are designed to restrict the purchase of ineligible items, some retailers intentionally bypass these restrictions. This type of fraud is challenging to detect because it often requires transactional audits or undercover investigations, both resource-intensive and time-consuming (Lad, 2024).

Another major challenge is identity theft, where fraudsters impersonate legitimate beneficiaries to access their benefits. This type of fraud is often facilitated by breaches in government databases or through social engineering attacks like phishing. Once fraudsters gain access to sensitive information, they can use it to apply for benefits, redirect payments, or transfer EBT card balances. Identity theft is particularly harmful because it directly affects legitimate recipients, who may be unable to access their benefits until the issue is resolved. Resolving these cases is time-consuming, requiring government agencies to conduct investigations, reissue cards, and compensate affected recipients(Anozie et al., 2024; Ogunyemi & Ishola, 2024a).

The issue of retailer collusion is another sector-specific challenge. Retailers authorized to accept SNAP payments play a critical role in the system, but some engage in fraudulent activities to exploit program loopholes. Collusion occurs when retailers process false transactions on behalf of beneficiaries, often in exchange for cash. For instance, a retailer may swipe an EBT card for $100 in a fraudulent sale but give the cardholder only $50 in cash. The retailer then pockets the difference. Since these transactions appear legitimate in system logs, they are difficult to identify without sophisticated detection algorithms or whistleblower reports. Retailer fraud is particularly damaging because it allows large sums of public funds to be misappropriated, often with limited means for recovery (Durojaiye, Ewim, & Igwe; O. Mokogwu, G. O. Achumie, A. G. Adeleke, I. C. Okeke, & C. Ewim, 2024).

Sector-specific challenges are compounded by the fact that public assistance agencies must prioritize both efficiency and equity. Aggressive anti-fraud measures could lead to "false positives," where legitimate beneficiaries are flagged for fraud, causing them to lose access to essential support. As a result, detection models must be carefully designed to minimize wrongful accusations and ensure that beneficiaries retain access to assistance while maintaining the integrity of public fund (Ogunyemi & Ishola, 2024b; Olaleye & Mokogwu, 2024a)s.

2.3. Technological and Policy Barriers

Technological and policy barriers significantly hinder the scalability, effectiveness, and ethical implementation of fraud detection systems in public assistance programs. While AI and machine learning have been heralded as transformative tools, their integration into existing systems is fraught with challenges. Scalability is a critical issue. Public assistance programs, like SNAP, handle millions of transactions daily (Attah, Garba, Gil-Ozoudeh, & Iwuanyanwu). Implementing AI-driven fraud detection systems at this scale requires robust computing infrastructure, significant storage capacity, and extensive training datasets. Many government agencies operate with limited IT budgets and legacy systems not designed to support large-scale AI integration. Transitioning from traditional rule-based systems to AI-powered models requires investments in hardware, software, and human resources with data science expertise. Moreover, training AI models requires large amounts of historical data, which may not be readily available or well-structured in existing government databases (Durojaiye, Ewim, & Igwe, 2024).

Data privacy is another major barrier. Since public assistance programs serve vulnerable populations, including low-income families and children, and heightened privacy and data protection concerns exist. Beneficiaries' personal and financial information must be safeguarded, as unauthorized access or misuse of this data could have serious social and legal repercussions. Privacy regulations, such as the General Data Protection Regulation (GDPR) in Europe and the Privacy Act in the United States, place strict controls on how government agencies can collect, store, and process personal data. These regulations limit the scope of data sharing between government departments, making it harder to create comprehensive datasets for AI model training. For instance, AI models that detect benefit misuse would benefit from access to cross-departmental data, such as employment history or tax filings, but privacy laws often restrict such access (A. O. Ishola, Odunaiya, & Soyombo, 2024a; Ogunyemi & Ishola).

Another significant barrier is system integration. Fraud detection models must work seamlessly with existing benefit distribution systems and payment platforms, such as EBT card processors and POS terminals. Integrating AI-based fraud detection into these systems without causing service disruptions is a major logistical challenge. Government systems are often fragmented, with different departments using separate platforms to manage different aspects of public assistance. Coordinating across multiple agencies to ensure smooth integration requires extensive collaboration, clear protocols, and substantial technical support (Bakare, Aziza, Uzougbo, & Oduro, 2024; A. Ishola, 2024).

Policy barriers further complicate AI deployment. While AI models can identify fraudulent patterns, agencies must ensure that action against beneficiaries is legally justified. For example, suppose an AI model flags a beneficiary for fraud. In that case, agencies must have clear, legally defensible criteria for denying or suspending benefits. Failure to do so could lead to lawsuits, public backlash, and accusations of bias. Ensuring compliance with anti-discrimination laws is critical, as flawed AI models may disproportionately flag certain demographic groups. Policymakers must also consider the potential for AI "black box" issues, where AI models make decisions that are not easily explainable to the public or to agency auditors (Ogunbiyi-Badaru, Alao, Dudu, & Alonge, 2024b; Onoja & Ajala, 2022).

Addressing these technological and policy barriers requires a multi-faceted approach. Governments must invest in modernizing IT infrastructure, adopt privacy-preserving AI techniques, and establish cross-agency data-sharing agreements. Equally important is the development of explainable AI (XAI) models that offer transparency in decision-making. Such models allow government officials to justify their decisions when beneficiaries challenge adverse actions, ensuring fairness and accountability.

3. Conceptual AI Framework for Fraud Detection

3.1. Core Components

The core components of an AI framework for fraud detection in public assistance programs are designed to leverage the power of advanced computational models to detect, prevent, and mitigate fraudulent activities. Unlike traditional rule-based systems that rely on static, predefined criteria, AI-driven models are dynamic, adaptive, and capable of learning from vast datasets. Key AI models used for fraud detection include machine learning (ML), anomaly detection, and predictive analytics.

Machine Learning (ML) is the backbone of modern fraud detection systems. It involves training algorithms to recognize patterns in large datasets and predict fraudulent behavior based on historical trends. Supervised ML models are commonly used in fraud detection, as they are trained using labeled datasets, where instances of fraud and non-fraud are clearly identified. The model "learns" to recognize the unique features of fraudulent behavior, such as unusual purchasing patterns, repeated transactions at specific times, or excessive cross-border transactions. Once trained, these models can accurately classify new, unseen transactions as legitimate or suspicious. On the other hand, unsupervised ML identifies patterns without pre-labeled data, making it particularly useful for detecting new or emerging types of fraud (AD Adekola & SA Dada, 2024; C. Mokogwu, G. O. Achumie, A. G. Adeleke, I. C. Okeke, & C. P.-M. Ewim, 2024).

Anomaly Detection is crucial in identifying unusual or abnormal activities that deviate from established norms. In the context of SNAP and EBT fraud detection, anomaly detection models can flag atypical transaction patterns, such as large purchases made in rapid succession, purchases made far from the beneficiary's usual location, or sudden spikes in spending. These models operate on the principle that fraudulent activity often deviates from normal behavioral patterns, allowing the system to identify outliers in real-time. Anomaly detection models are particularly useful for identifying new forms of fraud that traditional rule-based approaches may not yet capture.

Predictive Analytics further enhances fraud detection by forecasting the likelihood of fraudulent activities before they occur. By analyzing historical transaction data, these models can identify risk factors that are correlated with fraud, such as changes in purchasing behavior or sudden increases in high-risk transactions. For example, suppose a retailer has a history of collusion with beneficiaries. In that case, predictive models can flag their future transactions as high-risk, enabling proactive investigations. Predictive analytics helps government agencies anticipate potential fraud hotspots, allocate resources for prevention, and take preemptive actions before significant financial losses occur (AD Adekola & SA Dada, 2024; Bello & Olufemi, 2024).

These core components—machine learning, anomaly detection, and predictive analytics—form a comprehensive AI-driven approach to fraud detection. Each component addresses a specific aspect of fraud, from identifying known fraudulent patterns to detecting new and emerging threats. When combined, they create a multi-layered defense system that is adaptable, proactive, and capable of evolving alongside the changing tactics of fraudsters.

3.2. Interoperability

For an AI-powered fraud detection framework to be effective, it must be interoperable across various sectors and platforms. Interoperability refers to the ability of AI models to function seamlessly within different systems, databases, and organizational environments. Given the shared nature of fraud tactics across sectors, such as e-commerce, banking,

and public assistance programs, a unified AI framework can offer a cost-effective and efficient solution for combating fraud on multiple fronts (Attah, Garba, Gil-Ozoudeh, & Iwuanyanwu, 2024a; A. O. Ishola, Odunaiya, & Soyombo, 2024b).

One of the most critical aspects of interoperability is data integration. Public assistance programs, such as SNAP and EBT, operate within government databases, while e-commerce platforms store transactional data on private cloud-based systems. Creating data bridges that facilitate secure data sharing and integration is essential to build an interoperable AI framework. For example, insights gained from e-commerce fraud detection—such as patterns related to chargeback abuse or account takeovers—can be applied to public assistance programs to identify similar behaviors, like benefit trafficking or identity theft. Integrating these datasets allows the AI model to recognize cross-sector patterns, thereby improving the model's ability to detect fraud (Achumie, Ewim, Gbolahan, Adeleke, & Mokogwu; Attah, Garba, Gil-Ozoudeh, & Iwuanyanwu, 2024b).

Interoperability also requires cross-platform compatibility. AI fraud detection models should be compatible with a range of transaction systems, point-of-sale (POS) terminals, and digital payment platforms. For example, public assistance programs rely on EBT card systems, while e-commerce platforms use online payment gateways. Designing AI models that can analyze transaction data from both systems allows for cross-sector fraud detection, where suspicious activity on one platform may trigger an alert in another. This is particularly useful in identifying fraudsters who operate across multiple sectors. For example, a fraudster who exploits e-commerce return policies may use similar tactics to abuse SNAP benefits, such as returning items bought with EBT cards for cash refunds. Cross-sector interoperability enables agencies and private entities to share fraud intelligence, thereby creating a more unified defense.

System standardization is another crucial element of interoperability. Fraud detection frameworks must adhere to common data standards and protocols to ensure compatibility. For instance, financial institutions and e-commerce platforms often use standardized formats like ISO 8583 for payment transactions. Public assistance programs must align their data formats with these industry standards to enable seamless information exchange. Additionally, application programming interfaces (APIs) allow AI models to plug into existing transaction systems and databases, facilitating real-time fraud detection across sectors. By enabling interoperability, agencies can leverage insights from one sector to inform fraud detection strategies in another, thereby improving overall system efficiency and responsiveness (Dada, Okonkwo, & Cudjoe-Mensah, 2024).

3.3. Ethical Design

The development of an AI-powered fraud detection framework must prioritize ethical considerations to ensure fairness, accountability, and transparency. Public assistance programs serve vulnerable populations, including low-income families, elderly individuals, and children. As such, the design of AI models must be sensitive to the potential harms that could arise from false positives, discriminatory outcomes, and opaque decision-making processes. Ethical design principles help build trust, reduce bias, and ensure that fraud detection efforts do not inadvertently deny assistance to those in need.

One of the most pressing ethical concerns is algorithmic bias. AI models learn from historical data; if that data contains biases, the model may replicate and even amplify those biases. For instance, if an AI model is trained on data that disproportionately flags certain demographic groups as "high risk," the model may unfairly target these groups for fraud investigations. To address this, data scientists must ensure that training datasets are diverse, representative, and free from inherent biases. Techniques such as bias auditing and fairness testing can help identify and mitigate algorithmic bias before the model is deployed. Moreover, developers should use "explainable AI" (XAI) models, which provide clear, human-readable justifications for their decisions, thereby promoting accountability (Adewumi, Dada, Azai, & Oware, 2024).

Transparency is another key component of ethical design. Beneficiaries affected by fraud detection decisions should have access to explanations for why their transactions were flagged. Traditional AI models, especially those built using deep learning, operate as "black boxes," where the logic behind decisions is difficult to understand. To avoid this, explainable AI models can offer human-readable justifications, such as "Transaction flagged because of unusual purchase location" or "High frequency of purchases in a short period." Transparency builds trust and allows beneficiaries to challenge unjust decisions. It also enables government agencies to defend their use of AI in court, thereby reducing the risk of legal challenges (Olaleye & Mokogwu, 2024c).

Accountability is equally important in ethical AI design. When AI models make errors—such as flagging legitimate beneficiaries as fraudsters—there must be a process for affected individuals to seek redress. Government agencies must establish mechanisms for appeal, review, and correction. Additionally, accountability requires regular audits of the AI

system to ensure it remains fair and effective over time. This includes retraining the model periodically to reflect changes in fraud tactics and reviewing its performance for signs of bias or error (Ogunyemi & Ishola; Olaleye & Mokogwu, 2024b, 2024c).

Privacy protection is a final ethical consideration, especially since public assistance programs handle sensitive beneficiary information. AI models require access to large datasets, but this access must be balanced with privacy rights. Privacy-enhancing technologies, such as differential privacy and federated learning, allow AI models to learn from data without exposing individual records. For example, federated learning allows AI models to be trained locally on devices, with only aggregated model updates being shared. This approach enhances privacy while maintaining the model's effectiveness (Durojaiye et al., 2024).

4. Economic and Social Implications

4.1. Economic Benefits

The economic benefits of implementing AI-powered fraud detection in public assistance programs are substantial. Fraud drains valuable public resources that could otherwise be used to support vulnerable populations. By leveraging AI to detect and prevent fraudulent activities, government agencies can reduce financial losses, optimize resource allocation, and enhance operational efficiency.

One of the most immediate economic benefits is cost savings. Fraud in public assistance programs like SNAP and EBT often results in millions of dollars in lost funds annually. By deploying AI-driven fraud detection models, agencies can identify and prevent fraudulent transactions in real time, thereby reducing the volume of funds lost to fraud. For example, predictive analytics can flag high-risk transactions before they are fully processed, enabling authorities to freeze or review them. This proactive approach minimizes the need for costly, time-consuming post-fraud investigations and fund recovery efforts. Governments can redirect these savings toward expanding benefits, enhancing program infrastructure, or supporting other social welfare initiatives (Alao, Dudu, Alonge, & Eze, 2024; Ogunbiyi-Badaru et al., 2024a).

Operational efficiency is another significant economic benefit. Traditional fraud detection methods, such as manual audits and whistleblower reports, are labor-intensive and slow. These methods require human investigators to review transaction logs, interview beneficiaries, and verify claims, which can take weeks or months. AI models, on the other hand, operate continuously and autonomously, analyzing thousands of transactions in seconds. By automating fraud detection, public assistance agencies can significantly reduce the workload of human auditors and investigators. This allows agencies to reallocate human resources to more complex cases that require human judgment, further improving efficiency (Attah et al., 2024b).

Resource optimization is also a key economic advantage. By detecting and addressing fraud early, public assistance programs can ensure that resources are allocated to legitimate beneficiaries who genuinely need support. For instance, if an AI model identifies identity theft cases where fraudsters are posing as legitimate recipients, the agency can quickly intervene, recover funds, and reallocate them to eligible individuals. This ensures that limited financial resources are distributed equitably, rather than being lost to fraudulent schemes. Furthermore, with fewer funds being misused, government agencies are less likely to face budget shortfalls, which can otherwise trigger calls for austerity measures or cuts to vital assistance programs (Attah et al.; N. I. Okeke, Bakare, & Achumie, 2024).

Finally, improved public trust and accountability have indirect economic benefits. When citizens see that government agencies are taking strong, transparent action to prevent fraud, they are more likely to support the continued funding of public assistance programs. Public perception of government efficiency and accountability increases, which, in turn, strengthens political support for social welfare initiatives. Effective fraud prevention can also reduce the pressure for increased oversight, audits, and administrative reviews, each carrying a significant cost. Thus, an AI-powered fraud detection system reduces direct financial losses and creates long-term cost savings by improving public confidence and reducing oversight burdens (A. Ishola, 2024).

4.2. Social Equity

Social equity is a core principle underpinning public assistance programs that aim to support vulnerable and underserved populations. However, fraud in these programs jeopardizes social equity by diverting resources away from those in genuine need. AI-driven fraud detection systems can help restore equity by ensuring that benefits are distributed fairly while minimizing the risk of false accusations and unjust denial of assistance.

A key aspect of social equity is fair access to benefits. Fraud can distort access by depleting program funds and creating administrative bottlenecks. For instance, when fraudsters steal benefits through identity theft or card skimming, legitimate recipients may experience delays in accessing their funds. By detecting and preventing such fraud, AI systems help maintain public assistance programs' integrity, ensuring that only eligible beneficiaries receive the intended support. This contributes to a more equitable distribution of resources and protects vulnerable populations from being unfairly deprived of essential aid.

Preventing wrongful accusations and "false positives" is another crucial element of social equity. Traditional fraud detection systems often rely on static rules, such as flagging large or geographically distant purchases as suspicious. However, such rules may inadvertently target legitimate beneficiaries, especially those who travel for work or relocate to new areas. AI-powered fraud detection, particularly models incorporating explainable AI (XAI), can reduce these false positives by considering the broader context of a beneficiary's behavior. For example, suppose an AI system recognizes that a beneficiary's transaction history shows a pattern of monthly interstate purchases. In that case, it will be less likely to flag similar future transactions as fraudulent. By reducing the risk of false accusations, AI systems promote fairness and ensure that beneficiaries are not unfairly penalized.

Protecting vulnerable populations is a critical aspect of promoting social equity. Public assistance programs often serve low-income families, children, elderly individuals, and marginalized communities. Fraudsters who steal from these programs deplete public resources and undermine beneficiaries' financial security. AI systems can identify and address identity theft more quickly, reducing the time beneficiaries spend without access to essential benefits. Moreover, by mitigating the risk of wrongful denials, AI-driven systems help to protect marginalized groups from unnecessary hardship. Finally, equitable accountability is essential in the context of social equity. While fraud detection is important, it must be done fairly and in due process. Beneficiaries flagged for fraud should be able to challenge adverse decisions and seek redress. Ethical AI frameworks prioritizing transparency and accountability ensure that beneficiaries know the reasons behind AI-driven decisions. This allows them to appeal wrongful decisions, reinforcing the principle of "equity before the law." Without such safeguards, vulnerable populations could be unfairly punished due to opaque AI decision-making processes.

4.3. Policy Alignment

Effective fraud detection requires alignment between technological solutions and regulatory frameworks. AI-powered systems must comply with privacy laws, anti-discrimination regulations, and administrative due process rules. Policy alignment ensures that AI models are legally and ethically sound, reducing the risk of legal challenges and public backlash.

Data privacy and protection are paramount in policy alignment. Public assistance programs collect sensitive beneficiary information, including income details, personal identification, and transactional data. Regulations like the U.S. Privacy Act, the European Union's General Data Protection Regulation (GDPR), and state-level privacy laws establish strict guidelines for collecting, storing, and using this information. AI systems must comply with these laws to avoid potential breaches of beneficiary privacy. This can be achieved through privacy-preserving AI techniques, such as differential privacy and federated learning, which allow machine learning models to analyze data without exposing individual records.

Non-discrimination and bias mitigation are also crucial to policy alignment. Anti-discrimination laws, such as Title VI of the U.S. Civil Rights Act, prohibit public programs from discriminating based on race, ethnicity, or other protected characteristics. However, AI models trained on biased data may inadvertently flag certain groups as "high risk," leading to disparate outcomes. To address this, policymakers and system developers must conduct fairness audits, ensure demographic representation in training datasets, and prioritize the use of explainable AI (XAI) systems. When beneficiaries can understand why they were flagged for fraud, they are more likely to trust the system.

Accountability and due process are policy considerations that affect how beneficiaries are treated when flagged for potential fraud. Due process rights require that beneficiaries be notified of adverse decisions, given the opportunity to contest them, and provided with clear explanations. AI-driven fraud detection systems must align with these principles by offering human oversight and appeal mechanisms. For instance, if a beneficiary is flagged for potential fraud, they should receive a clear, comprehensible explanation of why the system reached that decision. Additionally, human reviewers should be able to override AI decisions if errors are discovered (Dada et al., 2024; Ogunyemi & Ishola; Olaleye & Mokogwu, 2024b).

5. Conclusion and Recommendations

Fraud in public assistance programs, such as SNAP and EBT, poses significant challenges that affect these initiatives' economic, social, and operational integrity. Fraudulent activities divert essential resources away from vulnerable populations, undermining the primary goal of public assistance programs. Traditional detection methods, such as manual audits and static rule-based systems, have proven inadequate in combating the sophistication and evolution of modern fraud schemes. To address these limitations, AI-powered fraud detection frameworks offer a proactive, efficient, and adaptive approach. By leveraging machine learning (ML), anomaly detection, and predictive analytics, AI frameworks can detect fraudulent patterns in real-time, significantly reducing losses and enhancing program integrity. This shift from reactive to proactive detection marks a critical evolution in the fight against fraud.

The conceptual AI framework for fraud detection incorporates essential components that ensure its adaptability, accuracy, and effectiveness. Machine learning algorithms enable the identification of emerging fraud patterns, while anomaly detection systems flag unusual activity in real time. Predictive analytics enhances foresight, allowing systems to anticipate and prevent fraudulent activities before they occur. Interoperability is another vital framework element, ensuring that AI models operate seamlessly across various platforms, such as public assistance systems, e-commerce platforms, and financial services. This cross-sector alignment strengthens the framework's ability to detect multi-sector fraud schemes, thereby enhancing the efficiency and effectiveness of fraud detection systems.

Ethical design principles ensure that AI-based fraud detection systems operate fairly and equitably. Issues of bias, transparency, and accountability must be addressed to protect beneficiaries from unfair treatment. AI models must be subjected to fairness audits to identify and correct potential biases that may target certain demographic groups unfairly. Explainable AI (XAI) tools should be utilized to provide beneficiaries with clear, comprehensible explanations for adverse decisions. Furthermore, redress mechanisms must be established to allow individuals to contest flagged fraud cases, ensuring that beneficiaries have the right to challenge and correct wrongful accusations. Incorporating ethical design principles strengthens trust in AI systems and ensures that public assistance programs remain equitable and just.

The economic and social implications of AI-driven fraud detection are profound. Economically, AI frameworks reduce financial losses, minimize operational costs, and optimize resource allocation. Public assistance programs can redirect resources toward their intended beneficiaries by detecting and preventing fraud at an early stage. Socially, AI frameworks promote fairness and equity, ensuring that eligible individuals can access the necessary benefits. False accusations of fraud, which can have severe consequences for vulnerable populations, are reduced through the use of ethical AI models. Policy alignment with legal frameworks, such as data privacy laws and anti-discrimination regulations, is crucial for ensuring compliance. Adhering to these regulations establishes a legally and ethically sound framework, thereby promoting AI's fair and transparent use in public resource protection.

Several recommendations must be implemented to fully realize the potential of AI-driven fraud detection. Ethical design principles should be embedded into AI models to ensure fairness, transparency, and accountability. Cross-sector interoperability should be prioritized to enable seamless data exchange across public assistance programs, e-commerce platforms, and financial services. Scalability must be emphasized to ensure that AI models can adapt to evolving fraud tactics. Privacy and data protection must be prioritized to comply with regulations such as GDPR and the U.S. Privacy Act. Public-private collaboration should be fostered to facilitate knowledge sharing and develop coordinated anti-fraud responses. Finally, accountability and continuous improvement mechanisms must be established to ensure that AI models remain fair, accurate, and effective over time. Together, these strategies provide a holistic and future-proof approach to fraud detection, safeguarding the economic and social integrity of public assistance programs.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Achumie, G. O., Ewim, C. P.-M., Gbolahan, A., Adeleke, I. C. O., & Mokogwu, C. Supply Chain Optimization in Technology Businesses: A Conceptual Model for Operational Excellence.

[2] Adekola, A., & Dada, S. (2024). Optimizing pharmaceutical supply chain management through AI-driven predictive analytics. A conceptual framework. Computer Science & IT Research Journal, 5(11), 2580-2593. doi:DOI: 10.51594/csitrj.v5i11.1709

[3] Adekola, A., & Dada, S. (2024). The role of Blockchain technology in ensuring pharmaceutical supply chain integrity and traceability. Finance & Accounting Research Journal, 6(11), 2120-2133. doi:DOI: 10.51594/farj.v6i11.1700

[4] Adewumi, G., Dada, S., Azai, J., & Oware, E. (2024). A systematic review of strategies for enhancing pharmaceutical supply chain resilience in the U.S. International Medical Science Research Journal, 4(11), 961-972. doi:DOI: 10.51594/imsrj.v4i11.1711

[5] Alao, O. B., Dudu, O. F., Alonge, E. O., & Eze, C. E. (2024). Automation in financial reporting: A conceptual framework for efficiency and accuracy in US corporations. Global Journal of Advanced Research and Reviews, 2(02), 040-050.

[6] Anozie, U., Dada, S., Okonkwo, F., Egunlae, O., Animasahun, B., & Mazino, O. (2024). The convergence of edge computing and supply chain resilience in retail marketing. . International Journal of Science and Research Archive, 12(02), 2769–2779. doi:DOI: 10.30574/ijsra.2024.12.2.1574

[7] Asolo, E., Gil-Ozoudeh, I., & Ejimuda, C. (2024). AI-Powered Decision Support Systems for Sustainable Agriculture Using AI-Chatbot Solution. Journal of Digital Food, Energy & Water Systems, 5(1).

[8] Attah, R. U., Garba, B. M. P., Gil-Ozoudeh, I., & Iwuanyanwu, O. Enhancing supply chain resilience through artificial intelligence: Analyzing problem-solving approaches in logistics management.

[9] Attah, R. U., Garba, B. M. P., Gil-Ozoudeh, I., & Iwuanyanwu, O. (2024a). Strategic frameworks for digital transformation across logistics and energy sectors: Bridging technology with business strategy.

[10] Attah, R. U., Garba, B. M. P., Gil-Ozoudeh, I., & Iwuanyanwu, O. (2024b). Strategic partnerships for urban sustainability: Developing a conceptual framework for integrating technology in community-focused initiatives.

[11] Bakare, O. A., Aziza, O. R., Uzougbo, N. S., & Oduro, P. (2024). A governance and risk management framework for project management in the oil and gas industry. Open Access Research Journal of Science and Technology, 12(01), 121-130.

[12] Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer Science & IT Research Journal, 5(6), 1505-1520.

[13] Blitstein, J., Hansen, D., Wroblewska, K., Thorn, B., Kessler, C., Giombi, K., . . . Lopez-Rios, M. (2023). Best Practices in Disaster SNAP Operations and Planning.

[14] Bosso, C. J. (2023). Why SNAP Works: A Political History—and Defense—of the Food Stamp Program: Univ of California Press.

[15] Dada, S., Okonkwo, F., & Cudjoe-Mensah, Y. (2024). Sustainable supply chain management in U.S. healthcare: Strategies for reducing environmental impact without compromising access. International Journal of Science and Research Archive, 13(02), 870–879. doi:DOI: 10.30574/ijsra.2024.13.2.2113

[16] Davies, G. K. Impact of Healthcare Fraud on Racial Disparities in Health Outcomes in the United States.

[17] Durojaiye, A. T., Ewim, C. P.-M., & Igwe, A. N. Designing a machine learning-based lending model to enhance access to capital for small and medium enterprises.

[18] Durojaiye, A. T., Ewim, C. P.-M., & Igwe, A. N. (2024). Developing a crowdfunding optimization model to bridge the financing gap for small business enterprises through data-driven strategies.

[19] Hassan, M., Aziz, L. A.-R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics, 6(1), 110-132.

[20] Ishola, A. (2024). Global renewable energy transition in fossil fuel dependent regions. World Journal of Advanced Research and Reviews, 24(01), 1373-1138.

[21] Ishola, A. O., Odunaiya, O. G., & Soyombo, O. T. (2024a). Framework for tailoring consumer-centric communication to boost solar energy adoption in US households.

[22] Ishola, A. O., Odunaiya, O. G., & Soyombo, O. T. (2024b). Stakeholder communication framework for successful implementation of community-based renewable energy projects.

[23] Ismaeil, M. K. A. (2024). Harnessing AI for Next-Generation Financial Fraud Detection: A DataDriven Revolution. Journal of Ecohumanism, 3(7), 811-821.

[24] Kuhn, M. A. (2021). Electronic benefit transfer and food expenditure cycles. Journal of Policy Analysis and Management, 40(3), 744-773.

[25] Lad, S. (2024). Harnessing machine learning for advanced threat detection in cybersecurity. Innovative Computer Sciences Journal, 10(1).

[26] Mills, R. M. (2022). Enhancing Anomaly Detection Techniques for Emerging Threats: Lancaster University (United Kingdom).

[27] Mokogwu, C., Achumie, G. O., Adeleke, A. G., Okeke, I. C., & Ewim, C. P.-M. (2024). A leadership and policy development model for driving operational success in tech companies. International Journal of Frontline Research in Multidisciplinary Studies, 4(1), 1-14.

[28] Mokogwu, C., Achumie, G. O., Gbolahan, A., Adeleke, I. C. O., & Ewim, C. P.-M. A Conceptual Model for Enhancing Operational Efficiency in Technology Startups: Integrating Strategy and Innovation.

[29] Mokogwu, O., Achumie, G. O., Adeleke, A. G., Okeke, I. C., & Ewim, C. (2024). A data-driven operations management model: Implementing MIS for strategic decision making in tech businesses. International Journal of Frontline Research and Reviews, 3(1), 1-19.

[30] Ogunbiyi-Badaru, O., Alao, O. B., Dudu, O. F., & Alonge, E. O. (2024a). Blockchain-enabled asset management: Opportunities, risks and global implications.

[31] Ogunbiyi-Badaru, O., Alao, O. B., Dudu, O. F., & Alonge, E. O. (2024b). The impact of FX and fixed income integration on global financial stability: A comprehensive analysis.

[32] Ogunyemi, F. M., & Ishola, A. O. Global competitiveness and environmental sustainability: financing and business development strategies for US SMEs.

[33] Ogunyemi, F. M., & Ishola, A. O. (2024a). Data-driven financial models for sustainable SME growth: Integrating green finance into small and medium enterprise strategies.

[34] Ogunyemi, F. M., & Ishola, A. O. (2024b). Encouraging investment in renewable energy through data-driven analytics and financial solutions for SMEs.

[35] Okeke, I. C., Agu, E. E., Ejike, O. G., Ewim, C. P.-M., & Komolafe, M. O. (2022). A conceptual model for financial advisory standardization: Bridging the financial literacy gap in Nigeria. International Journal of Frontline Research in Science and Technology, 1(02), 038-052.

[36] Okeke, N. I., Bakare, O. A., & Achumie, G. O. (2024). Forecasting financial stability in SMEs: A comprehensive analysis of strategic budgeting and revenue management. Open Access Research Journal of Multidisciplinary Studies, 8(1), 139-149.

[37] Olaleye, I., & Mokogwu, V. (2024a). Ehancing Economic Stability and Efficiency Through Strategic Inventory Control Innovation. International Journal of Advanced Economics, 6(12), 747-759. doi:DOI: 10.51594/ijae.v6i12.1750

[38] Olaleye, I., & Mokogwu, V. (2024b). Transforming Supply Chain Resilience: Frameworks and Advancements in Predictive Analytics and Data-Driven Strategies. Open Access Research Journal of Multidisciplinary Studies, 08(02), 085–093. doi:https://doi.org/10.53022/oarjms.2024.8.2.0065

[39] Olaleye, I., & Mokogwu, V. (2024c). Unlocking Competitive Advantage in Emerging Markets Through Advanced Business Analytics Frameworks. GSC Advanced Research and Reviews, 21(02), 419–426. doi:https://doi.org/10.30574/gscarr.2024.21.2.0455

[40] Onoja, J. P., & Ajala, O. A. (2022). Innovative Telecommunications Strategies for Bridging Digital Inequities: A Framework for Empowering Underserved Communities. GSC Advanced Research and Reviews, 13(01), 210–217. doi:https://doi.org/10.30574/gscarr.2022.13.1.0286

[41] Onoja, J. P., & Ajala, O. A. (2023). AI-Driven Project Optimization: A Strategic Framework for Accelerating Sustainable Development Outcomes. GSC Advanced Research and Reviews, 15(01), 158–165. doi:https://doi.org/10.30574/gscarr.2023.15.1.0118

[42] Robinson, A. M. (2020). Exploring Transformational Leadership of the Supplemental Nutrition Assistance Program: A Qualitative Phenomenological Study. Northcentral University,

[43] Shah, V. (2021). Machine learning algorithms for cybersecurity: Detecting and preventing threats. Revista Espanola de Documentacion Cientifica, 15(4), 42-66.

[44] Shoetan, P. O., & Familoni, B. T. (2024). Transforming fintech fraud detection with advanced artificial intelligence algorithms. Finance & Accounting Research Journal, 6(4), 602-625.

[45] Surak, K. (2023). The golden passport: Global mobility for millionaires: Harvard University Press.

[46] Waqas, M., Tu, S., Halim, Z., Rehman, S. U., Abbas, G., & Abbas, Z. H. (2022). The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges. Artificial Intelligence Review, 55(7), 5215-5261.