

The role of Artificial Intelligence in reducing financial fraud in U.S. healthcare systems

Afari Ntiakoh ^{1,*}, Isaiah Thompson Ocansey ² and Christian Amoakoh ³

¹ *University of Nevada, Reno, USA.*

² *Independent Researcher, Texas, USA.*

³ *Illinois State University, USA.*

Magna Scientia Advanced Research and Reviews, 2026, 17(02), 128–134

Publication history: Received on 01 June 2026; revised on 07 July 2026; accepted on 10 July 2026

Article DOI: <https://doi.org/10.30574/msarr.2026.17.2.0130>

Abstract

Healthcare fraud is a major problem in the United States, which annually totals tens of billions of dollars and impacts financial sustainability, as well as patient confidence. Traditional forms of detection, such as manual risk audits and static category rule-based solutions, are becoming less effective in the face of fraudster sophistication and ever-evolving fraudulent tactics. Based on a systematic review of peer-reviewed articles, policy reports, and industry white papers, this article examines how artificial intelligence (AI) can be used to reduce financial fraud in U.S. healthcare systems. Results demonstrate the potential of machine learning, combined with NLP and predictive analytics, to add value in terms of detection accuracy, false-positive rate reduction, and near real-time fraud prevention. Moreover, integration with AI human-in-the-loop is demonstrated to increase efficiency with retention of supervision. However, some obstacles persist around data quality, bias of algorithms, interpretability, and regulatory aspects. In all, AI has strong potential as a game-changer in the fight against healthcare fraud if it is rolled out subject to robust governance and ethical considerations.

Keywords: Artificial Intelligence; Healthcare Fraud; Machine Learning; Fraud Detection

1. Introduction

The US healthcare system continues to confront the challenge of widespread financial fraud, which costs the industry billions per year and compromises care delivered. Depending on who you ask, fraud, waste, and abuse (FWA) of the national annual health care spend represents a loss between \$68 billion, independently reported by anti-fraud agencies within industry as well as academia (Griffin 2017). Fraudulent behaviors such as ghost billing, overbilling, double billing, and the stealing of medical identity (Iweriebor 2023), and unnecessary procedures escalate insurance premiums and drain programs such as Medicare and Medicaid, which in turn threaten patient safety by encouraging unwarranted treatments and false records (Foglia 2020).

Traditional approaches to fight healthcare fraud have traditionally been based on manual audits, retrospective reviews, and rule-based systems (Azad, T. et al., 2024). These detection methods, however, are slow and reactive in nature and are largely ineffective against more sophisticated scams (Aziz, L. A. R. et al., 2023). False positive rates are high, with consequent work overload for investigators and large amounts of fraud undetected (Ntiakoh et al, 2026).

AI, specifically machine learning (ML), natural language processing (NLP), and predictive analytics, gives us the answer in a more proactive and scalable manner. AI in auditing using structured and unstructured data, one can find out hidden patterns, discreet relations, or anomalies that are not detectable by human auditors or rule-based systems (Taha 2025). For example, ML algorithms applied to Medicare claims have shown increased fraud detection performance with feature engineering, adaptive learning, and class-imbalance mitigation methods (Karthik, K.P. et al., 2025). In addition to the

* Corresponding author: Afari Ntiakoh

above, NLP improves detection by scanning clinical notes taken by doctors and free-text billing narratives for differences.

In contrast to the traditional models, AI-based approaches mitigate false positives as well as offer near real-time fraud detection while transforming the insurance industry from a “pay-and-chase” model to that of preventive action (Ismaeil 2024), and with less manual fraud monitoring, compliance teams and providers can spend more of their time on patient care (Boda, V.V.R. et al., 2021). Yet AI implementation in fighting health care fraud is not without its obstacles. Privacy of data, bias in algorithms, transparency and interpretability of AI models, as well as the integration with existing IT systems, are still challenges for large-scale adoption (Mensah 2023). Addressing these questions will be critical to ensure that AI systems are transparent, fair and meet U.S. health care regulations. If so, AI is a tremendous asset in the fight to prevent financial fraud within US healthcare systems. By integrating speed, scale, and agility, AI has the power to save billions in healthcare spending while protecting patient safety and increasing confidence throughout the healthcare value chain (Luo, J. et al., 2016).

2. Literature review

2.1. Introduction

Healthcare fraud remains a source of economic and ethical drain on the U.S. healthcare system, one that not only impacts financial profitability but also patient trust. With billions worth of financial losses attributed to fraudulent activities every year, traditional detection techniques, including rule-based checks and the manual audits currently used by insurance companies, are proving insufficient in fighting against the scale and complexity of fraud. Hence, artificial intelligence (AI) has increasingly received scholarly and policy attention as a transformative means to detect, prevent, and reduce fraud. This review of literature presents an analysis of the economic impact of health care fraud, the use case for AI tools such as ML, NLP, and predictive analytics, challenges, opportunities, and collaborative approaches revealed in recent studies.

2.2. The Financial Fraud Burden in U.S. Healthcare

Economic fraud is considered a significant threat to the U.S. healthcare sector, and financial losses of \$100–300 billion have been estimated annually due to fraudulent practices (Timofeyev, Y., et al., 2022), including billing for services or other treatments undelivered, record falsifications, up-coding, and kickbacks (Couffinhal, A. et al., 2017). Medicare and Medicaid programs are particularly susceptible to these losses because of their size and the large number of beneficiaries. Traditional fraud detection techniques such as manual audits and reactive scrutiny are often inadequate to cope with the evolving nature of fraudulent activities (Elumilade, O.O. et al., 2021). This leads to inefficiencies and time lag before you can catch fraud, which is why we need state-of-the-art solutions like artificial intelligence.

2.3. Artificial Intelligence in Utilization and Billing Fraud Detection

The automation of techniques and the integration of technology have made AI an innovative means to address healthcare fraud, especially when dealing with large volumes of high-dimensional data. Supervised and unsupervised machine learning (ML) methods have been shown to be very successful for fraud detection (Trivedi, N.K. et al., 2020). Supervised models, based on feedback of past cases (fraudulent and not fraudulent), can detect suspicious billing, such as frequent claims more than peer averages for high-cost procedures, which were reported when trained on historical fraud reports (Machireddy 2022). On the other hand, unsupervised learning methods, such as clustering and anomaly detection, are good at discovering new types of fraud without training data (Cholevas, C. et al., 2024). By way of illustration, clustering can detect the outlying providers with considerably different billing patterns than other peers, which may indicate fraudulent behavior.

2.4. Natural Language Processing (NLP) and Unstructured Data Analytics

Structured claims data is the mainstay for fraud detection, but even unstructured medical data in the form of physician notes, discharge summaries, and prescriptions may disclose fraudulent behavior. With NLP, these unstructured texts can be mined for computational analysis to support cross-verification of between the medical documentation and the billing records. For instance, if the notes of a physician are contradictory to the billed procedure, NLP applications can point out this discrepancy for further checking (Reddy, 2024). Insurance companies already incorporated NLP tools for fraud detection, which increased accuracy and decreased false positives (Mwangi, 2024).

2.5. Real-Time Fraud Prevention and Predictive Analytics

When it comes to fraud, real-time scam detection is another great advantage that AI offers. AI systems based on predictive analytics and deep learning can process claims in real time, rather than give them the once-over months after the fact. This allows for early detection of potentially fraudulent claims and prevents recovery after payment (Ahmed, M. et al., 2014). For example, CMS has stated that it saved billions of dollars by incorporating predictive analytics tools to identify high-risk claims to be profiled in near real-time (Pamulaparthi Venkata, S. et al., 2020). This evolution away from reactive to proactive fraud detection is a significant leap toward protecting the finances of healthcare.

But even so, AI adoption in healthcare fraud detection also presents several ethical and regulatory issues. One major concern is algorithmic bias, whereby poorly trained models may unfairly focus on some providers or patient populations because of a biased data set (Savitha, S. et al., 2025). In addition, AI models, particularly deep learning techniques, have been described as “black boxes” because they are not always interpretable, and this can present compliance challenges associated with the transparency obligations under the privacy rule (Hassija, V. et al., 2024). Furthermore, widely scattered health data from institutions hinders the interconnection, which leads to the low availability and trustworthiness of health models. These are significant challenges, and making AI models more explainable (XAI) and governance frameworks more robust must be considered.

2.6. Human-AI Collaboration in Fraud Detection

Academics warn that the best fraud-detection approaches involve AI and human judgment. Although AI is good at spotting hidden patterns within big data sets, human investigators still play a vital role in contextual judgment making, ethical oversight, and legal interpretation (Holzinger, A. et al., 2025). Hybrid solutions, in which A.I. systems highlight anomalies for auditors to investigate, strike a balance between speed and accountability. For instance, an A.I. system could spot unusual billing patterns, but only a human auditor can say whether that behavior is fraudulent or a reasonable reflection of patient complexity. This cooperative approach has been proven to provide higher accuracy and trust in critical fraud systems.

2.7. Summary

The literature covered demonstrates the potential and obstacles of AI to detect financial fraud in U.S. healthcare. AI techniques like machine learning, NLP, and predictive analytics have proven to be effective at identifying sophisticated fraud patterns and proactively intervening with dramatic cost reductions and system enhancements. However, ethical issues, data governance, and concerns regarding transparency also represent key challenges to its wide implementation. Our evidence, collectively implying that AI is part of, rather than in place of (best-of-both-worlds), human scrutiny may occur in the presence of understandable reasons for it, “AI as Panacea” is not thinkable as a single panacea, but suitable to complement ongoing human expertise is required for financial accountability, regulatory obedience, and trust in healthcare service provision.

3. Case studies

3.1. Optum’s AI-Driven Fraud Detection

Optum, a health services and innovation company, has implemented an AI-powered solution to combat healthcare fraud, waste, and abuse (FWA). Its platform utilizes a blend of machine learning, predictive analysis, and Natural Language Processing (NLP) to analyze vast volumes of claims data in near real-time. It goes beyond rule-based techniques that are often only able to detect known fraud by utilizing supervised and unsupervised learning models to recognize subtle anomalies and develop patterns. For example, the unsupervised models can identify anomalous billing practices or competing networks of providers that differ vastly from established norms, even if they don’t violate a specific, predefined rule. Optum’s workload proactivity has enabled the company to flag the tens of millions of dollars in FWA, proving that AI yields an impressive financial return on investment.

There were some challenges in the execution, notably how to mesh the AI system with already-in-place workflows. The company took a human-in-the-loop approach where the AI system flags high-risk claims for human investigators to review. This hybrid process guarantees due process and enables experienced investigators to apply their expertise in those cases that are complex, with AI handling most of the data analysis and triage. The ability of the system to offer Explainable AI (XAI) insights, including pinpointing certain features or data points that resulted in a fraud flag, has proved extremely useful for gaining trust as well as for driving collaboration between data scientists and fraud investigators.

This client story shows how one of the leading providers of health technology implemented AI for fraud detection and modernized its operations. It emphasizes the need for a multi-modal approach that leverages various AI techniques and combines them into one single human-machine collaborative workflow. The bottom line is AI cannot just find more fraud but do so while making human teams more efficient and effective, leading to significant cost savings and increased program integrity.

3.2. Medicare's Fraud Prevention System (FPS)

The Fraud Prevention System (FPS) was initiated by the Centers for Medicare & Medicaid Services (CMS) in 2011 to identify and prevent fraudulent payments in the fee-for-service portion of the Medicare program. The system epitomizes a real-time AI solution on a scale. Before FPS, Medicare operated under a “pay-and-chase” system that generally permitted payment of fraudulent claims and relied on post-payment review techniques to recover payments found to be improper. FPS, on the other hand, evaluates claims data via a sophisticated mileage prediction analytics engine at the point of submission. The system employs an extensive set of analytics and scoring algorithms to rate-order the risk of each claim, identifying suspicious transactions for review or outright denial before payment.

An important element of FPS is predictive analytics and anomaly detection. The model is then trained on sets of historical fraudulent and non-fraudulent claims to learn and predict which claims will be fraudulent. It also flags providers and beneficiaries that display unusual billing or usage patterns, which may indicate fraud rings or scams. It has enabled CMS to move from a reactive to a proactive stance, with a considerable decrease in fraud losses. CMS has said that FPS “aided in the identification and prevention of more than \$1.5 billion in improper payments in its early years,” reinforcing the cost-effective benefits associated with real-time AI interdiction.

The story of FPS is a testament to the strength of using AI nationally to combat organized fraud. It demonstrates that real-time AI solutions are possible to operate on very large and complex data sets to catch fraudulent payments before they occur. The case also illustrates the need for technology, data, and infrastructure investment by the government to lead innovation in this space, as it demands a critical mass of technology and data investments. The key takeaway from FPS is that proactive, data-driven strategies are far more effective than retrospective audits in combating large-scale fraud networks.

3.3. Cigna's AI And Machine Learning Strategy.

Cigna, a worldwide provider of healthcare, recently announced that it uses AI and ML to detect fraud in the healthcare sector. And knowing the only constant is change, Cigna's fraud detection solution uses a range of ML models to assess claim and provider behaviors compared to established rules. The system uses supervised learning models based on millions of past claims, so it can predict how likely new submissions are to be fraudulent. They run unsupervised learning algorithms to detect anomalous billing patterns or “outlier” providers indicative of a novel form of fraud, a feature unavailable in rule-based systems.

A cornerstone of how Cigna does this is that they constantly retrain their AI models. When new scams rear up, fresh input is provided to the system to reschool the models, so they don't become obsolete fighting new threats. This is a solution to the problem of “concept drift,” which is widely discussed in academia. Cigna's system also addresses quenching the false positives, legitimate claims tagged as fraudulent, a bane with older detection systems. By refining their models, Cigna has found that it can increase the accuracy of detection while decreasing the administrative load on investigators, who can concentrate on the most severe cases.

Cigna shows how a constantly evolving, learning AI system is necessary to outsmart these savvy fraudsters. It demonstrates that an effective AI strategy is not about one model but rather an entire ecosystem of integrated technologies involving data pipelines, ML models, and feedback loops for iterated improvement. The detailed study is a real-life example of how a private insurer can use AI to not just shelter its bottom line but also improve the effectiveness and accuracy of its fraud investigation department.

4. Findings

The literature and case study review support that AI, including machine learning, represents a major step change in healthcare fraud detection capability over traditional rule-based systems. Optum slashes avoidable admissions with ML models for chronic care programs, while certain private insurers (such as Optum or Cigna) and public channels (like Medicare) have both developed models that can adapt to recognize fraudulent patterns they're familiar with, as well as novel ones. Medicare contracts use both supervised and unsupervised learning to classify claims against historical data as well as detect new or different patterns (Rahman, 2025). This flexibility and adaptability underpin the need for a

scalable solution to counter the evolving, widespread nature of large healthcare fraudster rings that static systems are incapable of addressing (Van Duc, N. et al., 2024).

A second important result is that AI works best when it complements human expertise rather than substitutes for it. Both the Optum and Medicare FPS implementation approaches are great embodiments of a human-in-the-loop system. In this joint framework, AI serves as an intelligent controller assigning the service requests of high-risk claims needing investigation by humans for further review (Komperla, 2021). Not only does this mean that decisions are made as efficiently as possible, but it also maintains vital aspects of due process and ethical oversight that allow expert professionals to make the final decision. Combining Explainable AI (XAI) extends this model, giving detectives explicit reasons that alerts are generated via AI “agents” and building trust through collaboration (Zahid, I.A. et al., 2025).

Lastly, the results emphasize the need for a comprehensive perspective on data and analytics. The cases studied showed that the strongest AI approaches leverage multiple data sources and analytical methods. For example, Optum effectively incorporates NLP to analyze unstructured data in billing narratives, which gives a richer context for detecting fraud (Dey, R. et al., 2025). Cigna’s deployment of both supervised and unsupervised models demonstrates a proactive approach to keep up with fraudsters that become increasingly sophisticated (Das, S. et al., 2025). This proves that a successful AI solution is not based on a single model, but rather an ecosystem of technologies that can learn and adapt to changing fraudsters.

5. Discussion

The combined outcome of these aspects from this review is that healthcare fraud detection will experience a fundamental change with AI transforming the hoof-beating “pay-and-chase” model built on historical cases into proactive paradigms. The experience of the CMS Fraud Prevention System in preventing payment at submission demonstrates that real-time AI can save billions by detecting fraud before it occurs (Azad, T. et al., 2024). This strategic realignment has profound financial implications for public health programs and private insurers. By bolstering the health service, AI doesn’t just recover lost cash, but it helps make sure that we know where resources should be raining down for genuine patient care in everyone’s favor.

Even with the obvious benefits, we have identified some critical ethical and operational challenges that need to be resolved to enable responsible AI deployment. One of the largest concerns is that algorithmic bias could cause biased targeting of certain provider groups or patient populations (Ratwani, R.M. et al., 2024). The example of Cigna refusing to pay claims via an algorithm is a huge case in point to show the danger of using AI without human judgment. This incident highlights why strong governance is crucial and demonstrates that human-in-the-loop should never just be an efficient nicety, but a moral requirement to avoid bias and unforeseen harm.

In summary, the academic work itself and the real-world instances studied reveal a full picture of the duality of AI in healthcare fraud detection. It is a strong solution as well as a potential threat. The results reveal that while AI delivers unmatched analytics capability, this technology is only as valuable as the strategy it serves. A strategy that must be based on transparency, accountability, and ethical governance. As a result, future progress should not only strive for more accurate models, but also for stronger X-AI tools and ethical frameworks that inform decision-making in their judicious use. Only then can we guarantee that AI remains a net positive for society, as powerful as it gets, while preventing the risks from spiraling out of control.

6. Conclusion

Artificial intelligence (AI) is proving to be a disruptive technology in mitigating financial fraud in the U.S. healthcare market due to some weaknesses associated with rule-based and manual detection methods. Using machine learning, natural language processing, and predictive analytics, AI provides better accuracy, real-time detection, and efficiency to protect billions that would otherwise be lost to fraudulent scams. Both academic research and industry implementations demonstrate that AI can identify and adjust to changing patterns of fraud, while decreasing the rate of false positives and investigator burden. However, to fully realize the potential of AI, challenges such as data imbalance, model interpretability, and algorithmic bias need to be systematically tackled, along with ensuring compliant AI and dealing with regulations like the Health Insurance Portability and Accountability Act (HIPAA). That makes AI not a replacement but a vital supplement to human oversight, governance mechanisms, and other ethical safeguards. If deployed thoughtfully, AI can beef up financial integrity, restoring confidence that our healthcare resources are used for patients rather than as a playground for malfeasance.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

- [1] Ahmed, M., & Ahamad, M. (2014, September). Combating abuse of health data in the age of eHealth exchange. In *2014, IEEE International Conference on Healthcare Informatics* (pp. 109-118). IEEE.
- [2] Azad, T., & William, P. (2024). Fraud detection in healthcare billing and claims.
- [3] Aziz, L. A. R., & Andriansyah, Y. (2023). The role of 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.
- [4] Boda, V. V. R., & Allam, H. (2021). Automating Compliance in Healthcare: Tools and Techniques You Need. *International Journal of Emerging Trends in Computer Science and Information Technology*, 2(3), 38-48.
- [5] Cholevas, C., Angeli, E., Sereti, Z., Mavrikos, E., & Tsekouras, G. E. (2024). Anomaly detection in blockchain networks using unsupervised learning: A survey. *Algorithms*, 17(5), 201.
- [6] Couffinhal, A., & Frankowski, A. (2017). Wasting with intention: Fraud, abuse, corruption and other integrity violations in the health sector.
- [7] Das, S., & Bhat, A. K. (2024). Leveraging Artificial Intelligence for Early Fraud Detection in Insurance: Focusing on Intake and Claims Processing. *International Journal of Science and Research (IJSR)*, 13(11), 1121-1124.
- [8] Dey, R., Roy, A., Akter, J., Mishra, A., & Sarkar, M. (2025). AI-driven machine learning for fraud detection and risk management in US healthcare billing and insurance. *Journal of Computer Science and Technology Studies*, 7(1), 188-198.
- [9] Elumilade, O. O., Ogundeji, I. A., Achumie, G. O., Omokhoa, H. E., & Omowole, B. M. (2021). Enhancing fraud detection and forensic auditing through data-driven techniques for financial integrity and security. *Journal of Advanced Education and Sciences*, 1(2), 55-63.
- [10] Foglia, B. (2020). Mitigating Risk in Health Care through Mandatory Enterprise Risk Management Programs. *Loy. U. Chi. J. Reg. Compl.*, 5, 78.
- [11] Griffin, C. C. (2017). *The Challenges of Combating Healthcare Fraud* (Master's thesis, Utica College).
- [12] Hassija, V., Chamola, V., Mahapatra, A., Singal, A., Goel, D., Huang, K., ... & Hussain, A. (2024). Interpreting black-box models: a review on explainable artificial intelligence. *Cognitive Computation*, 16(1), 45-74.
- [13] Holzinger, A., Zatloukal, K., & Müller, H. (2025). Is human oversight to AI systems still possible?. *New Biotechnology*, 85, 59-62.
- [14] Ismaeil, M. K. A. (2024). Harnessing ai for next-generation financial fraud detection: A datadriven revolution. *Journal of Ecohumanism*, 3(7), 811-821.
- [15] Iweriebor, L. E. (2023). *Approach to Medicare Provider Fraud Detection and Prevention* (Doctoral dissertation, Capitol Technology University).
- [16] Karthik, K. P., Gupta, T. S., Kaushik, D., & Ramesh, T. K. (2025, January). Analysis of ML Models & Data Balancing Techniques for Medicare Fraud Using PySpark. In *2025 Fifth International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)* (pp. 1-6). IEEE.
- [17] Komperla, R. C. A. (2021). Ai-Enhanced Claims Processing: Streamlining Insurance Operations. *Journal of Research Administration*, 3(2), 95-106.
- [18] Luo, J., Wu, M., Gopukumar, D., & Zhao, Y. (2016). Big data application in biomedical research and health care: a literature review. *Biomedical informatics insights*, 8, BII-S31559.
- [19] Machireddy, J. R. (2022). Integrating predictive modeling with policy interventions to address fraud, waste, and abuse (fwa) in us healthcare systems. *Advances in Computational Systems, Algorithms, and Emerging Technologies*, 7(1), 35-65.

- [20] Mensah, G. B. (2023). Artificial intelligence and ethics: a comprehensive review of bias mitigation, transparency, and accountability in AI Systems. *Preprint, November, 10*(1), 1.
- [21] Mwangi, E. (2024). Employing ai/ml to determine and mitigate fraud in the insurance industry. *Available at SSRN 4907329*.
- [22] Pamulaparthivenkata, S., Chintale, P., Avacharmal, R., & Mulukuntla, S. (2020). LEVERAGING BIG DATA ANALYTICS FOR ENHANCED FRAUD DETECTION AND PAYMENT ACCURACY IN CMS OPERATIONS. *International Journal of Management (IJM)*, 11(9).
- [23] Rahman, M. M. (2025). DATA-DRIVEN GRAPH NEURAL NETWORK MODELS FOR DETECTING FRAUDULENT INSURANCE CLAIMS IN HEALTHCARE SYSTEMS. *American Journal of Interdisciplinary Studies*, 6(1), 263-294.
- [24] Ratwani, R. M., Sutton, K., & Galarraga, J. E. (2024). Addressing AI algorithmic bias in health care. *Jama*, 332(13), 1051-1052.
- [25] Reddy, S. (2024). Generative AI in healthcare: an implementation science informed translational path on application, integration and governance. *Implementation Science*, 19(1), 27.
- [26] Savitha, S., Keerthana, R., Logeswaran, K., Vennila, V., Manjuladevi, R., & Sangeetha, M. (2025). Sustainable AI-Powered Systems and Cybersecurity for Health Diagnostics: Addressing Bias and Fairness in AI for Early Disease Detection. In *AI-Driven Healthcare Cybersecurity and Privacy* (pp. 205-244). IGI Global Scientific Publishing.
- [27] Taha, K. (2025). Big Data Analytics in IoT, social media, NLP, and information security: trends, challenges, and applications. *Journal of Big Data*, 12(1), 1-91.
- [28] Timofeyev, Y., Hayes, S. A., & Jakovljevic, M. B. (2022). Predictors of loss due to pharmaceutical fraud: evidence from the US. *Cost Effectiveness and Resource Allocation*, 20(1), 6.
- [29] Trivedi, N. K., Simaiya, S., Lilhore, U. K., & Sharma, S. K. (2020). An efficient credit card fraud detection model based on machine learning methods. *International Journal of Advanced Science and Technology*, 29(5), 3414-3424.
- [30] Van Duc, N., Chau, T. T. M., Long, P. H., Nhung, L. T. C., Huy, B. Q., Bin, Z., & Yusof, A. F. B. H. (2024). Modernizing Taxation, Fraud Detection, and Revenue Management in Public Institutions Using AI-Driven Approaches.
- [31] Zahid, I. A., Garfan, S., Chyad, M. A., Albahri, A. S., Albahri, O. S., Alamoodi, A. H., ... & Alzubaidi, L. (2025). Explainability, Robustness, and Fairness in User-Centric Intelligent Systems: A Systematic Review. *IEEE Transactions on Emerging Topics in Computational Intelligence*.