Global Trends in Science and Technology

ISSN : 3079-5761
Volume 1, Number 1, January, 2025
https://doi.org/10.70445/gtst.1.1.2025.95-120

AI-Powered Anomaly Detection for AML Compliance in US Banking: Enhancing Accuracy and Reducing False Positives

Ashok Ghimire[1*]

[1]Westcliff University, USA

[1]ashok.ghimire1991@gmail.com

open access

Corresponding Author

Ashok Ghimire
ashok.ghimire1991@gmail.com

Article History:
Submitted: 21-01-2025
Accepted: 19-02-2025
Published: 25-02-2025

Keywords
AI powered AML, machine learning, deep learning, anomaly detection, fraud detection, risk scoring, Explainable AI (XAI).

ABSTRACT

AI detecting anomalies hasn't just been used to transform fraud detection for US banks, it's being used to reduce false positives. Current rule based systems create excessive alerts and it leads to inefficient costs and time. Machine learning, deep learning, and real-time analytics along with AI solve the problem with behavioral profiling, network analysis, and adaptive risk scoring to dramatically increase accuracy and efficiency. Explainable AI (XAI) still matters in order to maintain transparency and fairness, as per FinCEN and OCC. To comply with regulations, banks are coming up with regulatory sandboxes and AI governance frameworks. Crypto money laundering is becoming a growing issue as monitoring tools, such as block chain analytics and AI-driven crypto currency monitoring appear as the most effective way of tackling it. Real-time AI monitoring, predictive analytics, and federated learning for real collaboration without compromise to data privacy are also future trends of AML. With the integration of AI within regulatory compliant frameworks, US banks are able to improve the AML effectiveness, reduce costs and increase the financial security. In the banking world, AI powered AML solutions will transform the financial crime prevention, ensuring a more secure, efficient, and compliant banking system.

INTRODUCTION

The US banking system requires Anti-Money Laundering (AML) compliance as a major function that helps thwarting licit financial activities like: money laundering, terrorist fining and fraud. In the United States, the Bank Secrecy Act (BSA) of 1970 is considered as the starting point for the wide range of AML regulations; it mandates that the financial institutions put adequate measures in place to identify and report suspicious activities [1]. In the years since, more regulations like the USA PATRIOT Act (2001) and FinCEN's Customer Due Diligence (CDD) Rule (2018) have further reinforced banks' AML conditions, requiring banks to ramp up their monitoring systems and compliance programs. In reaction to these regulatory demands, banks have traditionally depended on a rule-based transaction monitoring systems to identify probable money laundering related transactions. Such systems work by applying predefined rules and thresholds and flag suspicious transaction for review by compliance teams [2]. However, rule based systems are plagued by some major draw backs such as very high false positive rates, man power inefficiencies and a lack of ability to detect sophisticated methods of money laundering. As criminals continue to evolve their tactics, these traditional methods are unable to keep up with the changing risks [3].

As a transformative technology, artificial intelligence (AI) has found its way in the AML domain, helping banks improve AML compliance with more accuracy and efficiency. Anomaly detection models driven by AI are based on ML and deep learning methodologies that allow aware amounts of transactional data and reveal hidden patterns in order to detect suspicious activities quicker and more effectively than rule-based platforms [4]. Overall, one of the main benefits of AI in AML Compliance is that they lower false positives while catching actual suspicious transactions. The algorithms of machine learning can work with historical data and keep updating their capabilities of detection to money laundering when new tactics are invented. Additionally, AI models can include behavioral analytics, network analysis and risk scoring to present a more comprehensive picture of customer activity and relationship [5].

In addition, AI powered AML solutions improve operational efficiency by automating the transaction monitoring process, offloading the work for human analysts and freeing up the compliance team to focus on cases that present a high risk. In addition, Natural language processing (NLP) techniques are used to further analyze unstructured data including regulatory filings, news reports and suspicious activity reports (SARs) to pick out emerging financial crime trends [6]. With US bank adoption of AI for AML compliance on the rise, there are regulatory, data privacy, and model interpretation challenges to deal with. More and more regulators like the Financial Crimes Enforcement Network (FinCEN) and the Office of the Comptroller of the Currency (OCC) are beginning to understand the possibility of AI and yet they always remind the importance of transparency, explain ability and comply with the compliance requirements [7].

CHALLENGES IN TRADITIONAL AML ANOMALY DETECTION

The issue that most plagues traditional AML (Anti Money Laundering) anomaly detection systems for US banking in particular is a high rate of false positives. However, the traditional AML systems solely rely on rule based methods where predefined thresholds or conditions trigger alarms to suspicious transactions. On the other hand, these rules have been used to a good extent to identify the known patterns of financial crime but have limited flexibility to adapt itself against this evolving technique of money laundering [8]. Therefore, because banks are deluged by a flood of false positive alerts, cases deemed suspicious that turn out to be legitimate, this proves to be a serious problem. According to industry reports, traditional AML systems can have false positive rates upwards of 95% which places an undue burden on operations teams. The manual review of flagged transactions is resource heavy for banks and ultimately increases the cost, inefficiencies and delays resulting in actual threats to be identified. Not only does this drain compliance budgets, but the time spent on non-money laundering risks reduces the ability to focus adequately on genuine money laundering risks [9].

Conversely, rule based systems are susceptible to missing complex money laundering activities, particularly those involving structured transaction, techniques of layering and movements across borders. Criminals always find new ways to launder their money through a variety of techniques to avoid detection, and they use any perceivable gaps in static rule based systems. This has traditionally made it difficult for banks to detect emerging threats in real time due to traditional models being unable to recognize complex transactional behaviors that differ from predefined patterns [10]. In the US, AML compliance is subject to very stringent regulatory environments that are also changing constantly. However, banks are required to conform to numerous regulatory requirements: the Bank Secrecy Act (BSA), USA PATRIOT Act, as well as the Financial Crimes Enforcement Network (FinCEN) guidelines. Also, institutions are required to implement international AML frameworks, e.g., those prescribed by the Financial Action Task Force (FATF) [11].

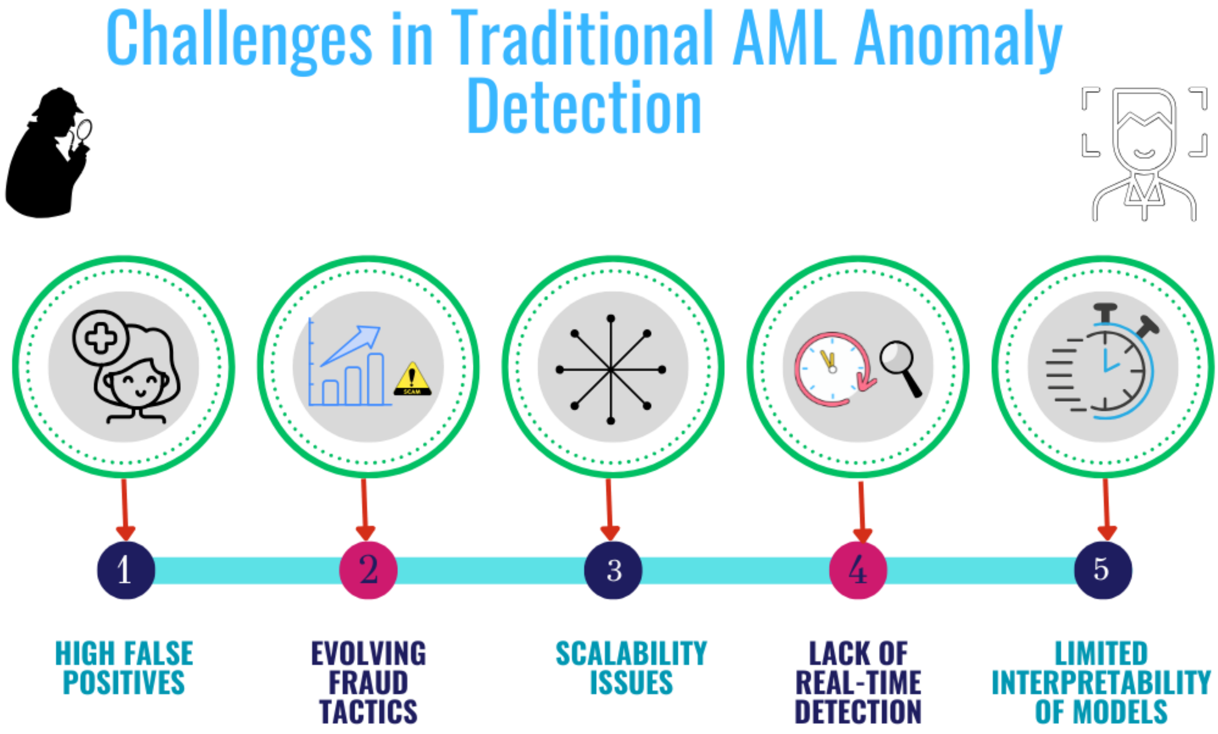
Challenges in Traditional AML Anomaly Detection
1
2
3
4
5
HIGH FALSE POSITIVES
EVOLVING FRAUD TACTICS
SCALABILITY ISSUES
LACK OF REAL-TIME DETECTION
LIMITED INTERPRETABILITY OF MODELS

Figure: 1 showing challenges in traditional AML anomaly detection

In the context of the financial sector, regulators mandate that financial institutions have sound AML programs in place, to conduct customer due diligence (CDD), to monitor transactions for suspicious activities, and to timely file Suspicious Activity Reports (SARs) when appropriate. Noncompliance can carries huge fines, reputational damage and legal consequences [12]. More than enough money has been set aside over the past decade as fines paid by US banks for AML violations, proving how important anomaly detection is. Yet, Compliance requirements typically add further burden on banks, so they must juggle between achieving the risk management and customer experience [13].

Monitoring more strictly can cause transaction delays finding unnecessary customer friction. Further, regulatory expectations with respect to explain ability and transparency in AML models make it cumbersome to deploy advanced AI driven solutions without clear explanation of its decisions [14]. Due to these challenges, banks are starting to look into AI powered AML solutions that can increase precision in detection, decrease false positives, and overall enhance AML compliance effectiveness. This section will explore how AI and machine learning models solve these issues with superior and adaptive anomaly detection in US banking [15].

AI-POWERED ANOMALY DETECTION MODELS

However, artificial intelligence (AI) has improved AML elimination by making use of complex anomaly detection designs that can look through huge datasets, spot dubious transfers, and cut back on false positives. In this regard, AI-based models can be divided into two category: supervised learning and unsupervised learning. The supervised learning models can be used on labeled datasets where historical transactions have been marked as suspicious or not [16]. In this way, these models learn patterns from past money laundering cases to predict future case's likelihood of being fraudulent. The common supervised learning algorithms utilized in AML include:

A collection of decision trees that improve the detection accuracy and lower the over fitting. It is Logistic Regression which gives the probability of a transaction being suspicious given few features like transaction size, frequency and customer profile. However, they work well with enough labeled data, but are ineffective when new money laundering techniques are found. Most of the models are trained on historical data, however criminals constantly evolve their tactics and a model trained on historical data may not be able to identify previously unseen fraud patterns [17]. On the other hand, the unsupervised learning models do not require labeled data. Instead they detect anomalies from unusual patterns that are present within the transactions and which differ from the norm [18]. They are very helpful in recognizing the new money laundering schemes that are growing. Common unsupervised techniques include:

Transactions are grouped according to their similar behaviors (ex. K means, DBSCAN) and flagged transactions that differ significantly. Neural networks that learn normal transaction patterns and call out deviations as possible problems are auto encoders. Anomaly: Detects anomalies by isolating transactions that do not conform to typical transaction's behavior [19]. Prior work illustrates that when selecting a model, unsupervised models do a better job at finding unknown types of money laundering than supervised models, while having more false positives. On the basis of the complexity, the AI powered AML detection models can further categorized from traditional machine learning models to the deep learning models [20].

Structured data (like transaction amounts, the locations, and time stamps) is scanned by machine learning models to search for unusual activities. The decision trees, support vector machines (SVM), and ensemble methods such as gradient boosting are included in these models. Because they are interpretable and can be fine-tuned to meet regulatory transparent requirements, they are widely used

[21]. Neural networks, and recurrent neural networks demonstrated on the datasets, have taken AML detection a step further by processing both structured and unstructured data. For instance, RNNs are good at finding suspicious sequence of transactions over time. In addition, Graph neural networks (GNNs) are being applied to AML detection because they can study relations between entities of a network and detect hidden financial crime networks [22].

CASE STUDIES OF AI IMPLEMENTATIONS IN US BANKS

It's not long before, several leading US banks have already put AI powered anomaly detection models into their AML compliance programs. Machine learning improves the detection accuracy of AML and reduces the number of false positives in AML transaction monitoring systems for instance JPMorgan Chase. To identify hidden relationships between high-risk entities, Wells Fargo has used AI based network analysis [23]. Deep learning techniques used by Citibank analyze high volume transactions in real time to give them a faster and more accurate risk assessment possible. US Banks can harness the power of AI powered models to make the AML compliance strong, track down the financial crimes more effectively and comply with the regulatory requirements while cutting down on the operational costs. We will then compare the different AI models that can be implemented for AML detection in the next section and will highlight their effectiveness alongside practices to ensure using the most suitable model in US banking [24].

Anti-Money Laundering (AML) compliance in US banking is facilitated by the use of AI to detect anomalies using anomaly detection models. The different AI models however, vary in accuracy, efficiency and adaptively. The comparison of these models assists financial institutions in identifying the most suitable approach for identifying suspicious activities which generates relatively less false positives. Broadly speaking, the type of AI models used within AML compliance can be defined in terms of machine learning (ML)-based models and deep learning-based models. Each one of them has its own merits and demerits [25]. Traditional AML systems based on Rule Based Models essentially base the detection of suspicious activity on predetermined rules like a transaction threshold or a relocation flag. They are both simple and interpretable, but produce high false positives and do not detect new ways of money laundering [26].

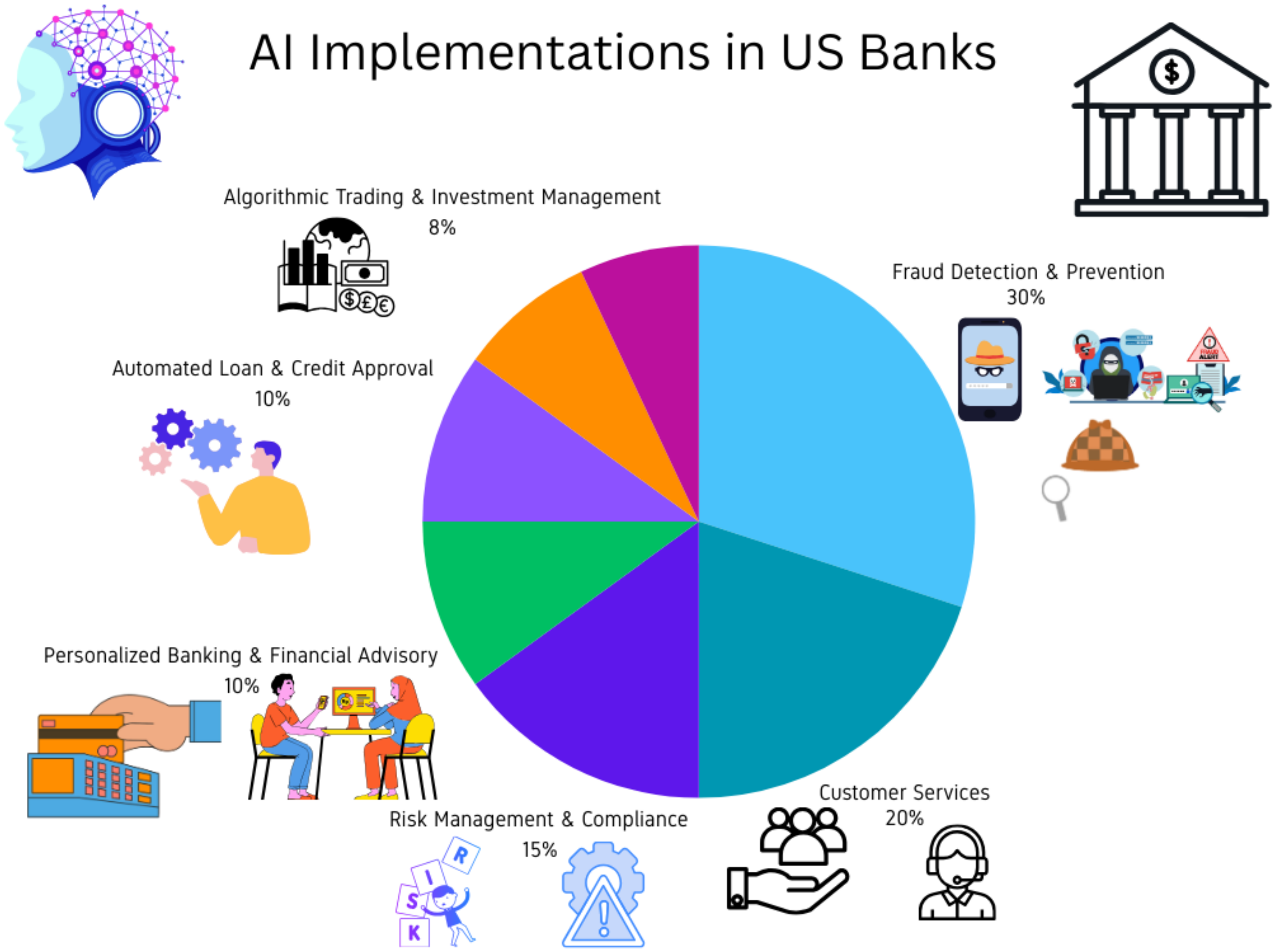

Figure: 2 showing AI implements in US banks

Rule Based Methods: Following rule based methods, AI models have the ability to learn something from historical data, adapt to new fraud patterns, and have more precise ways of detection to reduce false positives. Supervised Learning Models: These models take a labeled datasets (i.e., a dataset where you know that a certain transactions are fraudulent and other are legitimate), and use algorithms like, Decision Trees, Random Forest and Logistic regression. However, their reliance on past data does not offer them good utility to uncover new fraud techniques, but are instead useful for detecting known Money Laundering patterns [27].

Unsupervised Learning Models: Clustering models (K-Means, DBSCAN) and anomaly detection models (Isolation Forests, Autoencoders) are some examples of this type which do not require labeled data and are the most fit for picking unknown threats. They, however, tend to give rise to a more significant number of false positives that need further refinement [28].

US banks have greatly improved their money laundering activities detection with the help of Artificial Intelligence (AI). But to make full use of AI in Anti Money Laundering (AML) compliance, the models need to be improved using accurate data, real time monitoring and fair decision making. This section digs in on some key strategies to get the detection accuracy up in these AI enabled AML systems. Overall, the quality and diversity of the data used for training determines largely the accuracy of AI models [29]. Due to the evolving nature of money laundering tactics, the fact that these methods are adapted to the particularities of each country, and other privacy concerns, it is challenging for many financial institutions to obtain a high quality labeled dataset that was sourced with access to global financial crime data. In order to improve the performance of their model, banks should:

Use several sources of transaction data: Historical suspicious activity reports (SARs), deep learning models can also learn complex money laundering patterns when trained with multiple sources of transaction data. Clean and preprocess data for consistency and free from duplicates & errors: This ensures data integrity so that AI model built will be reliable [30].

Synthetic data: As labeled AML data is scarce, synthetic datasets can be leveraged that reflect real world transaction behaviors, and yet banks do not have to violate privacy law to create such data to train models [31].

Federate your learning: Financial institutions can use privacy preserving AI techniques including federated learning allowing banks to share insights without having to compromise sensitive data [32].

Real-Time Transaction Monitoring and Adaptive Learning: Batch processing for transactions takes place once they occur and become available in AML systems. Through AI, banks are able to monitor real time transactions which helps banks to detect suspicious activities in real time. Key approaches include: Real time analytics analysis of incoming transactions by AI models, identifying anomalies and taking immediate action including freezing funds for further review [33]. These are adaptive learning models: the AI systems learn from new data without using static rules and adjust fraud detection thresholds and hone their accuracy as emerging fraud patterns unfold. It aligns with behavioral profiling in that it monitors customer transaction behaviors over time to detect deviations. Alerts could include wire transfers to offshore accounts that suddenly spike in high value. Real time monitoring helps banks respond quickly to financial criminals and stop illicit fund movements before they gain traction [34].

Removes Bias and Improves Explain ability of the model. Despite the improvement potential of AI in AML compliance, there are potentially troubling aspects of bias and model interpretability. Financial institutions thus need to explain how AI makes decisions, to regulate how fair and how nondiscriminatory they are [35]. To address these challenges:

Bias detection and mitigation: Any impacts of bias on the transaction monitoring as an AI model must be audited and corrected to prevent a certain customer segments from getting unduly flagged as high-risk. Explainable AI (XAI) using interpretable machine learning techniques (e.g. SHAP (SHapley Additive Explanations)) enables banks to explain how AI models classify transactions and justify decisions [36].

Human-AI collaboration: Rather than auto detecting AML, AI should assist human analysts with both highlighting insights as well as presenting the ultimate decision on high risk cases for the compliance teams. Removing bias from and increasing transparency of AI powered AML systems will earn greater regulatory acceptance and increase trust in its users from other financial institutions and both businesses and consumers [37]. Detection accuracy in AI-powered AML systems better improves if you bring in high quality data, real time monitoring and fairness in the decision making. To reap the benefits of AI for AML detection as well as comply, reduce financial crime risks and retain regulatory trust, the best path for US banks is to implement these best practices [38].

REGULATORY CONSIDERATIONS FOR AI IN US BANKING

US banks operating in an anti-money laundering (AML) compliance space have to grapple with an intricate regulatory environment when employing AI powered solutions for AML compliance so as to maintain compliance with existing laws and be transparent about their AI processes. While AI presents an opportunity to improve both AML detection accuracy and the operational efficiency, fairness, explain ability, and strict adherence to rigorous compliance requirements are not negotiable [39]. Requires financial institutions to develop AML programs, record keeping of all transactions and filing of Suspicious Activity Reports (SARs) when required by the Bank Secrecy Act (BSA) of 1970. These compliance efforts need to be supported by AI models that can correctly identify and report illegal activities [40].

ISSN : 3079-5761
Volume 1, Number 1, January, 2025
https://doi.org/10.70445/gtst.1.1.2025.95-120

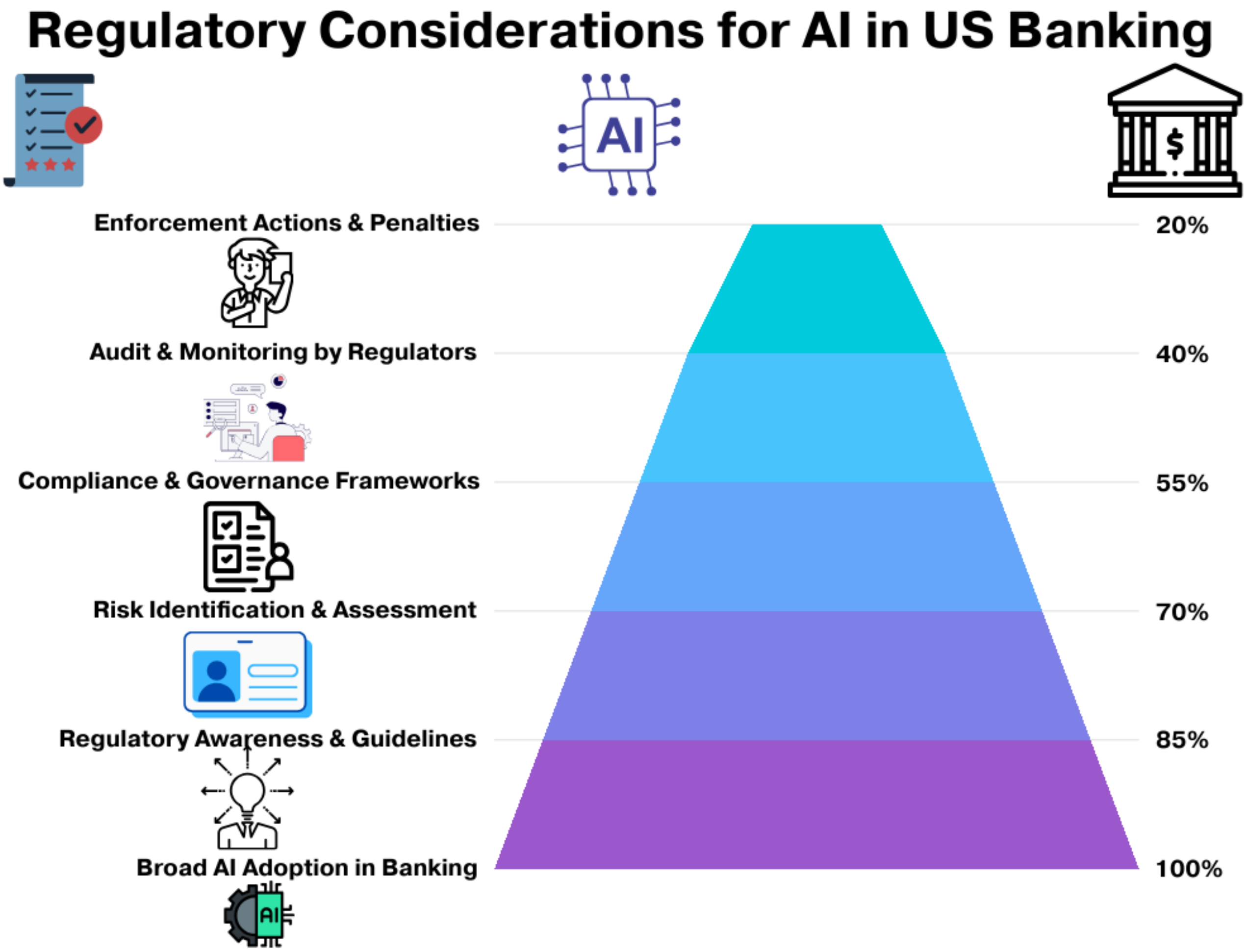

Figure: 3 showing regulatory considerations for AI in US banking

USA PATRIOT Act (2001): Is a strengthening of the AML enforcement through the requirement of the enhanced due diligence (EDD) of high-risk customers and transactions. And by automating risk assessment and finding anomalies in customer behavior, AI can assist banks with addressing these issues. The Financial Crimes Enforcement Network (FinCEN), a bureau of the US Department of the Treasury, themselves are the ones that set AML standards and ensure adherence [41]. In 2021, FinCEN published an Advanced Notice of Proposed Rulemaking (ANPR) stating that AI and machine learning have the potential to advance financial crime detection but acknowledging the importance of being able to explain and hold the systems accountable [42].

Office of the Comptroller of the Currency (OCC) and Federal Reserve Guidelines: These equivalent regulatory organizations regulate monetary institutions and need banks to verify that AI controlled AML programs meet the same compliance criteria and work fairly without unduly introducing risk. But US regulators praise AI's potential in AML compliance so long as decisions made based on them are interpretable, auditable and bias free. Regulators want model decision to be documented and flagged in transactions to be clearly justified to banks [43]. AML systems that utilize artificial intelligence must be run in an ethical and transparent manner so as not to lead to unintended biases or unfair treatment of the firm's customers. Key ethical concerns include: With Bias and Fairness, AI models must be trained on large datasets of diverse data to avoid adverse outcomes. An AI system that flags higher risk for some demographics or geographies may also lead to financial exclusion and compliance violations. Fairness audits should be applied by banks to discover and curtail bias [44].

Explain ability and Model Interpretability: The need for AI-driven AML systems to be explainable has been demanded by the regulators, for example, this also translates into 'model interpretability', i.e, it should be clearly comprehensible how each transaction monitoring decision was derived [45]. We also take a look at Explainable AI (XAI) techniques (SHapley Additive Explanations (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME)) that assist compliance teams and regulators to understand the way the AI generated risk assessment. While AI contributes in detecting AML, this element should not work independently. Hence, banks must retain HITL models, where the compliance team is to check AI generated alerts and decide upon suspicious transactions [46].

CHALLENGES IN AI ADOPTION FOR AML COMPLIANCE

However, there are a few hurdles that remain before AI can achieve its potential in AML compliance.

Regulatory Uncertainty: There is a fair bit of ongoing uncertainty around AI in banking and hence the regulatory frameworks lack standardized guidelines to regulate AI AML models. It's the nature of banks, they must always keep up with regulatory expectations as new ones emerge [47].

Model Validation and Testing: Financial institutions are mandated by regulators to validate the AI models, to run the tests with actual data and to ensure that it meets benchmarks to be in compliance. Periodic audits of AI models need to confirm their reliability and accuracy [48].

Privacy and Data Security: AI models use massive amounts of transactional data and how to protect users' data. When it comes to using AI in AML monitoring for banks, they must comply with data protection laws like Gramm-Leach-Bliley (GLBA) and ensure that they are secure when handling customer information [49].

The Path Forward: Aligning AI with Regulatory Expectations: Financial institutions should leverage AI for AML provided they adhere to the US banking regulations.

Develop Transparent AI Frameworks: Create the governance framework, which shapes how the AI models function, document their decision makings in the process, then make sure these frameworks comply with existing standards and regulations relevant to it. Banks should engage with regulators, such as FinCEN and the OCC, to work with them on AI policies and show that they are responsible adopters of AI. Instead of replacing traditional rule-based systems, banks should employ hybrid AML models that incorporate AI and significantly improve the systems by optimizing over thousands of potential user patterns and identifying network outliers [50]. US banks have an opportunity to improve fraud detection and efficiency of compliance with AI powered AML solutions. This is why regulatory adherence is necessary to maintain fairness, transparency and accountability of the AI driven AML systems. Financial institutions can improve AML compliance by aligning AI adoption with BSA and FinCEN requirements, and avoid regulatory risks and ethical issues related to AI implementation [51].

REDUCE FALSE POSITIVES IN AI POWERED AML SYSTEMS

In the US banking industry, one of the biggest challenges in AI based Anti-Money Laundering (AML) systems is their annoying tendency to generate high levels of false positives, or, in other words, it flags legit transactions as suspicious. A heavy operational burden is created for banks due to false positives in terms of both the cost to the bank and its compliance teams, which, in turn, slows investigations and potentially decreases customer satisfaction. To further improve AML compliance efficiency, it is critical to reduce false positive while maintaining high accuracy of detection [52].

Why Do False Positives Occur in AML Systems?

Currently, traditional AML detection systems are in fact based on rule-based approaches which will cause alerts when predefined conditions are take place. However, these systems are not adaptable and hence cause too many false positives. Just to be sure even AI AML models can give you false positives on:

Rigid: Many AML models still contain rigid transaction monitoring rules such as all transactions over $10,000 will be flagged regardless of normal behavior of the customer [53].

ISSN : 3079-5761
Volume 1, Number 1, January, 2025
https://doi.org/10.70445/gtst.1.1.2025.95-120

Contextual Understanding Deficit: In many at risk industries (e.g., real estate, trade, etc.), AI models often struggle to distinguish between highly suspicious transactions and, quite valid, high-value transactions. Poorly labeled training data, biased datasets, missing information, all these data quality issues can misclassify transactions by AI models [54].

Unsupervised Models Limitations: What unsupervised models know is that it it's not normal would typically be an anomaly, but not all anomalies are fraudulent. Perhaps a new business moving excessive wire transfers will be flagged since they do not act as expected. Banks must bring to bear advanced AI techniques and intelligent filtering techniques to minimize False Positives, to improve AML's efficiency [55].

STRATEGIES TO REDUCE FALSE POSITIVES IN AI-DRIVEN AML SYSTEMS

Behavioral Profiling: Customer transactional behaviors should be assessed across time by AI models so that normal variations for customer behaviors can be separated from actual suspicious behaviors. AI can reduce unnecessary alerts by linking accounts and entities within different transactions for linking of true criminal networks [56].

Data Enrichment: Both external data iteration (adverse media reports, company ownership registries, and relocation data) provides AI models with better information for decision making [57].

Hybrid AI-Rule-Based Approaches: Banks can instead implement hybrid models that blend the addictiveness of AI with human defined risk rules to replace traditional rule based AML systems only in part, rather than in full some cases. Besides, due to the capabilities of the AI models, they are able to prioritize the most critical alerts while filtering or sending through further analysis the other, lower risk alerts. This transparency provides regulators and compliance teams with needed transparency into AI decision making [58].

SHAP (SHapley Additive Explanations) and LIME (Local Interpretable Model-Agnostic Explanations) are two Explainable AI techniques to help banks understand why the transaction was flagged and to avoid additional reviews. Avonex is an IFN beta-1a, 30 microgram (mcg) dose, administered weekly by subcutaneous injection (under the skin; see the Spinal Medication page for more information) [59]. The recommended dosage of Rebif is 44 mcg, 22 mcg, or 8.8 mcg Intramuscular injection (into the muscle) taken three times a week. It can also be administered subcutaneously by injection under the skin.

ISSN : 3079-5761
Volume 1, Number 1, January, 2025
https://doi.org/10.70445/gtst.1.1.2025.95-120

Machine learning for risk scoring and adaptive thresholds: Risk levels are adjusted by AI driven risk based scoring systems based on customer profile, historical transaction and real time customer behavior. Rather than specifying a fixed threshold on every transaction, AI models allow the system to adapt thresholds based on changing risk factors. AI models capable of self-learning can fine tune the threshold over time, tend to reduce the number of false alerts and can also improve with detection accuracy [60].

Human-in-the-Loop (HITL) Model for Alert Validation: Yet, AI boosts AML detection greatly and compliance teams should still be engaged in making sure whether flagged transactions are genuine or not. The AI models benefit from human analysts providing feedback to eventually become even more accurate and avoid unnecessary escalations [61].

BENEFITS OF REDUCING FALSE POSITIVES IN AML COMPLIANCE

False Positives: Bank compliance professionals are able to direct resources to real risk rather than to reviewing excessive alerts by decreasing the amount of false positives. Lower false positive rates cut down on manual reviews and help lower AML compliance costs, as well as improve an investigator's workflow [62].

AI Also Improves Better Customer Experience: AI Driven Improvements prevent good customers from having to endure unwarranted delays or account freezes because of the wrong false AML alerts [63].

ML Based AML: It helps banks comply with regulatory requirements more effectively and avoid being overwhelmed by no actionable alerts. False positives are key in limiting the AI-powered AML systems, thereby allowing for better compliance efficiency and productivity, less operational costs, and restoring customer trust. US banks, by adopting context aware AI models, risk based scoring, explainable AI, hybrid rule AI, and the combination of all of the three, can vastly improve AML detection without flooding their staff with unnecessary alerts [64]. The implementation of these strategies results in smarter and effective AML compliance framework which complies with regulatory requirements and enhances financial crime prevention.

FUTURE TRENDS IN AI FOR AML COMPLIANCE IN US BANKING

However, with financial crimes becoming more developed, using AI in Anti – Money Laundering (AML) compliance in US banking will be driven by the emergence of new technologies, changes of the regulatory requirements and rising cooperation between financial institutions and regulatory authorities. We expect AI to play more important role in AML, making compliance systems more efficient, adaptive and proactive to catching financial crime. This section discusses the major trends that would transform the AI landscape for AML [65]. Traditional machine learning models have improved, but advanced AI techniques like the following will be used in the future to detect AML activity.

Deep Neural Networks (DL): Less financial institutions and banks will implement deep neural networks to scan for intricate money laundering patterns, a possibility that Rule based or simple machine learning models might not be effective to do. Graph Neural Networks (GNNs), therefore, are a good fit for graph mapping and analysis (e.g. transaction networks), are able to discover hidden links between seemingly independent accounts, and can identify complex money laundering schemes [66].

AI will enable NLP (Natural Language Processing) to go through enormous volumes of unstructured data (news articles, regulatory filings, legal documents) to uncover the financial crime risks, as well as to improvise adverse media screening, regulatory report analysis and KYC verification. Deep learning and hybrid AI models will advance AML detection accuracy and greatly reduce false positives; a significant compliance issue for compliance teams [67].

REAL-TIME AML MONITORING WITH AI AND BIG DATA ANALYTICS

Real time transaction monitoring is the future of AML compliance where banks can detect such activities on real time base instead of after the fact.

AI Driven AML Systems: With the help of AI, such systems will be able to integrate data from various sources, including various sources like transaction records, customer interactions, social media, and blockchain networks, in order to get a more holistic view of such suspicious activities. Banks will use cloud AI models to enable processing of large transaction volumes in an efficient and scalable manner with a security guarantee [68]. Rather, than just flagging fraudulent transactions, AI models will tell high risky behavior before it happens creating the opportunity for proactive AML

ISSN : 3079-5761
Volume 1, Number 1, January, 2025
https://doi.org/10.70445/gtst.1.1.2025.95-120

actions. Banks can improve fraud prevention and agility of compliance by integrating AI with real time data streams.

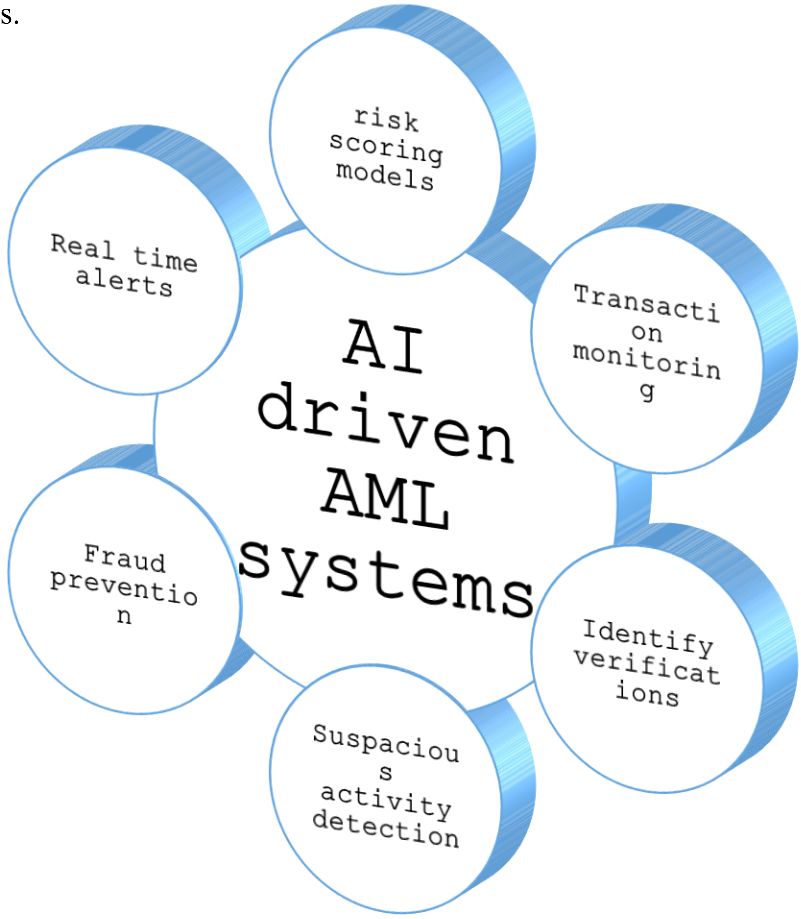

Figure: 4 showing AI driven AML systems

Explainable AI (XAI) for Regulatory Compliance: FinCEN (Financial Crimes Enforcement Network) and the OCC (Office of the Comptroller of the Currency) need to have transparency in AI decision making. The Explainable AI (XAI) will become the future AML compliance as it will make regulatory acceptance possible and avoid black box AI issues. Financial institutions and regulators partner to 'sandbox' AI models in protected environments to ensure these work within existing compliance standards before full deployment [69]. Banks will implement an AI governance framework to regularly audit their deployed AI models for fairness, accuracy and compliance with legal requirements. The AI algorithms will be designed in such a way that there will be built in interpretability, and compliance teams will know why those particular transactions are classified as suspicious. Because AI AML systems would be approved on the basis of explain ability and regulatory compliance, the adoption of explainable and regulatory compliant AI will be a key focus for the banks [70].

ISSN : 3079-5761
Volume 1, Number 1, January, 2025
https://doi.org/10.70445/gtst.1.1.2025.95-120

AI and Block chain for Anti-Money Laundering: As crypto currency and the notion of decentralized finance (DeFi) grow, so do criminal plans for laundering money. Block chain analytics is one way AI combined with block chain analytics will play a crucial role in monitoring illicit crypto transactions. AI models will check anomalous block chain transaction patterns, illicit addresses, and crypto currency mixing services utilized in money laundering. Future banking regulations might mandate crypto financial institutions to build in AI driven smart contracts that will automatically flag and freeze suspicious crypto transactions [71]. AI will improve global AML collaboration with banks and regulators as the criminal movement of illicit funds can be tracked in real time across multiple jurisdictions. A strong enforcement of AML in digital finance can be derived from AI driven block chain analytics to address emerging threats from crypto-based money laundering schemes [72].

AI-Driven Collaboration between Banks and Regulators: The AML compliance is switching to a smarter, collaborative approach where banks share, law enforcement and regulators share further AI added insights to fight against financial crimes better. Banks will use Federated Learning as a technique to train AI models over shared financial crime data without exposure of sensitive customer data [73].

Regulatory AI Frameworks: AI will be used for compliance in conjunction with regulatory databases (such as FinCEN's BSA E-Filing System) to automate and improve the accuracy of SAR (Suspicious Activity Report) filings as well as regulatory reporting. AI enabled cross border data sharing will boost AML efforts in which banks can leverage AI to detect and block money launderers operating in multiple jurisdictions efficiently [74]. This too will lead to enhanced AI driven collaboration which collectively will make for a more unified, real time way to conduct AML compliance with benefits for financial institutions and also the regulators. Deep learning techniques, real time watch lists, explainable AI, analytics of block chain and cross company collaboration will all play a role in the future of AI powered AML compliance in US banking.

CONCLUSION

Anti-Money laundering (AML) compliance is shifting gears in the realms of US banks as AI powered anomaly detection models are integrated into the current detection strategy. With the ever evolving threats on the financial sector posed by sophisticated money laundering schemes, AI presents a better, faster, and scalable solution to detecting these illicit activities. Banks can enhance their AML frameworks, raise detection accuracy and greatly cut down on false positives, which have been a long time challenge for compliance teams, by enabling machine learning, deep learning, and real time analytics.

AI in AML has one of the most crucial benefits which is its capacity to examine extreme amounts of transactions in real time and recognize suspicious transactions that are frequently missed by traditional rule-based systems. With behavioral profiling, network analysis and risk based scoring, AI system can differentiate between legitimate transactions and those relating to financial crimes. This assists compliance teams to not be swamped by unneeded false alerts and focus on more dangerous cases. Furthermore, graph neural networks (GNNs) and natural language processing (NLP) are enabling hidden links between entities to be revealed and risks identified on unstructured data such as news reports and regulatory filings.

While these advancements, regulatory compliance is still the critical factor for AI adoption in AML. Fintrics is well aware that AI models need to be explainable, auditable, fair — as US regulators such as FinCEN, the Office of the Comptroller of the Currency, and the Federal Reserve, for example, advice, emphasizing that technology alone is not the solution. Banks, therefore, should incorporate the Explainable AI (XAI) techniques to bring their explanations of flagged transactions in line with these requirements. Regulatory sandboxes are also being formed where financial institution get to test AI model sandboxes before full scale implementation. The integration of block chain analytics into AI models will be one more important trend in the future of AI in AML compliance. AI powered block chain monitoring tools are becoming necessary for tracking illicit transactions in terms of crypto currency and decentralized finance (DeFi) platforms as they bring about new money laundering risks. Through analyzing on-chain data, the wallets, and the transaction flows, the banks and regulators can use the help from the AI in order to prevent crypto based financial crimes better than anyone can manage.

From there on, the future of AI in AML compliance will depend on collaboration, regulatory alignment and constant innovation. For sharing information in a secure and privacy preserving manner, financial institutions, regulators, and law enforcement agencies need to construct secure and private AI frameworks that would help in all possible operations such as training, testing, evaluation, and storage. One promising approach is for banks to train AI models on shared financial crime data through what’s known as federated learning, in which banks train their own models from their own data in a way that does not expose sensitive information about their customers. US Banking has another major force in the fight against financial crime in the form of AI powered AML solutions?

Through harnessing of innovative AI technologies, improving model transparency and abiding by regulatory protocols, banks can actively improve their AML compliance framework, lower operational expenses and ultimately construct a more secure and robust financial system. Although there are still issues in using AI, strategic utilization of AI will keep shaping the AML compliance world, keeping financial institutions ahead in a dynamic financial playground.

REFERENCES

[1]. Zhang W, Chen L. Real-Time Transaction Monitoring Using AI: Detecting Suspicious Activities and Money Laundering in Banking. Asian American Research Letters Journal. 2024 Apr 28; 1(3).

[2]. Koduru L. Driving Business Success through AI-Driven Fraud Detection Innovations in AML and Risk Monitoring Systems. InDriving Business Success through Eco-Friendly Strategies 2025 (pp. 115-130). IGI Global Scientific Publishing.

[3]. Shan W. AI-powered fraud detection in banking: innovations, challenges and preventive strategies (Doctoral dissertation).

[4]. AI in Fraud Prevention: Techniques, Challenges, and Future Opportunities. (2024, September 26). Indika AI. Retrieved from https://www.indikaai.com/blog/ai-infraud-prevention-techniques-challenges-and-future-opportunities

[5]. AI in the banking sector: How fraud detection with AI is making banking safer. (n.d.). Infosys Bpm. Retrieved from https://www.infosysbpm.com/blogs/bpmanalytics/fraud-detection-with-ai-in-banking-sector.html

[6]. Artificial intelligence: Uses and associated risks in federally regulated financial institutions. (2023). Office of the Superintendent of Financial Institutions. Retrieved from https://www.osfi-bsif.gc.ca/en/about-osfi/reportspublications/osfi-fcac-risk-report-ai-uses-risks-federally-regulated-financialinstitutions

[7]. Buehler, K., Corsi, A., Weintraub, B., Jurisic, M., Siani, A., & Lerner, L. (2024, March 22). Scaling gen AI in banking: Choosing the best operating model. McKinsey & Company. Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/scaling-genai-in-banking-choosing-the-best-operating-model

[8]. Singh VB, Singh P, Guha SK, Shah AI, Samdani A, Nomani MZ, Tiwari M. The Future of Financial Crime Prevention and Cybersecurity with Distributed Systems and Computing Approaches. Meta Heuristic Algorithms for Advanced Distributed Systems. 2024 Apr 2:321-40

[9]. Kasowaki L, Alp K. Threat Intelligence: Understanding and Mitigating Cyber Risks. EasyChair; 2024 Jan 6.

[10]. Gnatyuk S, Berdibayev R, Aleksander M, Sydorenko V, Zhyharevych O, Polozhentsev A. Software System for Cybersecurity Events Correlation and Incident Management in Critical Infrastructure. InData-Centric Business and Applications: Advancements in Information and Knowledge Management, Volume 1 2024 Aug 8 (pp. 247- 269). Cham: Springer Nature Switzerland.

[11]. Malik AW, Bhatti DS, Park TJ, Ishtiaq HU, Ryou JC, Kim KI. Cloud digital forensics: Beyond tools, techniques, and challenges. Sensors. 2024 Jan 10; 24(2):433.

[12]. Sania NS, Gigras Y, Mahajan S. Gatividhi Guard: The Activity Guardian—Revolutionizing Security Information and Event Management (SIEM) Technology. Journal of Operating Systems Development & Trends. 2024;11(1):29- 44p

[13]. Oyeniyi LD, Ugochukwu CE, Mhlongo NZ. Developing cybersecurity frameworks for financial institutions: A comprehensive review and best practices. Computer Science & IT Research Journal. 2024 Apr 17; 5(4):903-25.

[14]. Olaiya OP, Adesoga TO, Ojo A, Olagunju OD, Ajayi OO, Adebayo YO. Cybersecurity strategies in fintech: safeguarding financial data and assets. GSC Advanced Research and Reviews. 2024; 20(1):050-6.

[15]. Oduri S. Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era. International Journal of Innovative Research in Science Engineering and Technology. 2024; 13:13632-40.

[16]. Oduri S. Continuous Authentication and Behavioral Biometrics: Enhancing Cybersecurity in the Digital Era. International Journal of Innovative Research in Science Engineering and Technology. 2024; 13:13632-40.

[17]. Mohanty RK, Kumar AP, Padmaja R, Prashanthi V. Deep Learning for Analyzing User and Entity Behaviors: Techniques and Applications. InConsumer and Organizational Behavior in the Age of AI 2024 (pp. 219-250). IGI Global.

[18]. Udeh EO, Amajuoyi P, Adeusi KB, Scott AO. Blockchain-driven communication in banking: Enhancing transparency and trust with distributed ledger technology. Finance & Accounting Research Journal. 2024 Jun 6; 6(6):851-67.

[19]. Kumar B, Malaviya MP, Dhodhiawala Z, Hafeez SA, Murala DK. Financial Fraud Detection and Prevention Using Blockchain and Integration of Hyperledger. IUP Journal of Computer Sciences. 2024 Oct 1; 18(4).

[20]. Ogbu AD, Iwe KA, Ozowe W, Ikevuje AH. Geostatistical concepts for regional pore pressure mapping and prediction. Global Journal of Engineering and Technology Advances. 2024; 20(01):105-17.

[21]. Althati C, Tomar M, Shanmugam L. Enhancing Data Integration and Management: The Role of AI and Machine Learning in Modern Data Platforms. Journal of Artificial Intelligence General Science (JAIGS) ISSN: 3006-4023. 2024 Feb 22; 2(1):220-32

[22]. Adeniran IA, Efunniyi CP, Osundare OS, Abhulimen AO. Enhancing security and risk management with predictive analytics: A proactive approach. International Journal of Management & Entrepreneurship Research. 2024; 6(8).

[23]. Safdar, N. M., Banja, J. D., & Meltzer, C. C. (2020). Ethical considerations in artificial intelligence. *European Journal of Radiology, 122*, 108768. https://doi.org/10.1016/j.ejrad.2019.108768

[24]. AI-Driven Fraud Detection in the U.S. Financial Sector: Enhancing Security and Trust. (2023). International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence, 14(1), 775-797. https://ijmlrcai.com/index.php/Journal/article/view/242

[25]. Martinez, P., et al. (2013). "NLP Integration in AML Compliance Systems." Journal of Financial Crime Prevention, 7(1), 55-68.

[26]. Venkata Manoj Tatikonda, Kamala Venigandla and Navya Vemuri. “Transforming customer banking experiences: Ai-Driven RPA for Customized Service Delivery,” International Journal of Development Research, 12, (11), 60674-60677.

[27]. Khan, H. U., Malik, M. Z., & Nazir, S. (2024). Identifying the AI-based solutions proposed for restricting Money Laundering in Financial Sectors: Systematic Mapping. Applied Artificial Intelligence, 38(1). https://doi.org/10.1080/08839514.2024.2344415

[28]. Zhang, Wei, and Lan Chen. "Real-Time Transaction Monitoring Using AI: Detecting Suspicious Activities and Money Laundering in Banking." Asian American Research Letters Journal 1.3 (2024).

[29]. D. Dhabliya, S. Saxena, J. Ratna Raja Kumar, D. Kumar Pandey, N. V. Balaji and X. M. Raajini, "Exposing the Financial Impact of AI-Driven Data Analytics: A Cost-Benefit Analysis," 2024 2nd World Conference on Communication & Computing (WCONF), RAIPUR, India, 2024, pp. 1-7, doi: 10.1109/WCONF61366.2024.10692261.

[30]. L. F. Pau, "Artificial intelligence and financial services," in IEEE Transactions on Knowledge and Data Engineering, vol. 3, no. 2, pp. 137-148, June 1991, doi: 10.1109/69.87994.

ISSN : 3079-5761
Volume 1, Number 1, January, 2025
https://doi.org/10.70445/gtst.1.1.2025.95-120

[31]. Nesterov, Vasyl. "Integration of artificial intelligence technologies in data engineering: Challenges and prospects in the modern information environment." Вісник Черкаського державного технологічного університету. Технічні науки 28.4 (2023): 82-90.

[32]. Al-Shabandar, R., Lightbody, G., Browne, F., Liu, J., Wang, H., & Zheng, H. (2019, October). The application of artificial intelligence in financial compliance management. In Proceedings of the 2019 International Conference on Artificial Intelligence and Advanced Manufacturing (pp. 1-6).

[33]. Villar, Alice Saldanha, and Nawaz Khan. "Robotic process automation in banking industry: a case study on Deutsche Bank." Journal of Banking and Financial Technology 5.1 (2021): 71-86

[34]. Gupta, Abhishek, Dwijendra Nath Dwivedi, and Jigar Shah. "Artificial intelligence-driven effective financial transaction monitoring." Artificial Intelligence Applications in Banking and Financial Services: Anti Money Laundering and Compliance. Singapore: Springer Nature

[35]. Rane, Nitin, Saurabh Choudhary, and Jayesh Rane. "Blockchain and Artificial Intelligence (AI) integration for revolutionizing security and transparency in finance." Available at SSRN 4644253 (2023).

[36]. Villar, A. S., & Khan, N. (2021). Robotic process automation in the banking industry: a case study on Deutsche Bank. Journal of Banking and Financial Technology, 5(1), 71-86.

[37]. Wang, Qianyu, Wei-Tek Tsai, and Tianyu Shi. "GraphALM: Active Learning for Detecting Money Laundering Transactions on Blockchain Networks." IEEE Network (2024).

[38]. Adams, B.E (2024). Cybersecurity for Environmental Sustainability: The Role of Cybersecurity on Decentralized Renewable Energy Systems (Off-grid and Microgrid). Journal of Emerging Trends in Engineering and Applied Sciences, 15(3), 100-115

[39]. Brenig, C., Schwarz, J., & Rückeshäuser, N. (2016). Privacy-preserving cryptocurrencies: Challenges and solutions. Journal of Economic Perspectives, 30(3), 65-90. (Details missing; please verify and provide full citation)

[40]. Chen, X., Zhang, Y., & Liu, W. (2021). Machine learning in financial fraud detection: An overview. Artificial Intelligence Review, 54(1), 29-60. (Details missing; please verify and provide full citation)

[41]. Dalsaniya A, Patel K, Swaminarayan PR. Challenges and opportunities: Implementing RPA and AI in fraud detection in the banking sector.

[42]. Gartner. (2021). Gartner identifies top security and risk management trends for 2021. Gartner. Goldshteyn, G. & Tierney, S. (2024) What Is a Bank? Available at: https://www.nerdwallet.com/article/banking/what-is-a-bank

[43]. Hull, J. C. (2012). Risk management and financial institutions. John Wiley & Sons. Hull, J. C. (2018). Risk management and financial institutions (5th Ed.).

[44]. John Wiley & Sons. Kashyap, A. K., Rajan, R. G., & Stein, J. C. (2020). Banks as liquidity providers: An explanation for the coexistence of lending and deposit-taking. Journal of Finance, 57(1), 33-73.

[45]. Kenton, W. (2023). Risk Control: What It Is, How It Works, Example. Available at: https://www.investopedia.com/terms/r/risk-control.asp

[46]. Kindleberger, C. P., & Aliber, R. Z. (2011). Manias, panics and crashes: A history of financial crises. Palgrave Macmillan.

[47]. Knapp, E. D., & Langill, J. T. (2015). Chapter 8-risk and vulnerability assessments. Industrial Network Security (Second Edition), edited by Eric D. KnappJoel Thomas Langill, Syngress, Boston, 209- 260.

[48]. Kou, G., Peng, Y., & Wang, G. (2014). Evaluation of classification algorithms using MCDM and rank correlation. International Journal of Information Technology & Decision Making, 13(01), 197-225. Li, J., & Tong, S. (2018). The determinants of cross-border M&A success. Journal of Corporate Finance, 50, 111-132.

[49]. Majaski, C. (2023). Retail Banking vs. Corporate Banking: What's the Difference? Available at: https://www.investopedia.com/articles/general/071213/retail-banking-vs-commercial-banking.asp

[50]. Peddada, K. (2013). Risk Assessment and Control. A paper presented at the International conference "Governance & Control in Finance & Banking: A New Paradigm for Risk & Performance" in Paris, France, on April 18-19, 2013.

[51]. Rajagopal, P., & Venkatraman, V. (2020). Private Banks in India: Evolution and Prospects. Journal of Banking & Finance, 29(1), 76-84

[52]. Udo-Okon, T. N. and Akpan, E. E. (2024). The Challenges of Artificial Intelligence in Library Management System. Intercontinental Academic Journal of Library and Information Science, 6(1), 96-107

[53]. Maree, C., Modal, J. E., & Omlin, C. W. (2020). Towards responsible AI for financial transactions. IEEE symposium series on computational intelligence (SSCI), https://doi.org/10.1109/SSCI47803.2020.9308456

[54]. Mesbah, N., Tauchert, C., Olt, C. M., & Buxmann, P. (2019). Promoting Trust in AI-based Expert Systems. Twenty-fifth Americas Conference on Information Systems, https://aisel.aisnet.org/amcis2019/ai_semantic_for_intelligent_info_systems/ai_semantic_for_intelligent_info_systems/6

[55]. Moreno, D., & Takalo, T. (2016). Optimal bank transparency. Journal of Money, Credit and Banking, 48(1), 203-231. https://doi.org/10.1111/jmcb.12295

[56]. Musyaffi, A. M., Baxtishodovich, B. S., Afriadi, B., Hafeez, M., Adha, M. A., & Wibowo, S. N. (2024). New Challenges of Learning Accounting With Artificial Intelligence: The Role of Innovation and Trust in Technology. European Journal of Educational Research, 13(1), 183. https://doi.org/10.12973/eu-jer.13.1.183

[57]. Negi, P. S., & Dangwal, R. C. (2021). Managerial effectiveness and its correlates in Indian banking industry. PSU Research Review, 5(2), 170-181. https://doi.org/10.1108/PRR-05-2018-0014

[58]. Ng, M., Coopamootoo, K. P., Toreini, E., Aitken, M., Elliot, K., & van Moorsel, A. (2020). Simulating the effects of social presence on trust, privacy concerns & usage intentions in automated bots for finance. 2020 IEEE European symposium on security and privacy workshops (EuroS&PW), https://doi.org/10.1109/EuroSPW51379.2020.00034

[59]. Nkomo, B. K., & Breetzke, T. (2020). A conceptual model for the use of artificial intelligence for credit card fraud detection in banks. 2020 Conference on Information Communications Technology and Society (ICTAS), https://doi.org/10.1109/ICTAS47918.2020.233980

[60]. Noreen, U., Shafique, A., Ahmed, Z., & Ashfaq, M. (2023). Banking 4.0: Artificial intelligence (AI) in banking industry & consumer's perspective. Sustainability, 15(4), 3682. https://doi.org/10.3390/su15043682

[61]. Okpara, A. (2015). Self awareness and organizational performance in the Nigerian banking sector. European Journal of Research and Reflection in Management Sciences, 3(1). https://ssrn.com/abstract=3122403

[62]. Ozyilmaz, A., Erdogan, B., & Karaeminogullari, A. (2018). Trust in organization as a moderator of the relationship between self-efficacy and workplace outcomes: A social cognitive theory-based examination. Journal of Occupational and Organizational Psychology, 91(1), 181-204. https://doi.org/10.1111/joop.12189

[63]. Polyportis, A. (2024). A longitudinal study on artificial intelligence adoption: understanding the drivers of ChatGPT usage behavior change in higher education. Frontiers in Artificial Intelligence, 6, 1324398. https://doi.org/10.3389/frai.2023.1324398

[64]. Prisznyák, A. (2022). Artificial intelligence in the banking sector. ECONOMY AND FINANCE: ENGLISH-LANGUAGE EDITION OF GAZDASÁG ÉS PÉNZÜGY, 9(4), 333-340. https://doi.org/10.33908/ef.2022.4.4

[65]. Purwanto, P., Kuswandi, K., & Fatmah, F. (2020). Interactive applications with artificial intelligence: The role of trust among digital assistant users. Форсайт, 14(2 (eng)), 64-75. https://doi.org/10.17323/2500-2597.2020.2.64.75

[66]. Truby J, Brown R, Dahdal A. Banking on AI: mandating a proactive approach to AI regulation in the financial sector. Law and Financial Markets Review. 2020 Apr 2;14(2):110-20.

[67]. Khan, M. T., Akter, R., Dalim, H. M., Sayeed, A. A., Anonna, F. R., Mohaimin, M. R., & Karmakar, M. (2024). Predictive Modeling of US Stock Market and Commodities: Impact of Economic Indicators and Geopolitical Events Using Machine. Journal of Economics, Finance and Accounting Studies, 6(6), 17-33.

[68]. Nayyer, N., Javaid, N., Akbar, M., Aldegheishem, A., Alrajeh, N., & Jamil, M. (2023). A new framework for fraud detection in bitcoin transactions through ensemble stacking model in smart cities. IEEE Access. Nerurkar, P. (2023). Illegal activity detection on Bitcoin transactions using deep learning. Soft Computing, 27(9), 5503-5520.

[69]. Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. Electronic Markets, 33(1), 37.

[70]. Podgorelec, B., Turkanović, M., & Karakatič, S. (2019). A machine learning-based method for automated blockchain transaction signing including personalized anomaly detection. Sensors, 20(1), 147.

[71]. Rahman, A., Debnath, P., Ahmed, A., Dalim, H. M., Karmakar, M., Sumon, M. F. I., & Khan, M. A. (2024). Machine learning and network analysis for financial crime detection: Mapping and identifying illicit transaction patterns in global black money transactions. Gulf Journal of Advance Business Research, 2(6), 250-272.

[72]. Rahouti, M., Xiong, K., & Ghani, N. (2018). Bitcoin concepts, threats, and machine-learning security solutions. Ieee Access, 6, 67189-67205. Saeidimanesh, S. (2024). Transaction Graph Analysis for Bitcoin Address Classification: Traditional Supervised Machine Learning and Deep Learning Methods (Doctoral dissertation, Concordia University).

[73]. Shahbazi, Z., & Byun, Y. C. (2022). Machine learning-based analysis of cryptocurrency market financial risk management. Ieee access, 10, 37848-37856.

[74]. Sizan, M. M. H., Chouksey, A., Miah, M. N. I., Pant, L., Ridoy, M. H., Sayeed, A. A., & Khan, M. T. (2025). Bankruptcy Prediction for US Businesses: Leveraging Machine Learning for Financial Stability. Journal of Business and Management Studies, 7(1), 01-14.