

How Deep Learning Techniques Can Combat Money Laundering by Organized Crime Groups in South Asia's Banking Channels

Sankul Kabra* and Saira Gori

Gujarat National Law University, Attalika Avenue, Knowledge Corridor, Koba,
Gandhinagar, Gujarat, India.

* Corresponding author. Email: sankulphd202021@gnlu.ac.in
<https://doi.org/10.12982/CMUJASR.2025.002>

Editor:

Yos Santasombat,
Chiang Mai University, Thailand

Article history:

Received: March 20, 2024;

Revised: May 24, 2024;

Accepted: June 11, 2024.

ABSTRACT

Money laundering poses a significant threat to the economic stability and security of nations, particularly in regions like South Asia. The evolving nature of money laundering demands advanced technologies to enhance detection and prevention mechanisms. One such advanced technology is deep learning, which has the ability to analyze vast datasets, identify patterns, and adapt to evolving financial crime tactics. This article explores the increasing use of deep learning as a powerful tool in the fight against money laundering orchestrated by organized crime groups in South Asia and addresses the primary challenges associated with employing deep learning techniques for combating money laundering. This article contributes to the discourse on enhancing anti-money laundering efforts in the South Asia region by proposing the adoption of cutting-edge deep learning methodologies within banking institutions to mitigate the threat posed by organized crime groups engaged in illicit financial activities.

Keywords: Money laundering, Deep learning, Organized crime

INTRODUCTION

The United Nations Office on Drugs and Crime (UNODC) approximates that the annual volume of money laundering (ML) worldwide constitutes roughly two to five percent of global gross domestic product, equating to between a staggering \$800 billion to \$2 trillion. This poses a significant and formidable threat to the global economy and its security (Tiwari et al., 2020). South Asia, with its diverse and dynamic economies, is susceptible to organized crime groups (OCGs) engaging in ML. This illicit practice not only undermines financial institutions but also fosters corruption and jeopardizes national security. ML involves transforming proceeds obtained from criminal activities into legitimate-looking funds, essentially disguising unlawfully

sourced money within the regular financial cycle or money circulation process (Sobh, 2020) through a complex sequence of banking transfers or commercial transactions. The primary goal is to make the money appear legitimate, concealing its illicit source and allowing individuals or organizations to enjoy the proceeds without arousing suspicion (Tiwari et al., 2020).

Typically, the process of ML consists of three stages (Levi & Soudijn, 2020): (i) “placement,” involving the introduction of cash into the financial system, (ii) “layering,” characterized by intricate financial transactions aimed at concealing the illicit origin of the cash, and (iii) “integration,” wherein gains are derived from the transactions involving illegal funds. The most opportune stage for identifying a suspicious transaction is during the placement step, as the process becomes increasingly intricate beyond this point, making it challenging to trace transactions that are either layered within or outside the purview of the banking system (Levi & Soudijn, 2020; Kute et al., 2021).

Article 7 of the United Nations Convention against Transnational Organized Crime provides for measures to combat money laundering (Schloenhardt et al., 2023). The convention mandates member nations formulate regulations for banks, non-bank financial institutions, and other susceptible bodies to prevent and detect money laundering. These rules should focus on identifying customers, keeping records, and reporting suspicious transactions (Schloenhardt et al., 2023).

Financial institutions often face penalties for inadequate control measures. For instance, the Commonwealth Bank of Australia was forced to pay a \$700 million penalty under Australia’s Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act 2006 in 2017. In 2019, there were 58 anti-money laundering penalties issued globally, amounting to a total of \$8.14 billion in fines, double that in 2018. In a recent case in 2020, Australia’s Westpac Bank was instructed to pay a record-breaking \$1.3 billion fine for violating Australia’s AML/CTF (Kute et al., 2021). HSBC also confessed to facilitating the laundering of \$881 million in drug profits for the Mexican Sinaloa cartel. The prosecutors and HSBC settled the matter by HSBC agreeing to pay \$1.92 billion in addition to the bank being placed on a five-year probation period (International Narcotics Control Board, 2022). This series of penalties levied against various financial institutions suggests that the current systems and controls are insufficient and ineffective in combating financial crime.

In this context, the integration of Artificial Intelligence (AI) technologies is imperative for augmenting capabilities to identify, track, and combat ML. Machine learning constitutes a branch of AI enabling computers to glean insights from data, recognize patterns, and formulate predictions (Lokanan, 2022). Deep learning, a subset of machine learning, relies on artificial neural networks to grasp intricate patterns and relationships within data. Unlike traditional programming, deep learning does not necessitate explicit instructions for every task, leading to its rising popularity driven by enhanced processing capabilities and the abundance of extensive datasets. These neural networks, inspired by the structure and function of human brain neurons, are adept at learning from vast amounts of data (Jensen & Iosifidis, 2023b).

ML frequently exploits weaknesses in systems and exploits existing legal frameworks. Deep learning algorithms excel in recognizing patterns indicative of money laundering. By analyzing transactional data, deep learning systems can

identify irregularities and flag suspicious activities, enabling authorities to intervene before the laundering process is completed (Sobh, 2020). Deep learning tools can conduct behavioral analysis on financial transactions, establishing a baseline of normal activity and subsequently identifying deviations that may signify illicit transactions. This dynamic approach allows for adaptive responses to evolving ML techniques (Sobh, 2020). Given OCGs often operate through intricate networks, network analysis is important to reveal hidden connections and relationships, aiding investigators in dismantling entire ML ecosystems.

This descriptive article provides an overview of Anti-Money Laundering (AML) regimes in South Asian countries and explores the measures undertaken by governments to address ML within their domestic jurisdictions. We delve into how OCGs engage in ML through banking and associated channels and examine the application of deep learning techniques and models to counter ML within banking channels. The article also sheds light on the primary challenges associated with combating ML through these deep learning techniques.

THE AML REGIMES IN SOUTH ASIAN COUNTRIES

As organized crime groups continue to exploit banking channels for illicit gains, the need for robust AML measures is becoming increasingly pressing. In this section, we delve into the intricate dynamics of AML regimes in South Asian nations.

INDIA

The Parliament of India enacted and uses the Prevention of Money Laundering Act 2002 (PMLA). The primary aim of the PMLA is to prevent ML and facilitate the confiscation of property linked to or derived from ML, along with addressing connected matters (Jain, 2023). To ensure the effective implementation of the PMLA, the Indian government established the central Financial Intelligence Unit – India (FIU-IND) in 2004, which consolidates and coordinates India's AML strategies (Jain, 2023).

FIU-IND is the central national agency tasked with receiving, processing, analyzing, and disseminating information related to suspicious financial transactions. It plays a crucial role in coordinating and strengthening the efforts of national and international intelligence, investigation, and enforcement agencies in the global fight against ML and the financing of terrorism. In alignment with the recommendations of the Financial Action Task Force (FATF), FIU-IND operates as an independent entity reporting directly to the Economic Intelligence Council, headed by the Finance Minister (Jain, 2023).

FIU-IND has to access financial, administrative, and law enforcement information from various sources for the analysis of Suspicious Transaction Reports (STRs) and the processing of references from other agencies. The primary functions of FIU-IND include serving as the central reception point for various reports, such as Cash Transaction Reports (CTRs), Non-Profit Organization Transaction Reports, Cross-Border Wire Transfer Reports, and Reports on the Purchase or Sale of Immovable Property (Ahmad, 2023). It analyzes this information to uncover transaction patterns indicative of ML and related crimes. Additionally, FIU-IND shares information with national intelligence/law enforcement agencies, regulatory

authorities, and foreign financial intelligence units, establishes and maintains a national database, coordinates the collection and sharing of financial intelligence through national, regional, and global networks, and monitors and identifies key areas in ML trends, typologies, and developments through research and analysis (Ahmad, 2023).

The Enforcement Directorate has been designated as the enforcement body, endowed with extensive powers to conduct surveys, searches, seizures, property attachments, arrests, and the imposition of fines and penalties. Additionally, the Enforcement Directorate serves as the adjudicating authority under the PMLA (Pandey, 2023). The Reserve Bank of India (RBI) issued Know Your Customer (KYC) guidelines in 2013, establishing AML/CFT standards and procedures for conducting customer due diligence (CDD) in banks. These guidelines reference the Indian Banks' Associations guidance note on KYC norms and AML standards, which provides an indicative list of high-risk customers, products, services, and geographies for banks' risk assessment (Gupta et al., 2024). Moreover, the RBI instructs banks to consider risks arising from deficient/high-risk jurisdictions identified by the FATF Plenary at times (Gupta et al., 2024).

The Securities and Exchange Board of India issued guidelines outlining AML/CFT obligations for securities market intermediaries under the PMLA. These guidelines categorize clients from high-risk countries, Politically Exposed Persons, Non-Profit Organizations, and companies with beneficial ownership as 'clients of special category,' necessitating enhanced due diligence for such clients (Nishant, et al. 2023). The central board of direct taxes, responsible for implementing direct taxes, monitors politically exposed persons, very high net-worth individuals, and high net-worth individuals to mitigate tax risks and broaden the tax base in these taxpayer groups. The board collaborates with the FIU-IND and other regulators to enhance coordination and monitors matters related to FATF and other bodies dealing with AML/CFT that impact direct taxes (Pandey, 2023).

Courts in India have convicted a total of 25 individuals for ML, and over 400 arrests have been executed since the Enforcement Directorate was granted authority to investigate significant financial offenses. Official data reveals that the directorate has initiated a substantial 5,422 cases under the criminal provisions of the Act. Furthermore, it has provisionally attached assets valued at an impressive 104,702 million rupees through 1,739 orders issued up to March 2022 (Press Trust of India, 2022).

PAKISTAN

Pakistan has adopted a multi-agency approach to implement its AML. With that said, a comprehensive and coordinated risk-based strategy against ML is not fully in place (Sultan & Mohamed, 2023). While Pakistan utilizes financial intelligence to combat ML and predicate crimes, its Financial Monitoring Unit (FMU) has limited capacity to disseminate information and court permission is required (Jan, 2021). Law enforcement agencies in Pakistan have measures to freeze, seize, and prevent property dealing, primarily in predicate offenses cases, with limits to confiscation. Analysis indicates varying levels of understanding among competent authorities regarding ML risks in Pakistan, while the private sector's comprehension of risks is mixed. The cross-

border cash declaration system is not effectively utilized for cash and other seizures at the border (Sultan & Mohamed, 2023). Automated screening for customers and transactions, as per United Nations Security Council resolutions 1267 and 1373, is prevalent in banks and larger entities but limited in the non-banking sector and designated non-financial businesses and professions (DNFBPs) (Mukhtar, 2018).

Larger banks and exchange companies in Pakistan have a reasonable understanding of their AML obligations, conducting internal risk assessments, applying record-keeping requirements, and implementing risk-based CDD policies. However, deficiencies include the ineffective identification of beneficial owners (Zia et al., 2022). There is also no supervisory oversight for AML purposes, and no measures are in place to address ML risks from trusts. Pakistan lacks a formal framework for mutual legal assistance but can execute it based on treaties, reciprocity, and legislative provisions. Informal international cooperation is sought and provided, but law enforcement agencies are not effectively using the FMU to seek financial intelligence from foreign financial intelligence units (Mukhtar, 2018).

Law enforcement agencies in Pakistan have conducted 2,420 ML investigations, resulting in 354 prosecutions and one conviction related to ML. The proportionality and warning effect of sanctions against natural persons could not be assessed. The law enforcement efforts are inconsistent with the identified ML risks (Jan, 2021).

BANGLADESH

In 2002, Bangladesh enacted their Money Laundering Prevention Act, signaling the government's dedication to tackling ML. Subsequently, in 2007, Bangladesh ratified the United Nations Convention Against Corruption, further fortifying its AML efforts (Zafarullah & Haque, 2023). These laws facilitated international cooperation in combating ML and recovering unlawfully moved assets as well as establishing a robust legal framework for identifying, preventing, and prosecuting ML activities within the country. Moreover, they empower authorities to collaborate with foreign counterparts in cross-border investigations (Rana & Awwal, 2020). The government designated the Anti-Money Laundering Department of the Central Bank as the national FIU. This unit collects, analyzes, and disseminates financial intelligence related to ML and terrorist financing. This entity is instrumental in identifying suspicious transactions and sharing crucial information with law enforcement agencies (Zafarullah & Haque, 2023). ML represents a significant challenge to the economic stability and integrity of Bangladesh. Despite various initiatives aimed at addressing this issue, it persists, primarily fueled by clandestine mechanisms such as the hundi system (Momo, 2021).

Bangladesh has a large informal economy, characterized by cash-based transactions and a lack of transparency. This provides fertile ground for criminals to launder money through businesses that operate outside the formal banking sector. Bangladesh receives a substantial amount of remittances from its diaspora working abroad. While remittances contribute significantly to the economy, they also present opportunities for ML, especially through informal channels and unregulated money transfer services (Morshed & Rahman, 2021). The underground hawala or "hundi" system remains a primary ML risk in Bangladesh. This system is frequently utilized to transfer money and valuables outside of traditional banking channels, especially

for repatriating wages earned by Bangladeshi expatriates. Despite improvements in formal banking transfer services, the hundi system endures due to its capacity to evade taxes, customs fees, and currency regulations. In addition, Bangladesh's economy, driven by export sales and remittances, is susceptible to ML risks. The reliance on remittances, both official and through underground channels, underscores the imperative for vigilant AML measures (Morshed & Rahman, 2021).

Transparency International Bangladesh has recently disclosed that approximately US \$3.1 billion is illicitly transferred out of Bangladesh annually. Even this amount would result in a yearly revenue shortfall of approximately 120 billion taka (Jamal, 2022). Despite the measures, the effectiveness of Bangladesh's efforts to combat ML in its banking channels hinges on sustained commitment, robust enforcement, and collaboration with domestic and international stakeholders. Addressing underlying issues such as corruption, strengthening regulatory oversight, and promoting financial transparency, are essential to safeguarding the integrity of the Bangladeshi economy.

SRI LANKA

Sri Lanka's Parliament passed the Prevention of Money Laundering Act 2006 to criminalize ML in accordance with the provisions outlined in the Vienna and Palermo conventions (Sivaguru & Tilakasiri, 2023). Sri Lanka has established an independent FIU within the Central Bank of Sri Lanka, comprising personnel from various regulatory bodies, authorities, and law enforcement agencies (Hendeniya et al., 2023). The FIU is tasked with coordinating the efforts of relevant investigative agencies. The primary responsibility for investigating ML and terrorist financing offenses lies with the Sri Lankan Police Department. However, the Police Department has not yet formed any specialized investigation teams dedicated to probing ML and proceeds of crime (Financial Intelligence Unit of Sri Lanka, 2023).

The threat assessment of ML in Sri Lanka is based on an assumption that ML is closely linked to criminal proceeds. The Asia Pacific Group on Money Laundering (APG) maintains an overall medium ML threat level for Sri Lanka (Asia/Pacific Group on Money Laundering, 2021). The Working Group of APG has identified 26 ML cases that are currently in advanced stages of investigation conducted by LEAs. Among these, eight cases have undergone government audits and investigations resulting from focused audits (Asia/Pacific Group on Money Laundering, 2021). During the evaluated period, the Attorney General's department issued 54 ML/TF indictments. In this context, the APG Working Group has noted 28 indictments that involved ML charges, with three pertaining to TF charges linked to bank accounts. Among the information received on 33 indictments out of the total 54 cases, 28 were associated with banking institutions, bank accounts, and/or other financial products offered by the banking sector (Financial Intelligence Unit of Sri Lanka, 2022).

BHUTAN

Bhutan's Financial Intelligence Department (FID) operates as an independent and autonomous department established within the Royal Monetary Authority, in accordance with Bhutan's AML and CFT Act 2018. The Head of the FID is responsible

for day-to-day operations, management, and the execution of functions outlined in the AML and CFT Act 2018. Financial Institutions and DNFBPs are designated as reporting entities under the AML and CFT Act. Reporting entities are obligated to provide submissions to the FID in accordance with the Act. The FID analyzes transaction reports and generates actionable Intelligence Reports (IRs). The FID forwards the IRs to relevant LEAs based on the identified predicate offense. ML crimes are subject to a maximum nine years' imprisonment for a third-degree felony and fines (Royal Monetary Authority of Bhutan, 2018a).

The FID received 73,300 CTRs from reporting entities, a 5.3 percent increase compared to the previous reporting period in 2017. The statute empowers the FID to establish arrangements with foreign counterparts performing similar functions and bound by similar secrecy obligations, facilitating the exchange of financial intelligence (Royal Monetary Authority of Bhutan, 2018a). National risk assessments determined that Bhutan, on the whole, is evaluated as having a "medium" level of ML risk. This assessment is influenced by a "lower" likelihood of ML attempts, a "higher" probability that those engaging in ML activities go undetected, and a "medium" level of risk associated with inadequate sanctions for ML perpetrators. The primary factors contributing to these risk levels include the country's proximity to India, the inability of LEAs to identify ML activity during investigations of predicate crimes, and uncertainties surrounding the imposition and enforcement of ML-related sanctions (Royal Monetary Authority of Bhutan, 2018b).

NEPAL

The Nepal FIU operates within the Nepal Rastra Bank and possesses adequate resources, robust operational autonomy, established policies and procedures governing all its functions, and signed memoranda of understanding with other relevant agencies. The FIU is actively working to enhance its operations by implementing AML actions (Upadhyay, 2024). However, there is room for improvement in the STR reporting by financial institutions, and DNFBPs are not currently providing any reports. While key LEAs are utilizing financial intelligence, ongoing effort is required to enhance reporting by financial institutions and expand reporting from DNFBPs (Asia/Pacific Group on Money Laundering, 2023).

In Nepal, the foremost ML threats stem from corruption, tax evasion, and human trafficking, representing significant risks due to their potential to generate illicit proceeds and inflict adverse economic and social consequences (Biswakarma & Bhusal, 2023). The country's porous borders pose a substantial ML risk, closely linked to both domestic and foreign predicate offenses, such as narcotics trafficking, illicit gold and cash smuggling, and environmental crimes. Sectors particularly susceptible to ML include banking, cooperatives, dealers in precious metals and stones, casinos, and remittance providers. The prevalence of the informal financial system, including the use of hundis, further adds to the complexity of the ML landscape in Nepal (Biswakarma & Bhusal, 2023).

The Department of Money Laundering Investigation serves as the sole ML investigative agency. Although referrals to the department do not consistently align with Nepal's risk profile, it has successfully investigated 58 ML cases, resulting in 45 prosecution cases and the conviction of 32 natural persons for ML (Upadhyay, 2024).

The majority of these convictions are associated with self-laundering linked to banking offenses. However, Nepal faces a limited number of investigations, prosecutions, and convictions for other high-risk predicate crimes. Nepal has outlined significant policy objectives related to high-level confiscation but the translation of these objectives into institutional-level policies and procedures by LEAs and corresponding confiscation outcomes is still pending. The execution of 32 percent of requests is somewhat timely, and Nepal typically submits around 12 outgoing mutual legal assistance requests annually (Asia/Pacific Group on Money Laundering, 2023).

MYANMAR

The Central Bank of Myanmar takes an engaged stance in executing Myanmar's domestic AML program to safeguard the financial system from criminal activities linked to ML. Consequently, the Central Bank of Myanmar has issued regulatory directives which encompass compliance with CDD, record-keeping, and requirements for STRs and CTRs (Central Bank of Myanmar, 2022).

On October 21, 2022, the FATF designated Myanmar as a high-risk jurisdiction due to significant deficiencies in its efforts to combat ML/TF and the financing of proliferation. The day following this announcement, the Central Bank of Myanmar issued a response, highlighting that while Myanmar was included on the list of high-risk jurisdictions requiring action, it does not equate to the status of countries like North Korea and Iran, which are subject to countermeasure application by both FATF members and non-members (Nwe Oo & Yuwadee Thean-Ngarm, 2022). Consequently, the FATF has advised its members to implement proportional enhanced due diligence measures in response to the risks posed by Myanmar. While applying these measures, countries should ensure that the flow of funds for humanitarian assistance, legitimate non-profit organization activities, and remittances remains uninterrupted (FATF, 2023).

Myanmar is urged to persist in implementing its action plan to rectify these deficiencies. This includes: (1) demonstrating an improved comprehension of ML risks in key areas; (2) illustrating that on-site/off-site inspections are risk-based and hundi operators are duly registered and supervised; (3) showcasing an increased utilization of financial intelligence in LEA investigations and enhancing operational analysis and dissemination by the FIU; (4) ensuring ML investigations and prosecutions align with identified risks; (5) demonstrating the investigation of transnational ML cases with international cooperation; (6) illustrating an augmentation in the freezing/seizing and confiscation of criminal proceeds, instrumentalities, and/or property of equivalent value; and (7) managing seized assets to preserve the value of confiscated goods until the completion of the confiscation process (FATF, 2023).

ML BY OCGs THROUGH BANKING CHANNELS

While traditional ML methods remain prevalent, modern advancements have enabled launderers to adapt and leverage the internet to evade detection. The internet provides an avenue for launderers to elude scrutiny effortlessly. With the proliferation of online banking platforms, anonymous digital payment services, peer-to-peer

transfers via mobile devices, and the emergence of virtual currencies like Bitcoin, identifying illicit money transfers is increasingly challenging (Langdale, 2023). Tracking financial transactions and interrupting illegal money flows can cripple OCGs (International Narcotics Control Board, 2022).

The landscape of transnational OCGs in Southeast Asia has undergone swift evolution in recent times. Initially characterized by a surge in cross-border trafficking of synthetic drugs and various commodities, this transformation has been notably influenced by significant shifts in technology (Sullivan et al., 2020; Kabra & Gori, 2023). Prominent transnational OCGs have adopted technology, thereby revolutionizing the crime ecosystem within the region. These criminal networks use intricate financial structures, shell companies, and international transactions to obscure the trail of illicit funds (Nazar et al., 2023). The proliferation of online casinos and cyber-fraud has surged in Southeast Asia, following the advent of the COVID-19 pandemic (Nimma, 2022). Alarmingly, OCGs overseeing many of these activities have increased in sophistication. They employ advanced techniques such as data mining, blockchain technology and generative AI (Faccia et al., 2020). The involvement of organized crime amplifies the scale and complexity of ML activities, posing significant challenges for law enforcement and regulatory authorities (Nazar et al., 2023).

In east and Southeast Asia, criminals often employ point running syndicates, also known as 'moving ants', to transfer stolen funds across multiple bank or cryptocurrency exchange accounts, as well as online casinos, in order to conceal the origin and destination of the money. This informal method of money transfer, which frequently crosses borders, can involve hundreds or even thousands of individuals and has gained significant popularity among young people. These individuals offer their bank accounts and establish front companies for use by point running syndicates, assisting in account and company pass-through activities in exchange for a fee (United Nations Office on Drugs and Crime, 2024). Point running is frequently used to facilitate illegal online gambling and adds another layer to the process of ML, whereby funds are channeled through online gambling platforms and then cleaned by exchanging them for cash through the platform, thus legitimizing the source of the funds as casino winnings. Motorcades represent an expansion of point running syndicates, providing sophisticated layering schemes that involve routing money through multiple bank accounts for a percentage of the total laundered and transferred funds (Nimma, 2022). UNODC has also noted a common practice among large motorcade teams of collaborating with others when handling very substantial contracts to enhance concealment and efficiency (United Nations Office on Drugs and Crime, 2024).

These platforms have been widely exploited to intermingle and obscure illicit proceeds of crime under the guise of legitimate online gambling earnings (Faccia et al., 2020). This method often involves transaction miscoding to disguise the use of the casino platform and relies on third- and fourth-party payment providers to obscure the nature of the transactions (United Nations Office on Drugs and Crime, 2024). For example, prominent Asian OCGs, the Sam Gor drug trafficking network and the 14K triad, have been implicated in utilizing junkets to launder money through Australian casinos. In 2023, a casino operator paid a penalty of AU \$450 million for 546 violations of AML laws uncovered during the nation's investigation into casinos and junkets (Chief Executive Officer of AUSTRAC, 2022).

As authorities have gained a deeper understanding of third- and fourth-party payments, especially in the wake of initiatives like 'Operation Chain Break' and similar efforts in China, OCGs have adapted by increasingly incorporating cryptocurrencies into their illicit gambling activities. This shift presents significant challenges for investigators (Langdale, 2023). In the Philippines, several licensed casinos and representatives of junket operators were discovered to have played a significant part in laundering about US \$81 million stolen in a cyberattack linked to the Lazarus Group from the Bangladesh Central Bank in 2016. Although the funds initially flowed through banks and remittance firms, their trace vanished after being transferred to casino junket operators (United Nations Office on Drugs and Crime, 2024).

The rise of cyberspace and cryptocurrencies presents a fresh battleground for OCGs vying for dominance in expansive illicit markets involving drugs, arms, human trafficking, and sexual exploitation (Paula et al., 2016). Global drug cartels utilize Binance, the world's largest cryptocurrency exchange, to launder millions of dollars, alleged by the DEA. Consequently, Binance is said to be cooperating with investigators in efforts to apprehend those involved. The DEA's investigation suggests that transactions ranging from US \$15 million to \$40 million have been laundered through Binance. As the largest exchange globally in terms of daily cryptocurrency trading volume, Binance continues to attract attention amidst allegations of illicit activity (Yusoff et al., 2023).

COMBATING ML BY OCGS USING DEEP LEARNING MODELS

Organized crime systematically dismantles small businesses and erodes trust in democratic institutions. Conventional crime detection techniques such as pattern recognition and crime series analysis are insufficient since they mainly target violent or easily detectable crimes, not intricate and subtle expressions of ML. Consequently, there is an urgent need for alternative systems to assist criminal investigators in deciphering and exposing the complex structures of OCGs, which involve intricate interconnections of finances, politics, logistics, international relations, familial ties, and culture (Levi & Soudijn, 2020).

There is much to be done before the machines are capable of significantly advancing our efforts against organized crime. However, there has been a recent acceleration in the progress of machine learning. With an increasing amount of data becoming accessible, the integration of diverse datasets is smoother than ever (Canhoto, 2021). Additionally, visualization techniques, which simplify complexity by translating machine language into understandable indicators, are enhancing communication. Furthermore, the development of more sophisticated systems, not only focused on identifying patterns and correlations, but also on analyzing causation and structure, is on the horizon (Canhoto, 2021). In the context of law enforcement, this transition from focusing on patterns to understanding structures and from correlation to causality holds potential to shift approaches from addressing symptoms and individuals to targeting relationships and organizations (Lokanan, 2022).

Organized crime exhibits significant contextual and cultural variations, making it challenging to generalize patterns. These patterns not only differ between various criminal organizations but also vary among different regions within the same

organization, often structured like chapters (Ganapathy, 2020). To effectively train machine learning models, a diverse range of data on past offenses is necessary. Therefore, besides synthetic data, other extensive sources of data must be considered (Canhoto, 2021).

Deep learning, a branch of machine learning, employs neural networks to address complex problems. Modeled after the human brain's architecture, these networks comprise interconnected nodes arranged in layers to process and manipulate data. Central to deep learning is the utilization of deep neural networks with multiple layers, enabling the discovery of hierarchical patterns and features within data. Notably, deep learning algorithms autonomously refine and enhance their performance without manual intervention (Jensen & Iosifidis, 2023a). Network analytics involves examining the connections between interconnected entities to gain insights into their relationships. Rather than focusing solely on individual entities, this approach scrutinizes various components of the network to identify similarities with known ML methods and unusual customer behavior. These networks are constructed through connections between customers and their associated activities. These connections may be based on internal financial data, such as account transfers or joint ownership, or external data, such as shared addresses or common usage of the same machines (Richardson et al., 2019).

Network analytics complements the existing techniques used by many banks for AML monitoring, such as machine learning and fuzzy logic-based approaches. Metrics related to network structure, like connectivity, for each customer can enhance the accuracy of customer risk assessment or transaction monitoring models (Alkhalili et al., 2021). Moreover, fuzzy logic-based methods and deep learning techniques can be used for resolving customer identities which can be refined by analyzing the strength of connections between accounts. Apart from enhancing the efficacy of current methodologies, network analytics also equips investigators with novel capabilities. For instance, algorithms for community detection can identify groups of customers that may indicate illicit activities (Richardson et al., 2019).

Enforcement agencies could begin by constructing a network of customer connections using various methods such as account transfers, joint account ownership, and payments, both internally within the institution and externally with other institutions using destination account numbers (Shokry et al., 2020). Next, they could establish inferred connections between customers by examining shared addresses, employers, or social media information. While enterprise-grade graph databases are often the ideal end goal, initially, data could be stored in a standard relational database to commence the process. Even without sophisticated analytics, creating this database of connections will expedite investigations and provide data scientists with a valuable resource that can be utilized for AML purposes (Shokry et al., 2020). The key factors for success include accessing the appropriate external data sources, acquiring proficiency in network science techniques, and leveraging deep subject matter knowledge to guide model development (Richardson et al., 2019).

Within financial institutions, data from various internal banking systems, including retail banking, consumer banking, wealth management, institutional banking, etc., undergoes assessment in the rule-based AML system. This system evaluates each transaction against predetermined rules to identify (a) transactions amounting to \$10,000 or more, (b) money transfers to and from international sources,

and (c) suspicious activities indicative of ML or financial fraud (Kute et al., 2021). While rule-based systems are integral for banks and effectively flag transactions aligning with predefined rules (categories 'a' and 'b'), they encounter challenges in detecting emerging fraud patterns (category 'c'). If a transaction aligns with a rule, a red flag or alert is triggered, subsequently processed, and reported to regulatory bodies. The rules are defined based on threshold amounts for different transaction types in accordance with regulatory requirements, and recommendations provided by FATF (Manning et al., 2021).

Although rule-based systems play a crucial role, they tend to produce numerous false positive alerts for suspicious transactions, necessitating significant manual effort for triage. Some technologically adept financial institutions have begun to utilize AI/ML technology to automate such activities, aiming to enhance the accuracy of detecting suspicious activities (Chen et al., 2018).

DEEP LEARNING DETECTION METHODS FOR SUSPICIOUS TRANSACTIONS

Deep learning methods are powerful tools for detecting suspicious transactions within financial systems. These techniques leverage complex neural network architectures to automatically learn and extract intricate patterns from large volumes of transactional data. Financial transaction datasets for detecting ML activities typically comprise transaction records obtained from various sources such as banking institutions, financial regulators, and law enforcement agencies. These datasets may include structured data such as transaction amounts, timestamps, account identifiers, and transaction types, as well as unstructured data such as transaction descriptions or narratives (Jensen & Iosifidis, 2023b).

DATASET PREPARATION AND PRE-PROCESSING

Dataset preparation for deep learning models involves collecting a diverse range of transactional data, including both legitimate and fraudulent examples, while ensuring proper labeling. Pre-processing entails standardizing features, handling missing values, and potentially applying techniques like normalization or dimensionality reduction to optimize data for training deep neural networks (Watkins et al., 2020). Steps include the following.

1. Data Collection: Gathering transaction data from multiple sources while ensuring compliance with privacy regulations and data protection laws.
2. Data Cleaning: Removing duplicate entries, correcting errors, and handling missing values to ensure data quality.
3. Feature Engineering: Extracting information on transactions, such as frequency, amount, and patterns, to enhance the predictive power of the models.
4. Data Sampling: Balancing the dataset to address class imbalance issues, ensuring that the models are trained on representative samples of both normal and suspicious transactions.
5. Standardization: Scaling numerical features to a common scale to prevent features with larger magnitudes from dominating model training.

6. Anonymization: Masking or anonymizing sensitive information such as account numbers or customer identities to protect privacy and confidentiality (Jensen & Iosifidis, 2023b).

Annotating financial transaction datasets for training deep learning models involves labeling transactions as either normal or suspicious based on predefined criteria or expert judgment. Types of annotations include:

- (i) Expert Annotations: Domain experts, such as financial analysts or compliance officers, annotate transactions using their expertise and knowledge of ML patterns and typologies.
- (ii) Rule-Based Annotations: Predefined rules or thresholds are applied to classify transactions as suspicious, such as exceeding a certain transaction amount or frequency threshold.
- (iii) Semi-Supervised Learning: A combination of labeled and unlabeled data are utilized. Initially a subset of transactions is manually annotated, and then the model iteratively labels additional data points based on its predictions (Jensen & Iosifidis, 2023b).

DEEP LEARNING METHODS

ML detection solutions are divided into two main categories. The first category focuses on identifying suspicious transactions. Often AutoEncoder and Graph Convolutional Neural Network deep learning methods are used to detect suspicious transactions (Kute et al., 2021). The second category is dedicated to aiding the investigation of identified suspicious transactions or alerts flagged by rule-based systems. This category, commonly referred to as decision support systems, is when a multi-channel Convolutional Neural Network (CNN) utilizing Natural Language Processing (NLP) and a scalable Graph Convolutional Network investigate alerts (Kute et al., 2021).

Neural networks, a subset of machine learning algorithms inspired by the structure and function of the human brain, have proven to be powerful tools in analyzing financial transactions and detecting ML activities. Different types of neural networks, each with its unique architecture and capabilities, are utilized for this purpose (Lokanan, 2022). CNNs are particularly well-suited for analyzing financial transaction data due to their ability to capture spatial and temporal patterns. In the context of financial transactions, CNNs can be configured to analyze transaction sequences as images or time-series data, where each transaction represents a pixel or time step. CNNs excel at detecting patterns in such data, making them effective in identifying anomalies indicative of ML activities (Lokanan, 2022). Their layers include the input layers (each financial transaction is represented as input data), convolutional layers (applying filters to extract features from transaction sequences), pooling layers (pooling operations reduce the dimensionality of feature maps while preserving essential information), and fully connected layers (aggregate extracted features and make predictions about the likelihood of ML activities).

CNNs automatically learn hierarchical representations of transaction data, capturing both local and global patterns relevant to ML detection. CNNs are robust to noise and variations in transaction data, allowing them to generalize well to unseen instances of ML activities (Silva et al., 2023).

RECURRENT NEURAL NETWORKS (RNNs)

RNNs are another type of neural network commonly used to analyze financial transactions, particularly for their ability to model sequential dependencies and temporal dynamics. RNNs process input sequences one step at a time while maintaining a memory of previous steps, enabling them to capture long-term dependencies in transaction data (Lokanan, 2022). They are also configured in layers: an input layer (each financial transaction is fed into the network sequentially); recurrent layers (layers maintain a hidden state that captures temporal dependencies between consecutive transactions); and Fully Connected Layers (similar to CNNs, fully connected layers aggregate information from recurrent layers and make predictions about ML activities). RNNs can handle input sequences of variable lengths, accommodating the dynamic nature of financial transactions (Silva et al., 2023). In summary, while CNNs excel at capturing spatial patterns in transaction data, RNNs are adept at modeling temporal dependencies and long-term dynamics.

There are other deep learning techniques that have shown significant utility. Discussions of some of these follow.

Scalable Graph Convolution Neural Network: A Graph Convolutional Neural Network with scalability was employed by Weber et al. (2018) for forensic analysis of massive, dense, and dynamic financial data. The visualized results from this analysis serve as an effective decision support tool for AML analysts tasked with reviewing a substantial volume of alerts generated by rule-based AML systems (Weber et al., 2018). The methodology was developed and assessed using a synthetic graph (1 million nodes and 9 million edges) generated through the AML sim data simulator tool. In this context, a vertex represents an account with attributes like account number, account type, owner name, and account creation date, while an edge symbolizes a transaction with attributes such as transaction ID, amount, and timestamp. By utilizing escalated alerts and Suspicious Matter Reports (SMRs) as labeled data, a semi-supervised learning model predicts the suspiciousness of a given node and identifies potential bad actors in the transaction network based on direct or indirect connections with the node (Weber et al., 2018). Despite their potential, there are various challenges, including complexities arising from high-speed transaction systems, real-time systems, multi-channel updates, data size, data speed, data variety, and diverse business applications. Therefore, it is imperative to carefully contemplate the appropriate infrastructure, tools, and strategies to address these challenges and enhance the performance of future graph-based solutions (Kurshan et al., 2020).

Multi-channel Convolutional Neural Network: Han et al. (2018) introduced an innovative distributed and scalable framework utilizing deep learning-powered NLP technology to enhance AML monitoring and investigation. This framework conducts diverse levels of sentiment analysis, entity identification, relationship extraction, and link analysis across various data sources like news, tweets, and social media (Han et al., 2018). Each NLP module specializes in a particular data source for analysis, generating recommendations. The proposed framework is structured on a micro-service-oriented distributed architecture and an integration platform based on Advanced Message Queuing Protocol, employing databases such as Cassandra, Neo4j, and MySQL, along with Twitter and a news engine. The data considered comprises financial data relating to KYC, customers, accounts, and transactions, and

open data, including financial news articles, financial reports, fraud open databases, and social media content (Han et al., 2018).

AutoEncoder: Paula et al. (2016) introduced an unsupervised deep learning model designed for the classification of Brazilian exporters to assess the potential for fraudulent activities in exports. The model employs the AutoEncoder classifier to identify anomalies by considering typical transaction patterns within the data. Given that Brazilian exports extend to approximately 200 countries through the involvement of 50,000 legal entities engaged in shipping goods, the author utilized the foreign trade database from the Secretariat of Federal Revenue of Brazil to apply the deep learning model. The objective was to identify export organizations whose explanatory variables in their export operations deviate from the regular pattern (Paula et al., 2016).

Advancements in computing and storage infrastructure, coupled with the continuous generation of substantial volumes of data and the imperative to leverage this data for practical insights, have spurred extensive research in machine learning methodologies over the past decade. While achieving accurate predictions has been the central focus in model development, this pursuit has led to deficiency in transparency, interpretability, and explainability of ML models.

INTERPRETABILITY OF DEEP LEARNING MODELS

Attention-based models incorporate attention mechanisms that highlight relevant features or input sequences contributing to model predictions. By visualizing attention weights, analysts can interpret which aspects of transaction data influence models' decisions, enhancing interpretability (Kute, 2022). Deep learning models may integrate explainable AI techniques, such as Local Interpretable Model-agnostic Explanations or Shapley Additive Explanations, to generate explanations for individual model predictions. These techniques provide insights into models' decision-making processes, enabling stakeholders to understand the rationale behind model predictions (Tertychnyi et al., 2022).

Deep learning models can conduct feature importance analysis to identify the most influential features in distinguishing between normal and suspicious transactions. By ranking features based on their importance, analysts can prioritize high-impact variables and gain insights into the underlying patterns driving model predictions (Tertychnyi et al., 2022). Deep learning models may incorporate visualization techniques to depict model architectures, activation patterns, or decision boundaries. Visual representations help stakeholders understand the inner workings of the model and interpret its behavior, facilitating trust and confidence in model predictions (Tertychnyi et al., 2022).

EVALUATION METRICS AND MODEL PERFORMANCE

Deep learning models used in AML applications are typically evaluated using various performance metrics to assess their effectiveness in detecting suspicious transactions. Some specific performance metrics commonly used to evaluate deep learning models in AML include:

Accuracy: Accuracy measures the proportion of correctly classified transactions (both true positives and true negatives) out of the total number of transactions. Accuracy can be tested using the Formula: $(TP + TN) / (TP + TN + FP + FN)$. Accuracy provides an overall assessment of a model's effectiveness in correctly identifying both normal and suspicious transactions (Bui et al., 2020).

Precision: Precision measures the proportion of correctly identified suspicious transactions (true positives) out of all transactions classified as suspicious (true positives and false positives). Precision can be tested using the Formula: $TP / (TP + FP)$. Precision indicates the model's ability to avoid misclassifying normal transactions as suspicious, minimizing false positives (Bui et al., 2020).

Recall (Sensitivity): Recall measures the proportion of correctly identified suspicious transactions (true positives) out of all actual suspicious transactions (true positives and false negatives). Recall can be tested using the formula: $TP / (TP + FN)$. Recall assesses the model's ability to correctly detect suspicious transactions, minimizing false negatives (Youssef et al., 2023).

F1 Score: The F1 score is the harmonic mean of precision and recall, providing a balanced measure of a model's performance. An F1 score can be tested using the formula: $2 \times (Precision \times Recall) / (Precision + Recall)$. The F1 score considers both precision and recall, making it suitable for evaluating models in imbalanced datasets where the number of suspicious transactions is significantly lower than normal transactions (Bui et al., 2020; Youssef et al., 2023).

Confusion matrix: A confusion matrix provides a tabular representation of the model's predictions compared to actual labels, showing the number of true positives, false positives, true negatives, and false negatives. It helps in understanding the distribution of classification outcomes and identifying areas for improvement in the model (Youssef et al., 2023). These performance metrics collectively provide insights into the effectiveness, robustness, and reliability of deep learning models in detecting suspicious transactions related to ML. By evaluating these metrics, stakeholders can assess the model's performance and make informed decisions regarding its deployment in real-world AML systems.

Deep Learning Models v. Traditional Models: Deep learning models have shown promise in improving detection rates and reducing false positives compared to traditional statistical or machine learning models used for AML purposes (Domashova & Mikhailina, 2021). Deep learning models, such as CNNs and RNNs, can automatically learn hierarchical representations of complex patterns and relationships in financial transaction data. These models excel at capturing intricate patterns and anomalies in large-scale datasets, leading to higher detection rates of ML compared to traditional models (Domashova & Mikhailina, 2021). Traditional statistical or machine learning models, such as logistic regression, decision trees, or support vector machines, rely on manually engineered features and predefined rules to detect suspicious activities. While these models may achieve reasonable detection rates, they may struggle to capture intricate patterns or adapt to evolving ML tactics effectively. Traditional models may be limited by the complexity of the relationships between features and the inability to automatically learn from raw data (Kute et al., 2021).

False Positives: Deep learning models, particularly when trained on large and diverse datasets, can effectively learn to distinguish between normal and suspicious

transactions, leading to a reduction in false positives. By automatically learning complex patterns and representations from raw data, deep learning models can identify subtle indicators of ML while minimizing the occurrence of false alarms (Alotibi et al., 2022). Traditional models, especially when relying on manually engineered features and rule-based approaches, may produce a higher rate of false positives. These models may be prone to generating alerts based on rigid thresholds or simplistic rules, leading to a higher likelihood of false alarms. Moreover, traditional models may struggle to adapt to changing patterns of ML activities, resulting in a higher false positive rate over time (Kute et al., 2021).

In summary, deep learning models generally outperform traditional statistical or machine learning models in terms of detection rates and false positives for AML purposes. Deep learning's ability to automatically learn complex patterns and representations from raw data, combined with its adaptability to evolving trends, contributes to higher detection accuracy and lower false positive rates when identifying suspicious transactions related to ML.

INTEGRATION WITH CURRENT BANKING SYSTEMS

The integration of proposed deep learning models with existing banking systems and AML workflows is essential to ensure seamless adoption and maximize their impact on the efficiency of AML processes and daily operations of financial institutions. Deep learning models can be deployed as Application Programming Interfaces (APIs) that seamlessly integrate with existing banking systems and AML software platforms. APIs enable real-time interaction between models and banking systems, allowing for efficient data exchange and model inference (Alexandre & Balsa, 2023).

The proposed models can integrate into existing data pipelines within financial institutions, where transaction data is collected, processed, and analyzed for AML purposes. Integration with data pipelines ensures that the models receive timely access to transaction data for detection and monitoring. Deep learning models can be incorporated into automated AML workflows that orchestrate various tasks such as data ingestion, pre-processing, model inference, alert generation, and case management. Workflow automation streamlines AML processes and ensures that the models are seamlessly integrated into existing operational workflows (Youssef et al., 2023).

ADAPTABILITY TO EVOLVING ML TECHNIQUES

The deep learning models proposed here must be adaptable to emerging patterns of ML in order to combat the evolving strategies of organized crime groups. This can occur through continuous learning mechanisms, "transfer learning," and the ability to update knowledge bases without extensive retraining. "Transfer learning" is a technique where a model trained on one task is adapted or fine-tuned for a related task with a smaller dataset. By fine-tuning pre-trained models on updated datasets containing recent instances of ML activities, the models can quickly adapt to changing patterns and enhance their effectiveness in detecting novel ML strategies (Raiter, 2021).

“Online learning”, also known as incremental learning or streaming learning, enables models to update their knowledge continuously as new data becomes available. Deep learning models for AML can incorporate online learning mechanisms to adapt to emerging patterns of ML in real-time. By ingesting new transaction data incrementally and updating model parameters iteratively, these models can dynamically adjust their decision boundaries and feature representations to capture evolving ML tactics (Zand et al., 2020).

“Reinforcement learning” involves training models to make sequential decisions through trial and error, guided by rewards or penalties. Deep reinforcement learning approaches can be employed to train AML models to adapt to new ML patterns by continuously learning from interactions with the environment (Raiter, 2021). Models receive feedback based on the effectiveness of their decisions in detecting suspicious transactions, allowing them to iteratively improve their detection capabilities and adapt to changing ML strategies (Labanca et al., 2022).

“Active learning” is a technique where models iteratively select the most informative instances for manual annotation, thereby focusing human efforts on labeling instances that are most beneficial for improving model performance. Deep learning models for AML can incorporate active learning strategies to prioritize the labeling of new and uncertain instances that may represent emerging patterns of ML. By iteratively updating the training dataset with annotated instances, these models can continuously refine their knowledge base and adapt to evolving ML strategies (Labanca et al., 2022).

CHALLENGES OF CURRENT SYSTEMS DETECTING ML

While technology has streamlined banking services for customers, it has concurrently opened new opportunities for fraudulent activities. The surge in transaction volume and frequency, the existence of multiple customer channels, real-time transaction settlement, digital banking, and evolving fraud patterns have kept the landscape dynamic. Additionally, the continuously shifting regulatory environment poses an ongoing challenge for the industry (Oeben et al., 2019). The detection of suspicious ML transactions involves a multi-step classification process, making decisions at various levels such as the transaction level, alert level, case level, SMR level, and ultimately is enforced by law enforcement agencies. Some decisions are automated by software, while others necessitate human intervention for further investigation. The system’s capability to determine the degree of suspicion in a transaction can be enhanced, but the ultimate decision regarding whether a transaction involves ML or is legitimate is reserved for a well-established and responsible government agency (Dalla Pellegrina et al., 2020).

AML laws are distinctive in their requirement for private-sector entities to actively seek out suspicious activities among their customers and report them to FIUs without notifying the customers themselves. Such laws mandating private sector entities to uncover illicit behavior by their clientele are uncommon. While compliance laws, such as those addressing corruption, often necessitate companies to establish measures like whistleblowing to identify and report internal criminal activity, the obligation to detect and report the criminal activity of customers is less common (Maxwell et al., 2020). This places bank compliance departments in the uncomfortable

position of acting as government informants, conflicting with their traditional duty of maintaining customer confidentiality. However, there are valid reasons for imposing this obligation on financial institutions and insurance companies.

One reason is that the complexity of ML and its reliance on the customer relationship context means that only financial institutions have access to the necessary information to detect suspicious patterns. Furthermore, financial institutions have significant economic incentives to overlook criminal funds. Without legal requirements to identify and report criminal activities, economic incentives would likely lead institutions to accept deposits of illicit funds except in the most obvious cases of illegality. The third and fourth laws on AML have shifted toward a risk-based approach, allowing banks to develop detection rules tailored to their clients and business, promoting evidence-based decision-making to target the risks of ML and terrorist financing (Maxwell et al., 2020). Another significant obstacle hindering law enforcement's capacity to monitor ML activities is the issue of manpower. The shortage of federal agents means that only a fraction of the billions of dollars laundered annually can be effectively tracked down (Watkins et al., 2020).

Models with high prediction accuracy tend to be inherently non-interpretable, posing challenges for comprehending the rationale behind the decisions they make (Korauš et al., 2019). The data utilized by machine learning algorithms involves customer, account, and transaction information, raising concerns about the potential misuse or disclosure of confidential information when providing explanations for the decisions (Mashrur et al., 2020; Parne, 2021). People place their trust in a system when they have a precise understanding of its operations. However, black-box models lack interpretability, despite offering high accuracy, which can erode confidence and trust in the system.

REGULATORY AND PRIVACY CONCERNS

Regulatory compliance and adherence to global AML regulations and data privacy laws are critical considerations in the deployment of deep learning models for AML purposes. Financial institutions and businesses must comply with AML regulations imposed by regulatory authorities such as the FATF and local regulatory bodies. These regulations mandate the implementation of effective AML measures to prevent ML and terrorist financing activities. Data privacy laws, such as the European Union's General Data Protection Regulation and the California Consumer Privacy Act, impose stringent requirements for the collection, processing, and storage of personal and sensitive data. Financial institutions must ensure that AML efforts adhere to these laws to protect customer privacy rights (Thommandru et al., 2023).

Regulatory authorities may require financial institutions to provide explanations for AML decisions and ensure the interpretability of AML models. Transparent and interpretable models are essential for regulatory compliance, as stakeholders need to understand the rationale behind model predictions and decisions (Zand et al., 2020). Financial institutions should maintain comprehensive documentation detailing the development, deployment, and operation of deep learning models for AML. Transparent documentation enables regulatory authorities to assess the compliance of AML efforts and ensures accountability for model decisions (Thommandru et al., 2023).

By addressing regulatory challenges through transparent model architecture, compliance by design, data minimization, regular auditing, and documentation, the proposed deep learning models can ensure compliance with global AML regulations and data privacy laws. These measures help financial institutions deploy AML solutions that are effective, transparent, and compliant with regulatory standards (Thommandru et al., 2023).

POTENTIAL FOR FURTHER RESEARCH

AI holds immense potential for revolutionizing the detection and prevention of financial crimes. AI and ML algorithms are becoming increasingly sophisticated in identifying patterns and anomalies indicative of ML activities. Future advancements may include the integration of advanced neural networks, deep learning techniques, and NLP to improve detection accuracy and reduce false positives (Youssef et al., 2023). AI-driven predictive analytics can anticipate suspicious activities by analyzing vast amounts of data in real-time. This proactive approach enables financial institutions to identify potential ML schemes before they escalate, allowing for timely intervention and mitigation (Sobh, 2020). AML regulations are continually evolving to address emerging risks and challenges. AI-powered compliance solutions can automate regulatory reporting, transaction monitoring, and CDD processes, ensuring adherence to complex regulatory requirements while minimizing manual effort and errors (Sobh, 2020).

The integration of behavioral biometrics, such as keystroke dynamics and mouse movements, into AML systems adds an extra layer of security by authenticating users based on their unique behavioral patterns. This helps prevent identity theft and unauthorized access to financial accounts, thereby mitigating ML risks (Zia et al., 2022). The adoption of blockchain technology in AML frameworks offers transparent and immutable transaction records, facilitating traceability and auditability of financial transactions. AI algorithms can analyze blockchain data to detect suspicious patterns and identify potential ML activities within decentralized networks (Zia et al., 2022). A collaborative approach involving information sharing and cooperation among financial institutions, regulatory agencies, and law enforcement entities is crucial for combating ML effectively. AI-driven platforms can facilitate secure data exchange and collaboration, enabling stakeholders to leverage collective intelligence in identifying and disrupting criminal activities (Pazos et al., 2024).

Regulatory bodies are likely to impose stricter AML regulations and standards to keep pace with evolving ML techniques and emerging threats. This includes mandating the use of advanced AI/ML technologies, conducting regular audits and assessments, and promoting industry-wide best practices to ensure compliance and effectiveness in combating financial crimes (Pazos et al., 2024). As criminals evolve their ML tactics using sophisticated techniques, there is a pressing need for continuous innovation and adaptation in AML strategies. Financial institutions and regulatory agencies must invest in research and development to stay ahead of emerging threats, enhance detection capabilities, and deploy robust defense mechanisms against evolving ML schemes (Zia et al., 2022).

In summary, the future of AI/ML in AML holds tremendous promise for improving detection accuracy, enhancing regulatory compliance, and combating financial crimes effectively. However, staying ahead of evolving ML techniques employed by criminals requires continuous innovation, collaboration, and regulatory oversight to safeguard the integrity of the financial system and protect against illicit activities.

CONCLUSION

This article has provided a comprehensive examination of the challenges and opportunities of combating ML by OCGs within banking channels in South Asia. Through its analysis of AML regimes in South Asian countries and the measures undertaken to address ML within domestic jurisdictions, we see that despite existing regulatory frameworks, OCGs continue to exploit vulnerabilities within banking systems to launder illicit funds (Delle-Case et al., 2018). There is an urgent need for enhanced detection and prevention mechanisms.

In the relentless battle against ML in South Asia, deep learning has emerged as a powerful ally for law enforcement agencies. Its capacity to analyze vast datasets, recognize patterns, and adapt to evolving criminal strategies positions it as a transformative force in strengthening the resilience of financial systems against illicit activities (Jensen & Iosifidis, 2023b). As South Asian nations continue to confront the complex challenges posed by organized crime, the integration of AI technologies stands as a beacon of hope in the pursuit of a secure and transparent financial future.

In response to this imperative, this article has investigated how deep learning techniques and models can be applied to bolster AML efforts within financial institutions. By leveraging advanced computational methods, such as deep learning, banking institutions can significantly enhance their ability to identify suspicious transactions and mitigate risks associated with ML (Kute et al., 2021). However, the adoption of deep learning techniques for combating ML is not without its challenges. This article has highlighted key obstacles, including concerns related to data privacy, model interpretability, and regulatory compliance. Addressing these challenges will be paramount to the successful implementation of deep learning solutions within existing AML frameworks (Hoofnagle et al., 2019).

Combating ML by OCGs in banking channels demands a multifaceted approach that combines regulatory reform, technological innovation, and collaboration between financial institutions and law enforcement agencies. Moving forward, it is imperative for policymakers, regulators, and industry stakeholders to work together to strengthen AML measures, harness the potential of emerging technologies like deep learning, and adapt to the evolving tactics of OCGs in order to safeguard the integrity of the financial system and protect society from the deleterious effects of ML. Only through concerted and coordinated efforts can we effectively combat the scourge of ML and uphold the principles of transparency, accountability, and integrity in the global financial ecosystem.

FUNDING & DISCLOSURES

The authors report no funding by any person or organization nor any competing interests to declare.

REFERENCES

- Ahmad, A. (2023). A Critical Examination of India's Concerns and Responses to the Financing of Global Terrorism. *African Journal of Terrorism and Insurgency Research*, 4(2), 9.
- Alexandre, C.R., & Balsa, J. (2023). Incorporating machine learning and a risk-based strategy in an anti-money laundering multiagent system. *Expert Systems with Applications*, 217, 119500. <https://doi.org/10.1016/j.eswa.2023.119500>
- Alkhalili, M., Qutqut, M. H., & Almasalha, F. (2021). Investigation of applying machine learning for watch-list filtering in anti-money laundering. *IEEE Access*, 9, 18481-18496. <https://doi.org/10.1109/ACCESS.2021.3052313>
- Alotibi, J., Almutanni, B., Alsubait, T., Alhakami, H., & Baz, A. (2022). Money Laundering Detection using Machine Learning and Deep Learning. *International Journal of Advanced Computer Science and Applications*, 13(10). <https://doi.org/10.14569/IJACSA.2022.0131087>
- Asia/Pacific Group on Money Laundering. (2021). *Sri Lanka's progress in strengthening measures to tackle money laundering and terrorist financing*. <https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-fur/APG-Follow-Up-Report-Sri-Lanka-2021.pdf.coredownload.inline.pdf>
- Asia/Pacific Group on Money Laundering. (2023). *Anti-money laundering and counter-terrorist financing measures - Nepal*. <https://apgml.org/members-and-observers/members/member-documents.aspx?m=a6c4a803-0e15-4a43-b03a-700b2a211d2e>
- Biswakarma, G., & Bhusal, P. (2023). Banks' Level Factors Affecting the Effective Implementation of Anti-Money Laundering Practices in Nepalese Banks: An Employee and Customer Perspectives. *South Asian Journal of Finance*, 3(1), 1-22. <https://doi.org/10.4038/sajf.v3i1.53>
- Bui, D.T., Tsangaratos, P., Nguyen, V.-T., Van Liem, N., & Trinh, P.T. (2020). Comparing the prediction performance of a Deep Learning Neural Network model with conventional machine learning models in landslide susceptibility assessment. *Catena*, 188, 104426.
- Canhoto, A. I. (2021). Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research*, 131, 441-452. <https://doi.org/10.1016/j.jbusres.2020.10.012>
- Central Bank of Myanmar. (2022). *Regulatory and Supervisory Framework for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT)*. https://www.cbm.gov.mm/sites/default/files/regulate_launder/regulatory_and_supervisory_framework_for_aml-cft.pdf
- Chen, Z., Van Khoa, L.D., Teoh, E.N., Nazir, A., Karuppiah, E.K., & Lam, K.S. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: a review. *Knowledge and Information Systems*, 57, 245-285. <https://doi.org/10.1007/s10115-017-1144-z>

- Chief Executive Officer of AUSTRAC. (2022). *Statement of Claim* [Press release]. https://www.austrac.gov.au/sites/default/files/2022-03/20220301_Statement_of_Claim_stamped_0.pdf
- Dalla Pellegrina, L., Di Maio, G., Masciandaro, D., & Saraceno, M. (2020). Organized crime, suspicious transaction reporting and anti-money laundering regulation. *Regional Studies*, 54(12), 1761-1775. <https://doi.org/10.1080/00343404.2020.1772963>
- Delle-Case, A., Bailey, N., Carr, B., & Ekberg, M. (2018). Machine learning in anti-money laundering – Summary report. *Institute of International Finance*, 1-10.
- Domashova, J., & Mikhailina, N. (2021). Usage of machine learning methods for early detection of money laundering schemes. *Procedia Computer Science*, 190, 184-192. <https://doi.org/10.1016/j.procs.2021.06.033>
- Faccia, A., Moşteanu, N.R., Cavaliere, L.P.L., & Mataruna-Dos-Santos, L.J. (2020). Electronic money laundering, the dark side of fintech: An overview of the most recent cases. In *Proceedings of the 2020 12th International Conference on Information Management and Engineering* (pp. 29-34). <https://doi.org/10.1145/3430279.3430284>
- FATF. (2023). High-Risk Jurisdictions subject to a Call for Action - October 2023. <https://www.fatf-gafi.org/content/fatf-gafi/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-october-2023.html>
- Financial Intelligence Unit of Sri Lanka. (2022). *National Money Laundering and Terrorist Financing Risk Assessment of Sri Lanka 2021/2022*. https://fiusrilanka.gov.lk/docs/Other/NRA_Report_2021_22/Part_2_1.pdf
- Financial Intelligence Unit of Sri Lanka. (2023). *National Policy on Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) of Sri Lanka, 2023-2028*. https://irsl.gov.lk/wp-content/uploads/2023/09/National_AML_CFT_Policy_2023-2028.pdf
- Ganapathy, N. (2020). Organized Crime in Asia. In *Oxford Research Encyclopedia of Criminology and Criminal Justice*. <https://doi.org/10.1093/acrefore/9780190264079.013.577>
- Gupta, T., Wadkar, D., Shinde, T., Kunjeer, S., & Deokar, A. (2024). Decentralized E-KYC Blockchain Network for Central Bank. *International Journal for Research in Applied Science & Engineering Technology*, 11(3), 2005-2013. <https://doi.org/10.22214/ijraset.2023.49860>
- Han, J., Barman, U., Hayes, J., Du, J., Burgin, E., & Wan, D. (2018). NextGen AML: Distributed deep learning based language technologies to augment anti money laundering investigation. In *Proceedings of ACL 2018, System Demonstrations* (pp. 37-42). Association for Computational Linguistics.
- Hendeniya, H., Premarathna, W., & Tennekoon, S. (2023). The Effect of Corruption and Money Laundering on Banking Profitability and Stability of Licensed Commercial Banks in Sri Lanka. *Journal of Business and Technology*, 7(2), 33-55. <https://doi.org/10.4038/jbt.v7i2.98>
- Hoofnagle, C.J., Van Der Sloot, B., & Borgesius, F.Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, 28(1), 65-98. <https://doi.org/10.1080/13600834.2019.1573501>

- International Narcotics Control Board. (2022). *Report of International Narcotics Control Board for 2021*. <https://www.incb.org/incb/en/publications/annual-reports/annual-report-2021.html>
- Jain, M. (2023). Money Laundering in India: A Multi-Dimensional Advent. *Justice and Law Bulletin*, 2(2), 51-60.
- Jamal, E.O. (2022, July 2). Bangladesh's struggles with money laundering. *The Daily Star*. <https://www.thedailystar.net/opinion/the-overton-window/news/bangladeshs-struggles-money-laundering-1923629>
- Jan, J. (2021). Money-Laundering in Pakistan: Methods and means of Money Laundering and its connection with Terror Financing. *Current Trends in Law and Society*, 1(1), 1-7. <https://doi.org/10.52131/clts.2021.0101.0001>
- Jensen, R.I.T., & Iosifidis, A. (2023a). Fighting money laundering with statistics and machine learning. *IEEE Access*, 11, 8889-8903. <https://doi.org/10.1109/ACCESS.2023.3239549>
- Jensen, R.I.T., & Iosifidis, A. (2023b). Qualifying and raising anti-money laundering alarms with deep learning. *Expert Systems with Applications*, 214, 119037.
- Kabra, S., & Gori, S. (2023). Drug trafficking on cryptomarkets and the role of organized crime groups. *Journal of Economic Criminology*, 2, 100026. <https://doi.org/10.1016/j.jeconc.2023.100026>
- Korauš, A., Gombár, M., Kelemen, P., & Backa, S. (2019). Using quantitative methods to identify insecurity due to unusual business operations. *Entrepreneurship and Sustainability Issues*, 6(3), 1101. [https://doi.org/10.9770/jesi.2019.6.3\(3\)](https://doi.org/10.9770/jesi.2019.6.3(3))
- Kurshan, E., Shen, H., & Yu, H. (2020). *Financial crime & fraud detection using graph computing: Application considerations & outlook* [Paper presentation]. Second International Conference on Transdisciplinary AI (TransAI). <https://doi.org/10.48550/arXiv.2103.01854>
- Kute, D.V. (2022). *Explainable Deep Learning Approach for Detecting Money Laundering Transactions in Banking System*. University of Technology, Sydney.
- Kute, D.V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep learning and explainable artificial intelligence techniques applied for detecting money laundering—a critical review. *IEEE Access*, 9, 82300-82317.
- Labanca, D., Primerano, L., Markland-Montgomery, M., Polino, M., Carminati, M., & Zanero, S. (2022). Amaretto: An active learning framework for money laundering detection. *IEEE Access*, 10, 41720-41739.
- Langdale, J. (2023). Money laundering in Australian casinos. *Journal of Money Laundering Control*, 26(7), 99-109. <https://doi.org/10.1108/JMLC-09-2022-0136>
- Levi, M., & Soudijn, M. (2020). Understanding the laundering of organized crime money. *Crime and Justice*, 49(1), 579-631. <https://doi.org/10.1086/708047>
- Lokanan, M.E. (2022). Predicting money laundering using machine learning and artificial neural networks algorithms in banks. *Journal of Applied Security Research*, 19(1), 20-44.
- Manning, M., Wong, G.T., & Jevtovic, N. (2021). Investigating the relationships between FATF recommendation compliance, regulatory affiliations and the Basel Anti-Money Laundering Index. *Security Journal*, 34, 566-588. <https://doi.org/10.1057/s41284-020-00249-z>

- Mashrur, A., Luo, W., Zaidi, N.A., & Robles-Kelly, A. (2020). Machine learning for financial risk management: a survey. *IEEE Access*, 8, 203203-203223. <https://doi.org/10.1109/ACCESS.2020.3036322>
- Maxwell, W., Bertrand, A., & Vamparys, X. (2020). *Are AI-based Anti-Money Laundering (AML) Systems Compatible with European Fundamental Rights?* [Paper presentation]. ICML 2020 Law and Machine Learning Workshop.
- Momo, S.I. (2021). *Mechanism and effects/impacts of money laundering in Bangladesh: preventive measures at Dhaka Bank's AML-CFT department.*
- Morshed, M.M., & Rahman, T. (2021). *The Phenomenon of Trade-Based Money Laundering in Bangladesh - A Critical Review.* <https://doi.org/10.31235/osf.io/gw9qd>
- Mukhtar, A. (2018). Money laundering, terror financing and FATF: Implications for Pakistan. *Journal of Current Affairs*, 3(1), 27-56.
- Nazar, S., Raheman, A., & Anwar ul Haq, M. (2023). The magnitude and consequences of money laundering. *Journal of Money Laundering Control.* <https://doi.org/10.1108/JMLC-09-2022-0139>
- Nimma, S. (2022). Money Laundering in the Cyberworld: Emerging Trends. *Indian Journal of Integrated Research in Law*, 2(2), 1. <https://ijirl.com/wp-content/uploads/2022/03/MONEY-LAUNDERING-IN-THE-CYBERWORLD-EMERGING-TRENDS.pdf>
- Nishant, S., Virangana, W., & Shukla, B. (2023). *India FATF: An India Perspective.* <https://www.mondaq.com/india/money-laundering/1328958/fatf-an-india-perspective>
- Nwe Oo, & Yuwadee Thean-Ngarm. (2022). *Myanmar: Myanmar Blacklisted By The FATF.* <https://www.mondaq.com/financial-services/1246052/myanmar-blacklisted-by-the-fatf>
- Oeben, M., Goudsmit, J., & Marchiori, E. (2019, August 12). *Prerequisites and AI challenges for model-based Anti-Money Laundering* [Paper presentation]. AI for Social Good - IJCAI 2019 Workshop, Macao.
- Pandey, D. (2023). A comparative analysis of the FIUs and FATF compliance of Canada, Australia, The Netherlands and India. *Journal of Money Laundering Control.* <https://doi.org/10.1108/JMLC-09-2023-0155>
- Parne, P. (2021). Artificial Intelligence & Machine Learning Role in Financial Services, *CS & IT Conference Proceedings*, 11(15), 37-42.
- Paula, E.L., Ladeira, M., Carvalho, R.N., & Marzagão, T. (2016). Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering. *2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 954-960. <https://doi.org/10.1109/ICMLA.2016.0172>
- Pazos, J.F.M., González, J.G., Lorenzo, D.B., & Morales, J.A.R. (2024). Fraud Transaction Detection For Anti-Money Laundering Systems Based On Deep Learning. *Journal of Emerging Computer Technologies*, 3(1), 29-34. <https://doi.org/10.57020/ject.1428146>
- Press Trust of India. (2022, June 9). Money laundering: 25 people convicted in India till now. *Times of India.* <https://economictimes.indiatimes.com/news/india/money-laundering-25-people-convicted-in-india-till-now/articleshow/92107517.cms?from=mdr>

- Raiter, O. (2021). Applying supervised machine learning algorithms for fraud detection in anti-money laundering. *Journal of Modern Issues in Business Research*, 1(1), 14-26.
- Rana, S., & Awwal, M.R. (2020). Reasons behind Money Laundering and Ways to Controlling it in Bangladesh. *Canadian Journal of Business and Information Studies*, 2(6), 157-169. <https://doi.org/10.34104/cjbis.020.01570169>
- Richardson, B., Williams, D., & Mikkelsen, D. (2019). *Network analytics and the fight against money laundering*. <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/network-analytics-and-the-fight-against-money-laundering>
- Royal Monetary Authority of Bhutan. (2018a). *Anti-money laundering and combating the financing of Terrorism Rules and Regulations*, 2018.
- Royal Monetary Authority of Bhutan. (2018b). *National Money Laundering and Financing of Terrorism Risk Assessment*. <https://www.rma.org.bt/RMA%20Publication/NRAReports/NRAonMLFT.pdf>
- Schloenhardt, A., Calderoni, F., Lelliott, J., & Weißer, B. (2023). *UN Convention against Transnational Organized Crime: A Commentary*. Oxford University Press.
- Shokry, A.M., Rizka, M.A., & Labib, N.M. (2020). Counter terrorism finance by detecting money laundering hidden networks using unsupervised machine learning algorithm. In *Proceedings of the International Conferences on ICT, Society and Human Beings (ICT 2020), Connected Smart Cities (CSC 2020) and Web Based Communities and Social Media (WBC 2020)* (pp. 89-97). <https://www.iadisportal.org/digital-library/mdownload/counter-terrorism-finance-by-detecting-money-laundering-hidden-networks-using-unsupervised-machine-learning-algorithm>
- Silva, Í.D.G., Correia, L.H.A., & Maziero, E.G. (2023, May 29). Graph Neural Networks Applied to Money Laundering Detection in Intelligent Information Systems. *Simpósio Brasileiro de Sistemas de Informação (SBSI)*. *Simpósio Brasileiro de Sistemas de Informação (SBSI)*. <https://sol.sbc.org.br/index.php/sbsi/article/view/25139>
- Sivaguru, D., & Tilakasiri, K. (2023). The phenomenon of trade-based money laundering (TBML) – a critical review in Sri Lankan context. *Journal of Money Laundering Control*, 26(6), 1088–1099. <https://doi.org/10.1108/JMLC-10-2022-0151>
- Sobh, T.S. (2020). An intelligent and secure framework for anti-money laundering. *Journal of Applied Security Research*, 15(4), 517-546. <https://doi.org/10.1080/19361610.2020.1812994>
- Sullivan, T., Smith, J., Ombler, F., & Brayley-Morris, H. (2020). Prioritising the investigation of organised crime. *Policing and Society*, 30(3), 327-348. <https://doi.org/10.1080/10439463.2018.1533961>
- Sultan, N., & Mohamed, N. (2023). The role of information sharing in combating money laundering: the importance and challenges of mutual legal assistance for developing jurisdictions like Pakistan. *Journal of Money Laundering Control*, 26(6), 1242-1260. <https://doi.org/10.1108/JMLC-09-2022-0128>

- Tertychnyi, P., Godgildieva, M., Dumas, M., & Ollikainen, M. (2022). Time-aware and interpretable predictive monitoring system for Anti-Money Laundering. *Machine Learning with Applications*, 8, 100306. <https://doi.org/10.1016/j.mlwa.2022.100306>
- Thommandru, A., Mone, V., Mitharwal, S., & Tilwani, R. (2023). *Exploring the intersection of machine learning, money laundering, data privacy, and law* [Paper presentation]. 2023 International Conference on Innovative Data Communication Technologies and Application.
- Tiwari, M., Gepp, A., & Kumar, K. (2020). A review of money laundering literature: the state of research in key areas. *Pacific Accounting Review*, 32(2), 271-303. <https://doi.org/10.1108/PAR-06-2019-0065>
- United Nations Office on Drugs and Crime. (2024). *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*. https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf
- Upadhyay, A. (2024). Financial opacity and financial secrecy: lessons for Nepal. *Journal of Money Laundering Control*, 27(2), 383-394. <https://doi.org/10.1108/JMLC-03-2023-0049>
- Watkins, R.C., Reynolds, K.M., Demara, R., Georgiopoulos, M., Gonzalez, A., & Eaglin, R. (2020). Tracking dirty proceeds: exploring data mining technologies as tools to investigate money laundering. *Police Practice and Research*, 4(2), 163-178. <https://doi.org/10.1080/15614260308020>
- Weber, M., Chen, J., Suzumura, T., Pareja, A., Ma, T., Kanezashi, H., Kaler, T., Leiserson, C. E., & Schardl, T. B. (2018). Scalable Graph Learning for Anti-Money Laundering: A First Look (arXiv:1812.00076). *arXiv*. <https://doi.org/10.48550/arXiv.1812.00076>
- Youssef, B., Bouchra, F., & Brahim, O. (2023, March 5-7). State of the Art Literature on Anti-money Laundering Using Machine Learning and Deep Learning Techniques. In *The 3rd International Conference on Artificial Intelligence and Computer Vision* (pp. 77-90). http://dx.doi.org/10.1007/978-3-031-27762-7_8
- Yusoff, Y.H., Azlan, N.A.F., Zamzuri, N.N.M., Sufian, N., Kurniawan, S.N.R., & Hassan, R. (2023). Areas of Technology That Helps in Combating Money Laundering: A Concept Paper. *Journal of Academic Research in Business and Social Sciences*, 13(5), 949-959. <https://doi.org/10.6007/IJARBSS/v13-i5/16588>
- Zafarullah, H., & Haque, H. (2023). Policies, instrumentalities, compliance and control: combatting money laundering in Bangladesh. *Journal of Money Laundering Control*, 26(1), 189-204. <https://doi.org/10.1108/JMLC-10-2021-0109>
- Zand, A., Orwell, J., & Pfluegel, E. (2020, June 15-19). *A secure framework for anti-money-laundering using machine learning and secret sharing* [Paper presentation]. 2020 International Conference on Cyber Security and Protection of Digital Services, Dublin, Ireland. <https://doi.org/10.1109/CyberSecurity49315.2020.9138889>
- Zia, M.A., Abbas, R.Z., & Arshed, N. (2022). Money laundering and terror financing: issues and challenges in Pakistan. *Journal of Money Laundering Control*, 25(1), 181-194. <https://doi.org/10.1108/JMLC-11-2020-0126>