Intelligent Anti-Money Laundering System*

Shijia Gao, Dongming Xu, Huaiqing Wang, and Yingfeng Wang

Abstract—Criminal elements in today’s technology-driven society are using every means available at their disposal to launder the proceeds from their illegal activities. While many anti-money laundering solutions have been in place for some time within the financial community, they cannot adapt to the ever-changing risk and methods in relation to money laundering. In order for a more adaptive, intelligent and flexible solution for anti-money laundering, the intelligent agent technology is applied in this research. Intelligent agents with their properties of autonomy, reactivity and proactivity are well suited for money laundering prevention controls. Several types of agents are proposed and a novel and open multi-agent architecture is presented for anti-money laundering. A prototype system for money laundering detection is also developed to demonstrate the advances of the proposed system architecture and business value.

Index Terms—Anti-money laundering, Artificial intelligence application, Intelligent agents.

I. INTRODUCTION

Since the mid-1980s, money laundering (ML) has been increasingly recognized as a significant global problem, with serious economic and social ramifications [1]. Today, ML has become a key funding mechanism for international religious extremism and drug trafficking, and curtailing these illegal activities has become an important focus of governments as part of their ongoing wars on terrorism and drug abuse. Following the terrorist activity on September 11, 2001, there has been an increased focus in the United States and across the globe on the prevention of ML and terrorist financing.

Increasingly, anti-money laundering (AML) systems are being implemented to combat ML. However, the traditional rule-based solutions suffer from a number of drawbacks, such as ineffective thresholds, high false positive problem, lack of pattern recognition function, and insufficient data processing capability. In this research, we apply intelligent agent technology to ML prevention controls by taking advantage of agent’s autonomy, reactivity, proactivity, and social ability.

The organization of this paper is as follows. Next section briefly reviews the relevant literature on ML, AML, AML systems, and intelligent agent. Section III presents the architecture, development, and operation of a multi-agent-based AML system. The final section addresses some conclusions as well as the future work.

II. BACKGROUND

A. Money Laundering and Anti-Money Laundering

Money laundering (ML) is a term usually used to describe the ways in which criminals process illegal or “dirty” money derived from the proceeds of any illegal activity (e.g. the proceeds of drug-dealing, human trafficking, fraud, theft or tax evasion) through a succession of transfers and deals until the source of illegally acquired funds is obscured and the money takes on the appearance of legitimate or “clean” funds or assets [2]. ML is a diverse and often complex process that need not involve cash transactions. ML basically involves three independent steps that can occur simultaneously [3]:

- Placement – the process of transferring the proceeds from illegal activities into the financial system in such a manner as to avoid detection by financial institutions and government authorities.
- Layering – the process of generating a series or layers of transactions to distance the proceeds from their illegal source and obscure the audit trail.
- Integration – the unnoticed reinsertion of successfully laundered, untraceable proceeds into an economy.

The International Monetary Fund (IMF) estimates that the aggregate size of ML in the world could be somewhere between 2 and 5 percent of global gross domestic product (GDP), equivalent to approximately US$590 billion to US$1.5 trillion annually. According to Celent Communications, the amount of illicit funds traveling through ML channels is estimated to reach over US$926 billion worldwide by the end of 2005, and grow at an annual rate of 2.7%. However, those are just estimates – the full magnitude of the problem is still not known with any certainty.

Recent years have witnessed a growing number of highly publicized money laundering scandals involving major

* This research is supported by a strategic research grant (No. 7001805) from the City University of Hong Kong.
B. Anti-Money Laundering Systems

In an effort to detect potential ML schemes, many financial institutions have deployed AML detection solutions and enterprise-wide procedural programs. The solutions worked by establishing fixed rule-based thresholds by analyzing how certain established usage scenarios comply within those boundaries. Most financial institutions will establish a threshold based on a set monetary value for each transaction and detecting specific ML patterns and user scenarios that breached those thresholds. The shortcomings associated with those solutions are summarized as follows:

- Those solutions have an inherent inability to detect ML schemes of smaller amounts that may come in under a defined threshold limit. For instance, in investigating the financing behind the events of 9/11, the terrorists have been discovered frequent transactions of small sums that are below the usual cash transaction reporting thresholds.
- Problem of false positive, which means there are transactions over a set limit that are marked as suspicious but that do not represent any existing identified risk to the institution.
- Those solutions have had difficulty detecting ML schemes by using current industry information to profile and confirm certain patterns of suspicious laundering activities.
- Although those rule-based systems have some pattern recognition capabilities, they do not have learning or generalization abilities and can only match patterns that they already know. As new ML schemes developed, many of these solutions were unable to uncover them, providing criminals with new avenues to circumvent detection and the law.
- Transaction volumes in the financial instructions are very large and are increasing. Those existing systems do not have enough capabilities to check every transaction in a comprehensive and consistent manner. Too few checks are costly in terms of undetected ML activities.

ML detection and prevention is notoriously difficult. The complex nature of financial products, services, and ML itself, ML is dynamic and adapts over time according to changing conditions. Patterns of behavior change as money launderers become aware of the techniques being used to combat them. Given such behavior, there are no set rules that can be applied to detect patterns of ML. Fixed rules can be applied to mitigate against certain extreme behaviors and to enforce defined regulations. However, embedding static rule-based systems into electronic transaction environments does not provide adequate safeguards to combat ML. It is therefore vital to tackle the problem using technology that adapts, so that systems can be dynamic in the way that they respond to changes in the patterns of ML.

C. Intelligent Agents

The development of intelligent agents (IAs) and multi-agent systems (MASs) has recently gained popularity among IS researchers. Although there is no universally accepted definition of the term “agent,” and indeed there is a good deal of ongoing debate and controversy on this very subject, the central point of agents is that they are autonomous: capable of acting independently, exhibiting control over their internal state. Wooldridge and Jennings suggest a precise description of agents; one that may be widely adopted in artificial intelligence communities as well as general computing areas. An agent is defined as a computer system that is situated in some environment, and is capable of autonomous action in that environment in order to meet its design objectives. Furthermore, agents are able to act without the intervention of humans or other systems: they have control both over their own internal state, and over their behavior. An intelligent agent (IA) is one that is capable of flexible autonomous action in order to meet its design objectives, where flexibility includes properties such as autonomy, social capability, reactivity, and proactivity. A generic agent has a set of goals, certain capabilities to perform tasks, and some knowledge about its environment.
To achieve its goals, an agent needs to use its knowledge to reason about its environment and the behaviors of other agents, to generate plans and to execute these plans.

A MAS consists of a group of agents, interacting with one another to collectively achieve their goals. By absorbing other agents’ knowledge and capabilities, agents can overcome their inherent bounds of intelligence [11]. One of the current factors (and arguably one of the more important ones) fostering MAS development is the increasing popularity of the Internet, which provides the basis for an open environment where agents interact with each other to reach their individual or shared goals.

In recent years, there has been considerable growth of interest in the design of a distributed, intelligent society of agents capable of dealing with complex problems and vast amounts of information collaboratively. Since agent technology provides flexible, distributed, and intelligent solutions for business applications, researchers have proposed to design and develop numerous intelligent-agents based business systems [12]–[14]. The main benefits of an agent-based approach come from its flexibility, adaptability, and decentralization.

III. INTELLIGENT ANTI-MONEY LAUNDERING SYSTEM

Our intelligent anti-money laundering system (IAMLs) provides the ability to monitor every single financial transaction, discovering unusual behavior, and separating out those transactions that are determined to represent a true risk for the financial institutions. The IAMLs is able to learn and adapt, comprehending new ML schemes as they arise. It takes an enterprise-wide approach, determining every transaction that is unusual as opposed to looking for specific patterns or behaviors while analyzing both the client profile and the transactions undertaken by the financial firm. The analysis and design of a novel agent-based IAML is described in this section.

A. Deployment of Intelligent Agents

Besides being complex, AML is also a kind of collaboration process, in which multiple organizations and a mixture of human activities and automated tasks are involved. In order to design the architecture of a multi-agent AML solution, we decomposed the process of AML into several autonomous phases, in which each agent is delegated a particular task to exhibit its goal-oriented and reactive behavior, and cooperate with others to pursue their goals. The process of AML usually consists of the phases of data collecting, ML risk monitoring, behavior diagnosing, and suspicious activity reporting. Furthermore, data collecting involves internal and external data collection, while ML monitoring is composed of client profile assessment and transaction risk measurement. Accordingly, the taxonomy of intelligent agent for AML is outlined in Figure 1, in which several intelligent agent classes are applied to provide a set of AML functionalities for existing financial institutions. The details of these agents are described in the following subsection.

![Figure 1. Agent hierarchy for anti-money laundering](image)

B. System Architecture

The value of any AML solution has to be based on its ability to uncover suspicious financial activities by identifying the specific individuals or organizations that may be involved [15]. However, given the complex nature of ML prevention controls, an automated solution cannot attach suspicion to any activity detected – it can only detect activity worthy of analyst interpretation. Human ML expertise is required to determine if that activity is suspicious and worthy of reporting. Therefore, the optimum way to implement ML prevention controls is as a synthesis of human expertise and automated intelligence. In this research, the automated system performs the detection work, raising alerts for transaction deemed suspicious, while the human analysts perform investigation into the cases that are raised.

There are two ways to develop the AML solution: we can reengineer existing financial systems to support AML functions, or develop an independent AML system to link with the existing applications through which all client and transaction data would pass during its lifecycle. The existing financial systems are distributed in various institutions, e.g., banks, insurance companies, security trading firms. Our work is to fundamentally use internal resources to build software capabilities to interact with legacy systems.

Based on the analysis above and the deployment of intelligent agents in the previous subsection, the architecture of the IAMLs is portrayed in Figure 2, which describes the internal interactions among agents and the external relationship between the IAMLs and existing financial systems.
The agents are distributed in financial organizations or departments involved in AML; they communicate with each other through the Internet. As related before, all these agents work autonomously and collaboratively in the multi-agent environment. Each agent focuses on its particular task without inventions from outside. And by drawing on other agents’ knowledge and capabilities, agents can overcome their inherent bounds of intelligence and work collaboratively to pursue their goals.

The User Agent enables users to view the current state of the financial transactions and ML monitoring, diagnosing, and reporting processes and allows them to convey their own judgments, opinions, and arguments relative to ML detection to the rest of financial institution. The agent also enables the corresponding users to issue requests to the other agents in the system.

The Data Collecting Agents enable the system to collect data internally and externally. In particular, the Internal Data Collecting Agent is in charge of acquiring real-time data from existing financial systems for the client profile assessment, transaction risk measurement, and further behavior diagnosis and reporting. Several kinds of data related to possible ML schemes are required for ML prevention controls, such as client profiles, financial transaction details, account reference data, client reference data, historical statistics, etc. On the other hand, the External Data Collecting Agent retrieves open data from ML watchdog agencies, national government, and other authorities. The data includes international standards, official thresholds, watch list, legislations, etc. All the other Monitoring Agents, Diagnosing Agent, and Reporting Agent may request data relating to their task from the Data Collecting Agents, if required.

Two kinds of Monitoring Agents include Client Profile Monitoring Agent and Transaction Monitoring Agent, are proposed in our system to monitor potential ML schemes on a client-by-client, transaction-by-transaction basis. Both agents comply with the global-accepted core policy for effective ML controls – KYC (KnowYourCustomer).

- The Client Profile Monitoring Agent is to assess a wide variety of detailed information relating to the client’s account, typically collected at the time that the account is opened. The agent provides a single view of the client profile incorporating all of the various financial relationships that the account has an affiliation with. The types of analytical activities that are part of the agent client profiling processes include, but are not limited to: watch list name screening, high risk country alerting, financial source or channels, business relationship, and political affiliation. Each client is classified into different risk profiles. And based on the client risk classification, the agent determines the frequency and the intensity of monitoring.
- The Transaction Monitoring Agent is to identify transactions that pose the greatest risk for potential
ML activities. Transaction determined to be of a higher risk can vary from organization to organization based on their lines and types of business. For instance, the risk associated with transactions from a bank would be different from those associated with an insurance agency or a securities firm. In general, the transaction risk behavior include, also not limit to [15]: rapid movement of funds in or out of the account, sudden activity into a previously dormant account, frequent changes to an account, recurring transactions, hidden account relations, offsetting trades, settlement and/or standing instructions of an account, the movement of funds without a corresponding trade, and the deposit of excess collateral into an account.

Normally, if a questionable client profile or an unusual transaction is captured by the Monitoring Agents, a risk report will be issued and sent to the Behavior Diagnosing Agent for further investigation. However, an emergent suspicious activity report (SAR) could be issued to be reported to the user for instant action. When receiving the risk reports from Monitoring Agents, the Behavior Diagnosing Agent will start its diagnosing process to investigate the complex behavior that is commonly associated with ML schemes. This agent may conduct analysis on risk reports from Monitoring Agents and request any additional information if necessary to examine the cases. The agent allows financial institutions to detect wrongdoing by finding suspicious patterns of behavior that may be hidden behind large volumes of financial data. It is also able to identify suspicious events and entities that build over time, thereby separating them from every day events and transactions in order to target the offending behavior.

When the Behavior Diagnosing Agent identified unusual or suspicious behavior, a suspicious activity report (SAR) will be automatically produced and sent to the Reporting Agent (RA). Then the RA will present and communicate a potential ML alert to the appropriate compliance personnel through the User Agent for case management investigation and action. Alternatively the RA will automate or take a specific course of action, for example, interfering with standard operations to block a particular suspicious transaction. Cases for investigation are filtered and prioritized based on the severity of the alert. The RA is able to support the business process to assist with suspicious case investigation. It does this by providing evidence of client activity and information, ensuring the case officer has all of the relevant customer intelligence at hand. If necessary, additional information is requested from Behavior Diagnosing Agent. This allows them to make a fact based decision and it also demonstrates regulatory due diligence in the process. The RA also facilitates combining the automatically generated alerts with suspect manual reports, to build the case for investigation. The reporting facilities within the RA provide a complete tracking system and audit trail for managing actions in response to detected events or suspicious behavior. Such comprehensive reporting allows the financial institutions to demonstrate compliance to the AML rules and adherence to the regulatory requirements.

C. System Operation

In order to evaluate our architectural design, a prototype has been implemented. The prototype system carries out the analysis, monitoring, diagnosing, and reporting using simulated client profile and financial transaction data based on a small number of intelligent agents.

Within our prototype, the Data Collecting Agents continuously collect relevant simulated client and transaction data in real time, automatically response to any data request from other agents in a timely manner. The Monitoring Agents and Behavior Diagnosing Agent are pre-configured with detailed ML scenarios. These scenarios are patterns of behavior that are of interest to the organization and based on the Regulator’s compliance rules (e.g., FATF 40 Recommendations). The scenarios are adaptable and can easily be extended. The agents have the flexibility to allow the organizations to incorporate their own specific business scenarios reflecting their security practices. In addition, various advanced techniques are combined into a holistic, risk-based approach. By evaluating other risk factors, the most relevant alerts are raised. With a risk-based approach, a combination of rules, anomaly detection, neutral network, fuzzy logic, linear programming are employed and assigned a risk weighting. For each scenario, scores are assigned to each risk factor, and then multiplied by the risk weighting to get the overall scores. By so doing, financial organization is able to more effectively evaluate the subtle patterns of ML in the context of other existing risk attributes. When dealing with previously unseen patterns, these agents are able to remember the patterns, for future reference, and make generalization about them. In this way, they can adapt to different inputs and produce findings on both previously seen and previously unseen patterns. The User Agent provides the interface to the user, who may be a ML analyst. It communicates and cooperates with other agents, automatically executes its operation, and gives different response to environmental changes. The User Agent is instructed by the user during initialization to start the data simulation and the autonomous monitoring and diagnosing activities. Subsequently, the agents perform their tasks continuously and accurately until the user asks them to stop or change their goal.

The following suspicious ML scheme example illustrates how our prototype works. Three months of simulated banking transaction data shows deposits were made daily to a foreign currency account totaling about US$350,000. In the same period of time, there are 10 wire transfers totaling US$2.7 million to a bank in the United Arab Emirates. These unusual activities are captured by the Transaction Monitoring Agent and are forwarded to the Behavior Diagnosing Agent by a risk report. In order to investigate this case, the Behavior Diagnosing Agent request client profile
analysis from the Client Profile Monitoring Agent, source and destination account information and transaction details from the Transaction Monitoring Agent, and related additional data from the External Data Collecting Agent. After the risk-based analysis, three alerts with reasoning were given by the prototype: the first one is “Relationship with terrorism,” since company profile shows most of the transactions of this company were conducted by countries associated with terrorist activities (e.g., United Arab Emirates, which is identified as a high risk country). The second alert is “The company was involved with several drug transactions occurred in Colombia,” it is because based on the findings of the Drug Enforcement Administration and the bank records, the company was always receiving money from accounts owned by Columbia organizations. The third one is “Unclear source of a large amount of money,” where no materials showed how money is earned from its business, only records indicated that the company received money from individual accounts of other countries or Columbia companies or banks.

IV. CONCLUSIONS

This paper explores the approach of applying intelligent agents for money laundering prevention controls to overcome the limitations of existing anti-money laundering (AML) solutions. A novel and open multi-agent-based AML system is designed and implemented, in which various classes of intelligent agents are proposed to provide a set of functionalities for AML. In sum, our approach has several advantages for AML:

- **Intelligence:** Complex and distributed ML schemes can be identified and diagnosed by a number of intelligent agents through their properties, such as autonomy, reactivity, proactivity, and social ability.
- **Adaptivity:** Our system can not only perform autonomous monitoring and diagnosing work, but also be able to learn from its environment, adapt to changes in the environment and to make decisions that can then be delivered to and interpreted by human eyes.
- **System integration:** Through the User Agent, our intelligent AML system is able to easily integrate with legacy financial application.
- **Scalability:** It is easy to add more business functionalities into our system by adding more agents. It is also simple to modify, insert, or delete business rules or ML scenarios in the system.
- **Business values:** Our approach can offer significant business benefits in terms of reduced costs, business efficiencies, increased productivity and new style of operation.

By following the architecture, we will conduct further task analysis and knowledge acquisition on the prototype system. The system effectiveness will also be evaluated in the future.

ACKNOWLEDGMENT

The authors would like to thank Mr. Eddie Yingtat Yueng and Miss Nan Wu, who provided valuable help in literature collection.

REFERENCES