

INTELLIGENT MONEY LAUNDERING MONITORING AND DETECTING SYSTEM*

Yingfeng Wang, Department of Information Systems, City University of Hong Kong, Hong Kong (SAR), China
gilbert.wang@student.cityu.edu.hk

Huaiqing Wang Department of Information Systems, City University of Hong Kong, Hong Kong (SAR), China
iswang@cityu.edu.hk

Shijia Gao, UQ Business School, University of Queensland, Australia
c.gao@business.uq.edu.au

Dongming Xu, UQ Business School, University of Queensland, Australia
d.xu@business.uq.edu.au

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 dedicated efforts are contributed in combating with money laundering (ML) from multi-aspects, without a comprehensive and solid theoretical support, each of them is combating in its own way. To effectively and efficiently prevent and detect such diverse and complex activity, an Anti-Money Laundering (AML) solution should establish comprehensive, solid and fundamental knowledge framework of the monitoring and detecting process. Based on Simons' decision making theory this study proposed an intelligent-agent-oriented solution for money laundering monitoring and detecting process (MLMDP). In order for a more adaptive, intelligent and flexible solution for anti-money laundering, the intelligent agent technology is applied in this research to deal with the complex, dynamic, and distributed MLMDP. 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 money laundering monitoring and detecting processes.

Keywords: Anti-money laundering, Money laundering monitoring and detecting, Intelligent agents.

1 INTRODUCTION

Since the mid-1980s, money laundering (ML) has been increasingly recognized as a significant global problem, with serious economic and social ramifications. Criminal elements in today's technology-driven society are using every means available at their disposal to launder the proceeds from their illegal activities. The anti-money laundering (AML) effort by the United States began with the passage in 1970 of the Bank Secrecy Act. During the later 40 years, the global AML regime has been established with different domestic and international AML organizations founded by major jurisdictions. Various regulations, rules, and legislations kept being set up, modified and amended. In addition, related industries, especially financial institutions, such as banks, security trading companies, insurance companies, are induced to take their obligation to avoid direct contact with criminal money based on a firm's legal and enforcement foundation. Subject to the regulations of the Bank Secrecy

* This research is supported by a strategic research grant (No. 7001896) from the City University of Hong Kong

Act, financial institutions especially the banks, the core in the global financial system, are required to file the Suspicious Activity Report (SAR) to report known or suspected violations of law or suspicious activity. SAR is not only one of the effective passage through which industry can help in AML, but as well combined with prosecutions and convictions, forfeitures and seizure, and prices paid for money-laundering services, SAR becomes one of the main indirect indicators to assess the effectiveness of the AML regime in reducing crime (Reuter and Truman, 2004).

It is because the uncertainty and complexity of ML process that human experts can hardly handle the monitoring and detection tasks so as to file the SAR effectively and efficiently with their expertise and regulations only (Gao et al., 2006). Although increasingly many anti-money laundering solutions have been in place to help to file the SAR for some time within the financial community, they cannot adapt to the ever-changing risk and methods in relation to money laundering. Without a comprehensive analysis on current ML situations 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. Therefore based on Simon's decision making theory this study applied intelligent agent technology to ML prevention controls by taking advantage of agent's autonomy, reactivity, proactivity, and social ability (Gao et al., 2007; Wang et al., 2007)

2 BACKGROUND

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 (HM Treasury, 2004). ML is a diverse and often complex process that need not involve cash transactions. ML basically involves three independent steps, including placement, layering, and integration, which can occur simultaneously (IFAC, 2002).

Legal authorities in various jurisdictions have issued an accelerated level of pronouncements and taken enforcement steps focused on combating ML and related financial crime. In 1989, the Group of Seven Industrial Democracies (G-7) created a global ML watchdog organization called the Financial Action Task Force (FATF). In 1990, the FATF issued its first annual report, containing its now-famous FATF 40 Recommendations (FATF, 2003), which are the most important set of international anti-money laundering (AML) standards and have been a substantial force in encouraging government AML initiatives. In addition, FATF initialized the lists of Publicly Exposed Persons (PEP) and Non-cooperative Countries and Territories (NCCT) for indicating risky people and countries.

Cooperating with the major jurisdictions and laws, financial services industry, especially banks, was required to implement the report system to generate the currency transaction report (CTR), suspicious activity report (SAR), and etc. so as to initialize and facilitate the AML process. However, there are as many methods to launder money as the imagination allows, and the ML schemes being used are becoming increasingly sophisticated and complex as technology advances (CICA, 2005). ML is becoming increasingly difficult to detect and deter. Reuter and Truman (2004) summarized two basic pillars, **Prevention** and **Enforcement**, in global AML regime. The **Prevention** pillar is to prevent criminals from using private individuals and the financial institutions to launder the proceeds of their crimes. In this pillar, four key elements were identified (Reuter and Truman, 2004), including Customer due diligence (CDD), Reporting, Regulation and Supervision. The first and second elements summarized the responsibilities that the financial institutions are required to take to cooperate with the major jurisdictions and laws to fight against the criminal activities. The remaining two elements were focus on implementing and ensuring compliance with the anti-money laundering laws. The **Enforcement** pillar is designed to punish criminals when, despite prevention efforts, they have made the successful laundering of those proceeds. In this pillar, another four key elements were identified (Reuter and Truman, 2004), including List of predicate crimes, Investigation, Prosecution and punishment, and Confiscation. List of predicate crimes establishes the legal basis for criminalizing

ML, while investigation refers to using various detection and investigative techniques to identify specific instances of money laundering and link each to predicate crimes. If justified by the investigation, the third and fourth elements punish the criminals.

3 DECISION MAKING PROCESS MODEL OF MLMDP

The design purpose of this study is to propose a solid and comprehensive framework for an intelligent agent assist decision support system that targets improved end-users' decision making in dealing with MLMD and generating effective suspicious activity report (SAR), parallels human problem solving processes, and supports the major phases of decision making. To achieve decision support effectiveness, an ideal system should be built with reference to adapting a mature decision-making theory. Simon's (1977) decision making process framework identifies four different phases – **Intelligence, Design, Choice, and Review** – of the decision making process. In addition, Wang and Wang (2006) proposed a cognitive approach to manage the complex business process. In that study, they argued that changes of the environments resulted in dynamic and uncertain processes, which is exactly what happened in money laundering activities. The ML and AML environment state is moving all the time in world wide. The conceptual model developed in this study is mainly based on the well-know Simon's framework incorporating with Wang and Wang's (2006) cognitive approach.

Mainly based on Simon's framework, a conceptual process model for MLMDP is constructed by mapping Simon's decision making process model with the two pillars in AML regime (Reuter and Truman, 2004). In global AML regime, there are certain elements that must be conducted by human beings. In **Prevention** pillar, human efforts are essential for conducting regulation and supervision, and sanctions, since they are reflecting the enacted legislation. Similarly prosecution and punishment, and confiscation in **Enforcement** pillar represent the consequences of offense and disobeying of the law. Therefore, computer-based anti-money laundering systems (AMLSs) will not touch upon these areas. Another group of elements provides the domain knowledge for design and implementations of the systems, including the predicated crimes in history, and the investigation techniques. Thus, based on the former crimes and existing invigilation techniques, the intelligent AMLSs will help to perform the CDD and Reporting in **Prevention** pillar, in other words the monitoring and detection process in the whole anti-money laundering schema. Therefore, in this section, decision making process model of money laundering monitoring and detection process (MLMDP) is produced and discussed in detail. Figure 1 shows how the decision making process works in MLMDP and contributes to intelligent money laundering monitoring and detection systems (IMLMDs).

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. However, given the complex nature of ML prevention controls, either human analysts or automated tools can perform the task on their own. An automated solution cannot attach decision to any activity detected – it can only detect activity worthy of human investigators' interpretation and help to generate SAR. Human ML expertise is essential to determine if that activity is suspicious and performing follow-ups after receiving any warning messages from systems. Therefore, during the decision-making process in our proposed conceptual model, both automated solution (in Intelligence, Design and Choice phases) and human expertise (in Review phase) are involved.

To launder the proceeds from their illegal activities, criminals are using every means available at their disposal. Moreover as money launders become aware of the techniques being used to combat them, they are changing their patterns of behavior all the time. Besides, the environment state of money laundering is quite unstable. Millions of financial transactions are being processed at any moment of the day. There can be millions of billions dollars are being washed through different institutions, using different mechanisms, during these transactions (Veyder, 2003). Accordingly regulations, rules, and legislations are being modified, amended, and issued all the time. In addition, the concealed and severe criminal activities, associated with money laundering, make the situation even more complicated. Under this circumstance, in the **Intelligence** phase, proactive, and reactive abilities of

intelligent agent are essential to take the responsibility in searching in the environment for the problems. To perform this activity, firstly, communication with legacy financial systems, for example the existing banking systems, is required. In money laundering prevention for cross-border and wire payments, operation may be required to be real or near real-time (Wicks, 2001). Therefore, to monitor transactions that possibly associated with money laundering requires run time communication between legacy financial systems with the IMLMDSs. To exam the criticality of transactions, information of the accounts conducting the transactions is also needed from legacy systems. Furthermore, monitoring every transaction and trying to find problems request certain technique. First is the transaction product type, since different kind of transactions will have different possibilities to be involved in money laundering process (Small and Byrne, 2005). The second is perform CDD, in other words check the client profiles. It requires the systems' ability to know: who is your real customer, what does your customer do for making money, where does your customer live or locate, and etc. (Kingdon, 2004). Based on this information, in this phase, only a portion of risky transactions will be further evaluated. Since to evaluate each single transaction is inefficient, the system should be able to filter a portion of low-risk transactions, such as the routine salary payment of a professor.

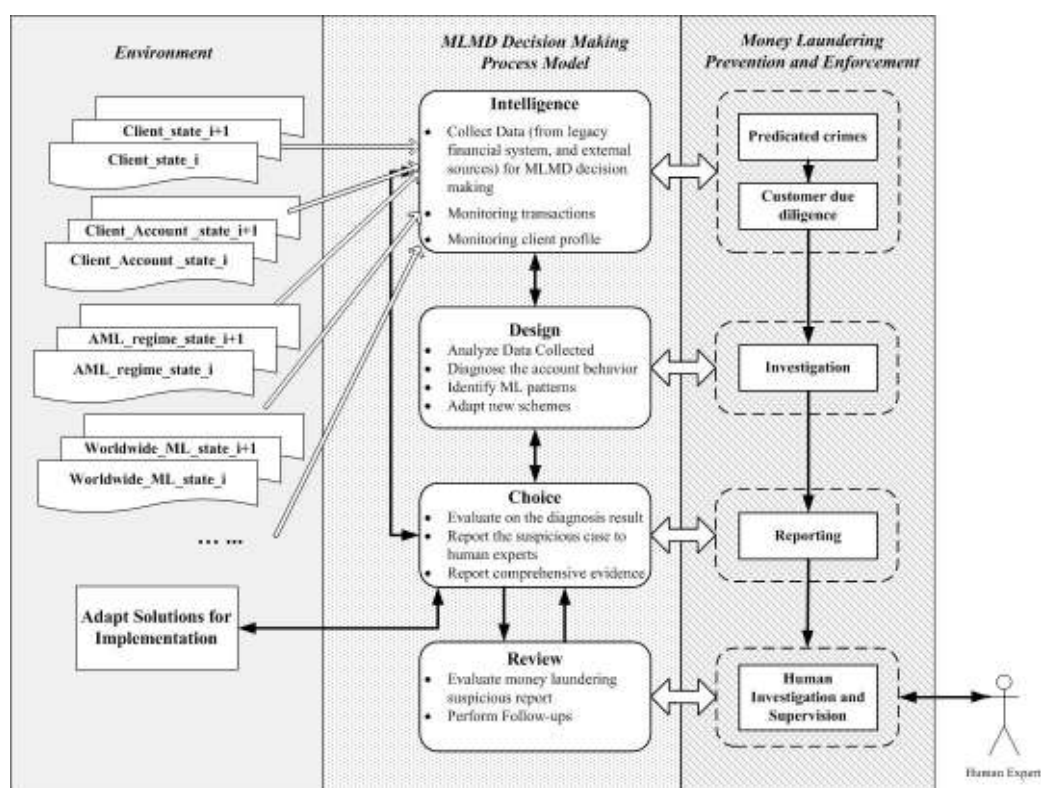


Figure 1. Decision Making Process Model of MLMDP

Money laundering always associates with unusual account behavior. Here, the next **Design** phase will assess the account behavior when receive the information from **Intelligence** phase. It is the unusual behavior instead of suspicious one that should be looked for, because there are no clues as to what constitutes “suspicious” behavior (Kingdon, 2004). One behavior can be probably involved in money laundering for one account, while the same behavior can be totally risk free for another account. There are no set rules that can be applied to detect patterns for money laundering (Wicks, 2001). Therefore, unusual behavior should be targeted. To identify the unusual behavior of an account requires a good understanding of what is normal and reasonable activity for particular types of client, taking into account the nature of the client business. This kind of knowledge can hardly be predefined. Therefore, intelligent agent’s learning abilities are essential for establishing and improving this knowledge. Behaviors are defined as unusual either in terms of amount (for example, by reference to comparative figures for similar customer, or to the regular fund movement in the same client account in the history)

or type of transaction (HKMA, 2004). Based on identifying the unusual account behavior, system can identify the patterns of ML, and provides the **Choice** phase with its findings.

In the **Choice** phase, the first task is to evaluate the detection result provided by **Design** phase. Based on the overall criticality of a transaction, the diagnosis on possible ML related transactions can be made. To complete the activity, analysis of the information provided by **Design** phase should be combined with the findings from **Intelligence** phase. If define the job performed in **Design** phase is to determine the dynamic risk of a transaction, then the one performed in **Intelligence** phase is to determine the static risk of the transaction. The overall risk level is determined based on the integration of both risks. By considering the information available, system in this phase should try the best to making the warning report for the suspicious case. Surely not all the transactions will get the warning report, but each one should be determined to hold a certain level of risk. To support human investigator, system should try best to provide comprehensive evidences with the warning report. Usually, one transaction doesn't in itself constitute a money laundering case. More transactions can be possibly correlated and contributed in the criminal activity. To search and report these correlated transactions, the **Choice** phase, need to review the transactions histories in the account to uncover the concealed abnormal transactions.

In the last **Review** phase, human investigators' interaction is necessary for evaluate the report produced by **Choice** phase, and further investigations.

4 MULTI-AGENT SYSTEM ARCHITECTURE FOR IMLMDS

ML detection and prevention is extremely difficult. Due to the complex nature of financial products, services, and ML itself, ML is dynamic and adapts over time according to changing conditions. To provide efficient and effective mechanisms to detect the possible money laundering activities by providing deep investigation, risk-based approach for conducting due diligence at account opening, monitoring, and some screening and searching processes is commonly used all over the world now (Banking Policy Department, 2004; CICA, 2004; FFIEC, 2005; HM Treasure, 2002). Generally it is believed that a risk-based approach will enhance the effectiveness of monitoring unusual or potentially suspicious activity to the extent such activity is distinguishable from legitimate activity (Wolfsberg, 2006). Therefore the risk-based approach is adopted and focused in this research.

The risks assessed by Risk Assessment Class are divided into two groups, namely Static Risk and Dynamic Risk. Static risk represents the intrinsic risk of transactions, such as the related client's profile, the product type, etc., while dynamic risk describes the behavior of an account, which will keep changing along with the incoming transactions.

The static risk assessment class basically assesses four kinds of risks, and determines a composite risk level of a transaction.

- Entity Risk – represents the risk of the client and counterparty, who conducted the transaction. It is composed of two risks, the name risk and business/occupation risk. Name risk is measured by checking whether the names of both sides of a transaction are on any Publicly Exposed Persons (PEP) lists. Business/Occupation risk is considering the businesses or occupations that the client and the counterparty are engaged in. Cash (and cash equivalent) intensive businesses, such as Casino, Money Service Business, are considered to possess high risk.
- Product Risk – represents the risk of the transaction type. As mention above different products possess different risk levels. The products, such wire transfer, cash deposits, which are hard to trace back to origins, are considered to possess high risk.
- Geography Risk – represents the risk of the nationalities and residences/locations of both sides of a transaction. The countries on public high risk country lists, for example NCCT, are considered to possess high risk.
- Amount Risk – represents the risk of amount in a single transaction. Federal Financial Institutions Examination Council requires that Customer Transaction Record (CTR) report must be offered to

identify currency activity greater than \$10,000 (FFIEC, 2005). Therefore as a basic requirement, the amount risk is measured by whether the amount involved in a transaction is over \$10,000

The Dynamic Risk Assessments basically assesses two kinds of risks, and determines an unusual risk of an account.

- **Accumulated Fund Flow Risk** – represents the risk of unusual fund movement within an account. There are several possible mechanisms to measure whether the account behaves abnormally by comparing with the historical usual movement. One of them is the increasing acceleration of the differences of short term and long term moving average of accumulated fund movement. Since fund inflow and outflow can happen in the same day, the account balance will not be able to reflect the abnormal situation. Every day an account has accumulated fund inflow and outflow value no matter there are any transactions occur or not. Moving average (MVA) is one of the oldest and most popular technical analysis tools in the stock market (Achelis, 2001). MVA of the stock price represents the consensus of investor expectations over a certain time period, thus it describes a moving trend of the stock price. Generally, short term MVA is more fluctuated than a long term MVA. The difference between short term and long term MVA can be used to measure the short term price fluctuation degree comparing with the long term trend. The MVA of accumulated fund flow of the account under monitoring represents the increasing trend of accumulate transaction amount, which works similarly to the stock price MVA. A sudden and significant acceleration in the difference between short term trend and long term trend suggests the unusual transaction activity. Since laundering dirty money always requires performing fund inflow or outflow, both flows should be monitored. In an account transactions are divided into two groups, since both fund inflow and outflow should be tested. Short term and long term moving average of accumulated fund inflow and outflow will be tested. The changing difference between them will be monitored. Any sudden and significant acceleration in the difference between short term trend and long term trend will get special attention. Besides, the average accumulated fund inflow and out flow amount will also be considered as a reference. When the historical data is unavailable, which means it is a recently created account, effective monitoring and detecting way is focusing on the client profile.
- **Accumulated Transaction Amount Risk** – Federal Financial Institutions Examination Council requires to identify not only any single currency activity greater than \$10,000, but also currency transactions involving multiple lower dollar transactions (e.g., \$3,000) that over a period of time (e.g., 10 days) aggregate to a substantial sum of money (e.g., \$30,000), (FFIEC , 2005) subject to BSA. It is because that the CTR threshold is so well-known that it is evadable for criminals.

Vahidov and Fazlollahi (Vahidov and Fazlollahi, 2004) proposed a generic architecture of multi-agent decision support system (MADSS). Partially adopted Simon's (Simon, 1977) decision making theory, they proposed MADSS framework based on the decision support pyramid. In that study, they demonstrated the effectiveness of the architecture in dealing with ill-structured problems such as investment decision making. Incorporating with Vahidov and Fazlollahi's architecture (Vahidov and Fazlollahi, 2004), a mapping system architecture is designed and proposed in this section can be produced based on the conceptual model, which are provided in previous sections. Proposed intelligent MLMD DSS (IMLMDS) provides efficient and effective services that help human investigator monitor every single transaction occurred, exam transactions that are possibly correlated to criminal activities after filtering risk-free ones, and provide human investigator with a risk level for each checked transaction, and explicit suspicious activity report for transactions that possess high risk.

Figure 2 shows the architecture of IMLMDS consisting of entities and agents, organized by the MLMD decision making process model presented above. External Entities include Data and Models that provide both internal and external information such as client profile, transactions, transaction history, etc. from existing financial systems and law ordinance, predicated crimes, new investigation techniques, etc. from external electronic sources to different agents and the user, on real time base or when information is required.

The **Intelligence** Group contains two groups for agents, namely information agents (**I**) and monitoring agents (**M**). They are

External Information Gathering Agent (I): By proactively searching, obtaining, and aggregating relevant information from external electronic resources, External Information Gathering Agent, is able to provide most updated information and knowledge, including the counterparty of a transaction information, which is important for perform monitoring and detection activities for transactions, the latest predicated crimes, which possessing the knowledge of current ML patterns and trends, and updated domain knowledge, such as newly developed investigation techniques. All of other agents from different groups may request information relates to their task from this agent, if necessary.

Internal Information Gathering Agent (I): By obtaining, aggregating, and assessing relevant information from existing financial systems, Internal Information Gathering Agent is able to provide run time transactions for monitoring, and other requested information, such as client profile, transactions in account history, currently used investigation techniques, valuable feedback from human experts. All of other agents from different groups may request information relates to their task from this agent, if necessary.

Client Profile Monitoring Agent (M): For each single transaction coming from existing financial systems, Client Profile Monitoring Agent will perform the monitoring job based on client profile. The purpose of perform such monitoring activity is to filter out some risk-free transactions, in other words is to identify the possible money launderer, since money laundering detection is equally about identify good customers as it is about identifying bad (Wicks, 2001). Two major aspects of Static Risk will be monitored and examined for both sides of a transaction, including Entity Risk, Geography Risk. Client's profile will be requested and supplied by Internal Information Gathering Agent, while information of the other side will be requested and supplied by External if available. If counterparty's information is not available, the counterparty bank's location will be used in Geography Risk test, while Entity Risk will be tested only based on client's profile.

Transaction Monitoring Agent (M): For each single transaction coming from existing financial systems, Transaction Monitoring Agent will monitor the transaction by testing the other two major aspects of the Static Risk. The product type will check and determined a certain risk level, while amount of each transaction will be tested based on FFIEC's CTR threshold, which is \$10,000

Basically, the **Intelligence** Group is responsible for two major tasks. Data and information searching and collecting are essential for the system to maintain functioning. Transaction filtering is also very important for improve the efficiency and capabilities of the system. For instance, transactions like a university professor receives his/her monthly salary or a business man pays a restaurant 20 USD for his dinner by credit card, are risk free, and will not be monitored and assessed by the IMDMLS. Thus the efficiency of the system can be improved, since perform the investigation on every single transaction is inefficient or even impossible, regarding the tremendous volume of transactions occurring in every second.

The **Design** Group contains only one but powerful **Behavior Detecting Agent**, which is responsible for monitoring the transaction patterns of the account and identify the unusual behavior of the account. Unusual transaction patterns, which are different from the usual account activities, could indicate the suspicious money laundering activities. To identify and report suspicious transactions requires the agent to have a good understanding of what is normal and reasonable activity for particular types of customer, taking into account the nature of the customer's business. This kind of knowledge can hardly be predefined. Therefore, intelligent agent's learning abilities are essential for establishing and improving this knowledge. The Behavior Detecting Agent is able to identifying transactions that are unusual either in terms of amount (for example, by reference to comparative figures for similar customer, or to the regular fund movement in the same client account in the history) or type of transaction (HKMA, 2004). That the increasing acceleration of the differences of short term and long term moving average of accumulated fund movement is used for detect the usual behavior of an account. Besides the measurement, according to FFIEC currency transactions involving multiple lower dollar transactions (e.g., \$3,000) that over a period of time (e.g., 15 days) aggregate to a substantial

sum of money (e.g., \$30,000) (FFIEC, 2005), will also be adopted. Based on the historical transaction data, the agent is able to detect the abnormal transactions.

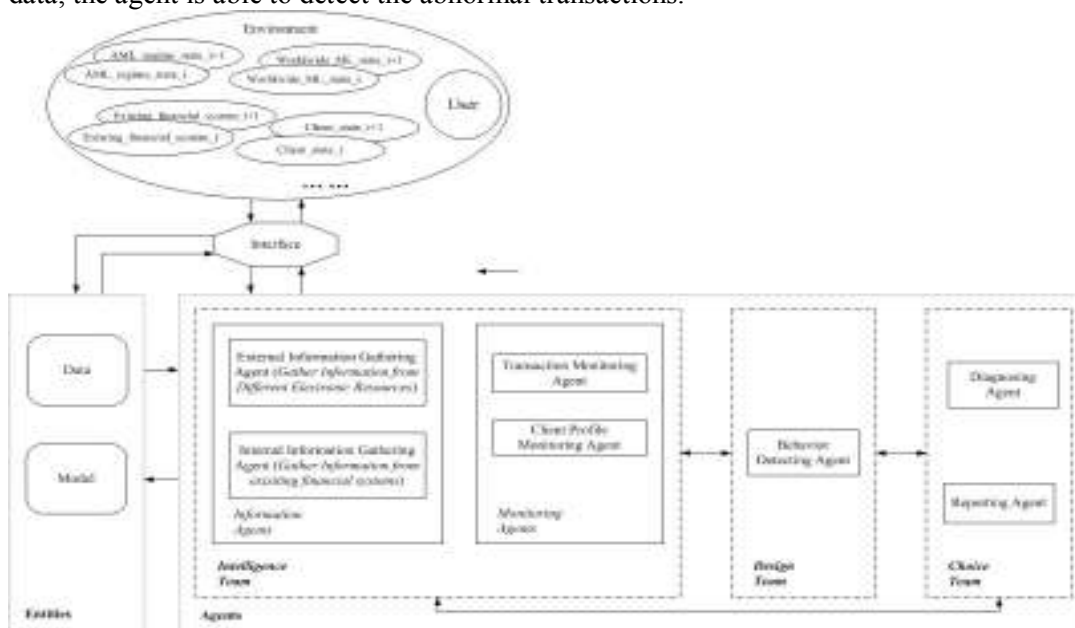


Figure 2. Multi-agent System Architecture

In the **Choice** Group, there are two agents, namely Diagnosing Agent and Reporting agent.

Diagnosing Agent: Receiving the detection result form Behavior Detecting Agent, Diagnosing Agent requests the monitoring result from monitoring agents. According to the table provided by Small and Byrne (2005), a composite risk level will be determined for each transaction by considering all the aspects of Static Risk. By integrating the Static Risk and Dynamic Risk, Diagnosing Agent will issue one potential ML alert out of four, including Extremely High, High, Medium, and Low, for reporting.

Reporting Agent: Reporting Agent will present and communicate a potential ML alert to the appropriate compliance personnel for case management investigation and action. Alternatively the Reporting Agent can automate or take a specific course of action, for example, interfering with standard operations to block a particular suspicious transaction. The agent 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 agent also facilitates combining the automatically generated alerts with suspect manual reports to build the case for investigation. The reporting facilities within the Reporting Agent 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.

5 SENARIO ANALYSIS

In this section, to demonstrate the system's operation, an artificial scenario is created with the similar ML techniques used in September 11th hijack incident and discussed in detail. A small corporation, running the business in low risk level industry, owned by an ordinarily U.S. citizen, John, owns an account in a New York bank. At beginning one and half years, the account appeared to be normal. The corporation's majority business activities are domestic transactions. On average the monthly

transaction amount was approximately US\$50,000 fund inflow and US\$40,000 fund outflow. But its business had never generated in excess of US\$10,000 a day. Recently a pattern of cash deposits below the Customer Transaction Record (CTR) reporting threshold occurs. Deposits were made daily to the account of foreign currency exchange totalling \$341,421 for approximately two-and-one-half-month period from different places in U.S. During the same period, the business initiated 10 wire transfers totalling \$2.7 million to a bank in the Myanmar. At the beginning deposit stage, the transactions will be considered as nothing special, because the client profile is general, transaction amounts are under threshold. Therefore no report or low risk report will be generated. When time goes on, several states of the transactions will keep changing in terms of both transaction profile and accumulated fund flow amount. It is because during the same period not only fund inflow but also the outflow is being generated. Furthermore, the totalling amount the fund inflow and outflow during around two-and-one-half-month is abnormally high comparing with those caused by usual transactions in the history. Furthermore, assuming that the fund amount involved in each of the 10 wire transfers is equal, when the first wire transfer occurs, the transferred amount US\$270,000 is much more than the normal situation, therefore, the short term MVA of accumulated fund outflow increases dramatically while long term MVA is much less affected. Based on certain criteria, it is determined that the abnormal transaction occurs based on unusually accelerated differences between short term and long term MVA. Thus the unusual account behaviour will be identified.

The abnormal behaviour of John's company's account will probably be identified in the beginning stage of the wired transfers. It is selected to demonstrate how the system helps human investigators to identify the unusually account behaviour. Figure 3 shows how the IMLMDS Web-services agents work collaboratively to monitor and detect such the suspicious activity.

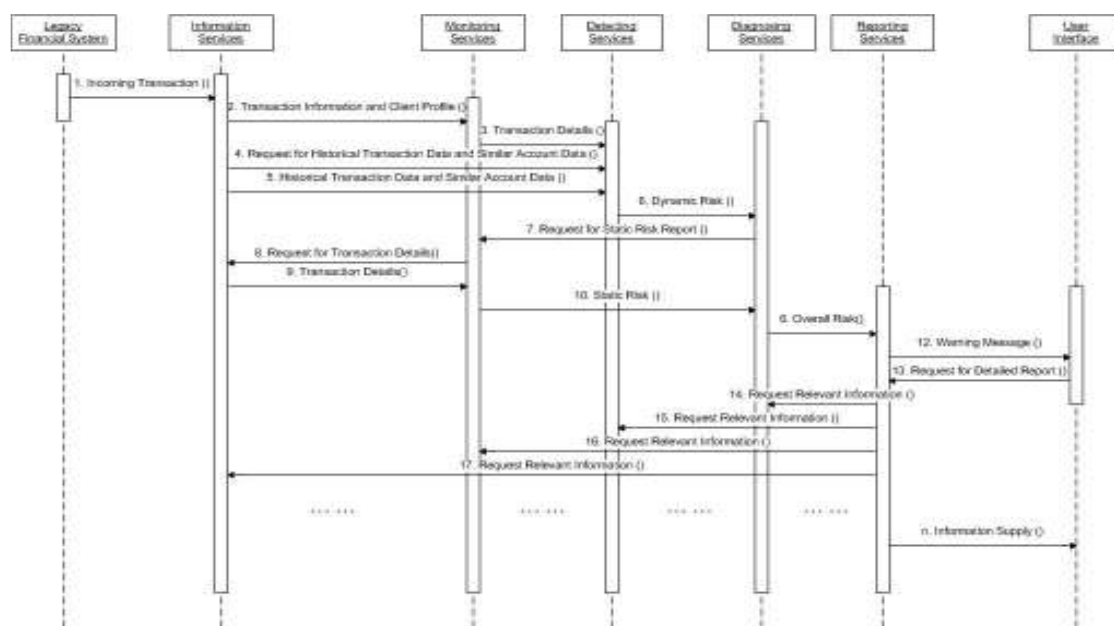


Figure 3. Operation Sequence within IMLMDS Web-services Agents

System operation process:

1. System receives incoming transactions from legacy financial systems, converts them the Web-services messages and passes them to the **Information Service** based on the UDDI.
2. **Information Service** provides **Monitoring Services** with necessary information to process, such as transaction product type, conducting client profile, etc.
3. **Monitoring Services** realized the risky product type and unusual transfer amount according to Customer Transaction Record (CTR) (FFIEC, 2005) threshold. Then refer the transaction to

- Detecting Services** for further analysis.
- 4-6. **Detecting Services** request and acquire the historical transaction data as well as the similar accounts average transaction amount from **Information Service**. The short term and long term MVA of accumulate fund inflow and outflow is calculated and the acceleration of the distances between short term and long term MVAs are examined. Considering the daily transaction amount of the company's account is quite small comparing with the wired transfer and same situation of average account activity of similar accounts, the high dynamic risk is referred to **Diagnosis Services**.
 - 7-10. As requested by **Diagnosis Services**, **Monitoring Services** request and receive more detail information, including the company's details, the transaction counterparty information, etc., of the transaction from **Information Services**. By considering the static risks of a transaction, including entity risk, which is low (because John and his company's profile is general and no bad records exist), geography risk, which is high (because the transaction counterparty is at Myanmar which is on the NCCTs list (FATF, 2006)), product risk, which is high, (because the transaction is conducted through high risk product, wired transfer (Small and Byrne, 2005)), and amount risk, which is high (because the amount is over-boundary (FFIEC, 2005)). The system determined the composite static risk level accordingly and send to **Diagnosis Services**.
 11. **Diagnosis Services** receive both the dynamic and static risk report, and then make a overall diagnosis, which is high risk and pass it to **Report Services**.
 12. **Report Services** issues a warning to human investigators based on the high risk diagnosis.
 - 13-n. Adapte to user's request, **Report Services** retrieves relevant details, including those having been mentioned above, and extra information, from all of the other services.

6 CONCLUSION

Considerable efforts from various aspects have been dedicated into the war of anti-money laundering. Diversified guidelines, regulations, and laws have been issued by governments, organizations, institutions, etc. Different kinds of anti-money laundering systems have been researched, designed and implemented. However, without a comprehensive and solid theoretical support, each effort combats ML in its own way. Therefore, an explicit formal presentation of the conceptual knowledge of monitoring and detecting ML process is needed

This study proposed a decision-making process model for AML by applying Simon's (1977) decision process model incorporating with Wang and Wang's (2006) cognitive approach. Based on this conceptual model, 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, the main contribution of this study to the research literature can be summarized as follows:

- The decision-making process model of AML: This is a conceptual model that identifies the specific activities involved in each decision-making phase for AML. The application of this model can lead to an unambiguous understanding of the concepts of AML, and provide a uniform framework with which different approaches can be integrated together to provide more sophisticated functions and facilities. Therefore, by creating a rich conceptual model, the study provides a solid framework for AML system practice.
- System design innovation: A novel and open architecture for AML has been designed. 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.

In short, this study leads to a new and more general perspective on the use of intelligent decision support agents to support money laundering monitoring and detecting. We believe our research findings will lead to a new stage of technology-mediated AML decision support. The results of this study highlight the fact that the important concepts, including the conceptual models, the agent and Web-services technologies, and the architectural considerations required for developing a financial application, which can assist AML decision making

References

- Achelis S. B. 2001. *Technical analysis from A to Z : cover every trading tool ... from the absolute breadth index to the zig zag*, 2nd ed. McGraw Hill, New York.
- Banking Policy Department. 2004. 'Revised supplement to the guideline on prevention of money laundering'. *Hong Kong Monetary authority Quarterly Bulletin*: 18-20.
- The CICA (The Canada Institute of Chartered Accountants) 2004. *Canada's anti-money laundering & anti-terrorist financing requirements*.
- FATF (Financial Action Task Force), 2003. *The Forty Recommendations*, http://www.fatf-gafi.org/document/28/0,2340,en_32250379_32236930_33658140_1_1_1_1,00.html.
- FATF (Financial Action Task Force). 2006. 'Annual Review of Non-Cooperative Countries and Territories 2005-2006', <http://www.fatf-gafi.org/dataoecd/0/0/37029619.pdf>.
- FFIEC (Federal Financial Institutions Examination Council). 2005. 'Bank Secrecy Act/Anit-money laundering Examination Manual', <http://www.occ.treas.gov/handbook/BSA-AMLIntro-overview.pdf>.
- Gao S., Xu D., Wang H., and Wang Y. 2006. 'Intelligent Anti-Money Laundering System' *Proceedings of the IEEE International Conference on Service Operations and Logistics, and Informatics*, Shanghai, China.
- Gao S., Wang H., Xu D., Wang Y., Shen W., and Yeung S. 2007. 'Intelligent Agent Assisted Decision Support for Family Financial Planning'. *Decision Support Systems*, 44(1)
- HKMA (Hong Kong Monetary Authority). 2004. Supplement to the Guideline on Prevention of Money Laundering. <http://www.info.gov.hk/hkma/eng/press/2004/attached/20040608e4a3.pdf>.
- HM Treasury 2004. *Anti-money laundering strategy*.
- IFAC (International Federation of Accountants) 2002. *Anti-money Laundering*.
- Kingdon J. 2004. 'AI fights money laundering'. *IEEE Intelligent Systems* 19 (3): 87-89.
- Reuter P. and Truman E. M. 2004. *Chasing dirty money: the fight against money laundering*. Institute for International Economics., Washington, DC,
- Simon H. A. 1977. *The new science of management decision*. Prentice-Hall, Englewood Cliffs, NJ,.
- Small R. and Byrne J. 2005. 'Risk Based Approach to Customer Due Diligence', http://www.bankersonline.com/tools/kb_riskratingsystem.pdf.
- Veyder F. 2003. 'Case study: Where is the risk in transaction monitoring'. *Journal of Financial Regulation and Compliance* 11(4): 323.
- Wang M. and Wang H. 2006. 'From Process Logic to Business Logic - A Cognitive Approach to Business Process Management'. *Information and Management*, 43: 179-193.
- Wang Y., Wang H., Gao S., Xu D., Ye K. 2007. 'Agent-oriented Ontology for Monitoring and Detecting Money Laundering Process', *The Second International Conference on Scalable Information Systems*, Suzhou China.
- Wicks T. 2001. 'Intelligent systems for money laundering prevention'. *Money Laundering Bulletin*.
- Wolfsberg Group. 2006. 'Guidance on a Risk Based Approach for Managing Money Laundering Risks', <http://www.wolfsberg-principles.com/risk-based-approach.html>