UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

A MULTI-AGENT BASED COUNTER TERRORISM SYSTEM THROUGH ANTI-MONEY LAUNDERING

BY
CHARLES KOECH

A RESEARCH REPORT SUBMITTED TO THE SCHOOL OF COMPUTING AND INFORMATICS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS OF THE MASTERS OF SCIENCE DEGREE IN COMPUTER SCIENCE OF UNIVERSITY OF NAIROBI

MAY 2016

Declaration

Student

I declare that this project report is my original work and has not been presented anywhere for academic awards before this presentation

Signature: ……. Date: ……

Koech Charles

P58/76125/2012

Supervisor

This project report has been submitted with my approval as the supervisor for the Master of Science degree in Computer Science of the University of Nairobi.

Signature: ……. Date: ……

Dr. Elisha T. Opiyo Omulo

Senior Lecturer

SCHOOL OF COMPUTING AND INFORMATICS

UNIVERSITY OF NAIROBI

Acknowledgements

I would like to express my sincere gratitude to the Almighty God for His mercies and grace, a gift of life and good health to pull through; the management of University of Nairobi, which gave me the environment and learning resources to undertake my Master's degree and write this project report; Dr. Elisha T. Opiyo Omulo, who, being my supervisor in this work, supported me all through and lead me through the academic path; and my friends Joseph Waititu, Andrew Murithi, Daisy Chebet and Philip Irode who gave me unfailing moral support to pull through this program.

Abstract

There has been increasing pressure for countries worldwide to have laws that govern anti-money laundering in face of rising crime posed by international terrorists. In Kenya for instance all financial institutions are supposed to report all suspicious transactions to Financial Reporting Centre. This is a central, national agency responsible for receiving, analyzing and disseminating disclosures of financial information. Money Laundering has been the main source funds for criminals and terrorist to fund their ill motifs. Over time criminals have develop sophisticated methods of 'cleaning' their illegally acquired funds through financial institution to conceal the original source of their funds. This project is a multi-agent system solution that seeks to cap terrorism in Kenya by reporting and stopping suspicious transactions through Anti-Money Laundering approach. Terrorism need a lot of funds to plan and execute their ill-modifies actions. Reducing the sources of funding implies reducing or stopping their power to execute their actions. The project is Multi-Agent System solution developed using C# and Bolari .NET with simulated financial data as inputs.

Keywords: Terrorism, Money Laundering, Anti-Money Laundering, Agent, Multi-agent system

Table of Contents

Declaration ii

Acknowledgements iii

Abstract iv

Table of Contents v

List of Tables vii

List of Figures viii

List of Abbreviations ix

CHAPTER 1: INTRODUCTION 1

1.0 Introduction 1

1.1 Problem statement 1

1.2 Objectives 2

1.3 Justification/Rationale of the study. 3

1.4 Scope and Limitations of study 3

CHAPTER 2: LITERATURE REVIEW 5

2.0 Introduction 5

2.1 Terrorism 5

2.2 Money Laundering 7

2.3 Anti-Money Laundering 8

2.4 Counterterrorism 10

2.5 Multi-agent systems 11

2.6 Related Systems 13

2.7 The Proposed system 15

2.8 Development Tools/Software 17

CHAPTER 3: METHODOLOGY 19

3.0 Introduction 19
3.1 MAS – CommonKADS methodology 19
3.2 Conceptualization 21
3.4 Analysis 24
3.5 Design 27
Why this methodology 28
CHAPTER 4: SYSTEM ANALYSIS, DESIGN AND IMPLEMENTATION 29
4.1 Conceptualization 29
4.2 Analysis 33
4.3 Design 39
4.4 Implementation 42
4.5 System Evaluation 45
CHAPTER 5: RESULTS AND DISCUSSION 47
Functionality of the prototype 47
Realism of the system 57
CHAPTER 6: CONCLUSION, RECOMMENDATIONS AND FUTURE WORKS 59
6.1 Conclusion 59
6.2 Recommendations 59
6.3 Future works 59
References 60
Appendices 63
Appendix A – Table structure 63
Appendix B – Sample Code 65
Appendix C –System Demo 73

List of Tables

Table 1: Enhanced CRC cards 23
Table 2: Actors and use cases 32
Table 3: Categorize client use cases for staff agent 32
Table 4: Client classifier agent textual template 34
Table 5: Client categorization agent activity's textual template 36
Table 6: Pre-determined client categorization rule. 37
Table 7: Organization Model 38
Table 8: The tasks in Unit Testing 45
Table 9: Watch List table 48
Table 10: New clients on watch list 48
Table 11: Suspected Accounts 49
Table 12: Financial Institution transactions 50
Table 13: Tagged financial transactions 52
Table 14: Transactions by suspected individuals/Organizations 54
Table 15: Suspicious Transactions 55

List of Figures

Figure 1: Decision Making/Problem-solving process model For AML adapted from Gao & Xu 2006 14
Figure 2: Architecture of the proposed system 18
Figure 3: Models of MAS-CommonKADS 21
Figure 4: Use case diagram 30
Figure 5: Message Sequence Charts for New client 31
Figure 6: Client categorization agent activity diagram 35
Figure 7: Client Categorization task inferences diagram 37
Figure 8: Flow diagram of client classifier Agent 39
Figure 9: Flow diagram of Money Laundering Agent 40
Figure 10: Flow diagram of Money Laundering Rules 41
Figure 11: Design Diagram displaying the interaction of agent 42
Figure 12: Proposed system interface flow diagram 43
Figure 13: Diagram displaying Agent Interactions 46
Figure 14: Agents' communication – New clients 49
Figure 15: Agents' communication – tagged transactions 55
Figure 16: Agents' communication –Suspicious transactions 56
Figure 17: Deployment Mode Diagram 57
Figure 18: Screenshot of agents after launch 73
Figure 19: Registering bank client. 74
Figure 20: Bank client registration screen 75
Figure 21: Agents' communication on new client 75
Figure 22: Money laundering rule setting 76
Figure 23: ReportingAgent communication 77

List of Abbreviations

AML Anti-Money Laundering

FRC Financial Reporting Centre

ML Money Laundering

MAS Multi-Agent System

CT Counterterrorism

OO Object-Oriented

FATF Financial Action Task Force

KYC Know Your Customer

CDD Customer Due Diligence

KYE Know Your Employees

KCYC Know the Customers of the Customer

KTYC Know the Transactions of Your Customers

KYBP Know Your Business Partners

CID Customer Identification

STR Suspicious Transaction Reports

OOSE Object Oriented Software Engineering

UML Unified Modeling Language

GUI Graphical User Interface

CRC Class Responsibility Collaboration

UER User-Environment-Responsibility

CHAPTER 1: INTRODUCTION

1.0 Introduction

The general aim of this paper is to explore how Anti-Money Laundering (AML) can be used to the fight against terrorism. Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets.

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 of 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 (Gao and Xu 2006).

An effective AML regime will have in place measures aimed at identifying and investigating such laundering activity and using the evidence obtained in bringing the person or persons concerned to justice. It will also have in place measures aimed at preventing the dissipation or loss of the proceeds of crime and recovering and/or confiscating them. An effective AML regime can therefore make a significant contribution to the fight against terrorism in at least two main ways: (i) it could help uncover evidence of criminal activity through identification of suspicious movements of financial assets, thus increasing the chances of a successful prosecution of the perpetrator of the crime; (ii) it also enables the tracing of criminal proceeds to facilitate their preservation, recovery and ultimate return to rightful owner.

1.1 Problem statement

Terrorism today has become a global threat to the security of every individual. Terrorism clearly has a very real and direct impact on human rights, with devastating consequences for the enjoyment of the right to life, liberty and physical integrity of victims. In addition to these individual costs, terrorism can destabilize Governments, undermine civil society, jeopardize peace and security, and threaten social and economic development.

Today, Money Laundering has become a key funding mechanism for international religious extremism, and curtailing these illegal activities has become an important focus of governments as part of their ongoing wars on terrorism. There has been an increased focus across the globe on the prevention of Money Laundering and terrorist financing. An effective Anti-Money Laundering regime can therefore make a significant contribution to the fight against terrorism by uncovering evidence of criminal activity through identification of suspicious movements of financial assets and enabling the tracing of criminal proceeds to facilitate their preservation, recovery and ultimate return to rightful owner.

Over and above the need for a financial institution to be able to identify money laundering activities, the other problem is that money laundering is getting more and more sophisticated making it difficult for financial institutions to detect this criminal activity. Financial institutions and governments thus require equally sophisticated systems that are adoptive and flexible to able to continue detecting money laundering activities.

The project proposes a multi-agent based system to provide an analysis of data held in financial institutions and to report and act in real time money laundering transactions that are meant to fund terrorism. The system is centrally placed so that it can sniff transaction done by various financial institutions. It will then determine whether the transactions executed amounts to money laundering or not. Money laundering transactions are then reported and/or transactions are stopped. It also contains a database of backlisted individual suspected of aiding terrorism. It will keep on monitor transactions and comparing the facilitators and beneficiaries against the backlisted suspects.

1.2 Objectives

To explore and build a multi-agent based system prototype model that will provide an analysis of transactions in financial institutions and report and act in real time on money laundering transactions that are meant to fund terrorism.

Specific objectives of the study are;

1. To explore and research on money laundering activities through financial institutions as a source of funding for terrorism in Kenya
2. To explore and research how multi-agent systems can be used as an anti-money laundering strategy in financial institutions in Kenya

3. To develop and test a multi-agent system prototype supporting anti-money laundering strategy meant to fund terrorism
4. To analyze the output of the prototype and give findings and recommendations of implementation of such a real world system.

1.3 Justification/Rationale of the study.

Money laundering has overtime become the third largest 'Business' behind the currency exchange and automobile industry. Criminals therefore find it very attractive as it legitimizes their illegally obtained funds. As a result, financial institutions come under pressure to ensure that they put in place measures to prohibit criminals from laundering their illicitly obtained funds. Financial institutions must therefore detect when their customers introduce illicit funds into their financial system.

Given that Money Laundering has become a key funding mechanism for global extremism and terrorism, financial institutions and governments requires equally robust systems that are adoptive and flexible to enable them in detecting and stopping money laundering activities that are specifically meant to fund terrorism to reduce the resources available to terrorists to fund their activities. The main objective of this study is to explore and build a multi-agent based system prototype model that can report and act in real time on money laundering transactions that are meant to fund terrorism. This model can assist the financial institutions in such an important task to fight the menace.

1.4 Scope and Limitations of study

This project will focus on Anti-Money laundering in Kenyan Financial Institutions to fight terrorist in Kenya. Owing the confidentiality and privacy laws of data held by financial institutions, it might not be feasible to get real transactions of individuals in financial institutions because they guard the confidentially of their clients. Most of the transactions to be used in the study therefore will be a simulation of the real transactions in the financial institutions.

Sources of names in watch list/consolidated list will be from reliable bodies and diligence and evidence will have been done before updating the list. Again some of these names might not be real names as the confidentiality of this data is paramount.

CHAPTER 2: LITERATURE REVIEW

2.0 Introduction

This chapter presents the literature review relating to money laundering activities in financial institutions and how terrorists use money laundering as a means to fund their activities. Due to complex nature of money laundering in financial institutions, it warrants the use of multi-agent based solution. The proposed system seeks to reduce and/or eliminate terrorism by detecting money laundering activities. Since terrorism activities need huge sum of money, reducing/minimizing money laundering implies fewer funds will be left at their disposal hence their capacity is rendered effortless.

2.1 Terrorism

Terrorism is the unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political.

Terrorism is commonly understood to refer to acts of violence that target civilians in the pursuit of political or ideological aims. In legal terms, although the international community has yet to adopt a comprehensive definition of terrorism, existing declarations, resolutions and universal "sectorial" treaties relating to specific aspects of it define certain acts and core elements. In 1994, the General Assembly's Declaration on Measures to Eliminate International Terrorism, set out in its resolution 49/60, stated 6 that terrorism includes "criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes" and that such acts "are in any circumstances unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or other nature that may be invoked to justify them." Ten years later, the Security Council, in its resolution 1566 (2004), referred to "criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a Government or an international organization to do or to abstain from doing any act". Later that year, the Secretary-General's High-level Panel on Threats, Challenges and Change described terrorism as any action that is "intended to cause death or serious bodily harm to civilians or noncombatants, when the purpose of such an act, by its nature or context, is to

intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act" and identified a number of key elements, with further reference to the definitions contained in the 1999 International Convention for the Suppression of the Financing of Terrorism and Security Council resolution 1566 (2004). The General Assembly is currently working towards the adoption of a comprehensive convention against terrorism, which would complement the existing sectorial anti-terrorism conventions. Here definition of terrorism which includes "unlawfully and intentionally" causing, attempting or threatening to cause: "(a) death or serious bodily injury to any person; or (b) serious damage to public or private property, including a place of public use, a State or government facility, a public transportation system, an infrastructure facility or the environment; or (c) damage to property, places, facilities, or systems…, resulting or likely to result in major economic loss, when the purpose of the conduct, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or abstain from doing any act." The draft article further defines as an offence participating as an accomplice, organizing or directing others, or contributing to the commission of such offences by a group of persons acting with a common purpose. While Member States have agreed on many provisions of the draft comprehensive convention, diverging views on whether or not national liberation movements should be excluded from its scope of application have impeded consensus on the adoption of the full text.

Impact of Terrorism

Terrorism has a direct impact on the enjoyment of a number of human rights, in particular the rights to life, liberty and physical integrity. Terrorist acts can destabilize Governments, undermine civil society, jeopardize peace and security, threaten social and economic development, and may especially negatively affect certain groups (Security Council resolutions 1373 2001 and 1377 2001)

- Threatens the dignity and security of human beings everywhere, endangers or takes innocent lives, creates an environment that destroys the freedom from fear of the people, jeopardizes fundamental freedoms, and aims at the destruction of human rights;
- Has an adverse effect on the establishment of the rule of law, undermines pluralistic civil society, aims at the destruction of the democratic bases of society, and destabilizes legitimately constituted Governments;

- Has links with transnational organized crime, drug trafficking, money-laundering and trafficking in arms, as well as illegal transfers of nuclear, chemical and biological materials, and is linked to the consequent commission of serious crimes such as murder, extortion, kidnapping, assault, hostage-taking and robbery;
- Has adverse consequences for the economic and social development of States, jeopardizes friendly relations among States, and has a pernicious impact on relations of cooperation among States, including cooperation for development;
- Threatens the territorial integrity and security of States, constitutes a grave violation of the purpose and principles of the United Nations, is a threat to international peace and security, and must be suppressed as an essential element for the maintenance of international peace and security.

On 28 September 2001, acting under Chapter VII of the Charter of the United Nations, it adopted resolution 1373 (2001), stating explicitly that every act of terrorism constitutes a "threat to international peace and security" and that the "acts, methods, and practices of terrorism are contrary to the purposes and principles of the United Nations." The resolution also requires all States to criminalize terrorist acts; to penalize acts of support for or in preparation of terrorist offences; to criminalize the financing of terrorism; to depoliticize terrorist offences; to freeze funds of persons who commit or attempt to commit terrorist acts; and to strengthen international cooperation in criminal matters.

2.2 Money Laundering

The term "money laundering" is used to describe the process by which the proceeds of crime ("dirty money") are put through a series of transactions which disguise their illicit origins, and make them appear to have come from a legitimate source ("clean money").

Money laundering is of great concern to law enforcement agencies, and for very good reason. The complex criminal activity which generates "dirty money", whether drug trafficking, arms smuggling, corruption, or other offences, are often extremely difficult to detect. Accordingly, finding and following the "money trail" has been a basic strategy to combat sophisticated crime. Success in money laundering means that detection of the predicate offence, and the identification of the offender, become that much more difficult (Hector and Lakshmi 2005)

Generally, money laundering occurs in three stages:

- **Placement**: Cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.

- **Layering**: Funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.

- **Integration**: Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

The fundamental challenge facing law enforcement authorities and commercial interests alike is to develop systems for the prevention and control of money laundering, without unduly restraining commercial activity: how to "harden the target" without having a chilling effect on enterprise. A similar balancing act will be necessary in order to achieve a compromise between the competing values of financial privacy and traceability.

2.3 Anti-Money Laundering

To fight these illegal activities, prevention, detection and prosecution techniques must be developed to form anti-money laundering processes. The Financial Action Task Force on Money Laundering (FATF), an inter-governmental organization founded in 1989 whose purpose is to combat money laundering and terrorist financing, developed The 40 Recommendations. The recommendations have been internationally recognized and implemented (over 130 countries) due to its simplicity and foundation upon solid principles (Financial Action Task Force 2004).

The Financial Action Task Force (FATF) is the global standard setting body for anti-money laundering and combating the financing of terrorism (AML/CFT). In order to protect the international financial system from money laundering and financing of terrorism (ML/FT) risks and to encourage greater compliance with the AML/CFT standards, the FATF identified jurisdictions that have strategic deficiencies and works with them to address those deficiencies that pose a risk to the international financial system.

The FATF Recommendations are the international standards that sets out what countries should do to have effective systems for preventing and addressing money laundering, terrorist financing and the financing of proliferation. The Recommendations set out the measures that countries should have in place within their criminal justice and regulatory systems; the preventive measures to be taken by financial institutions and other businesses and professions; the measures to ensure transparency on the ownership of legal persons and arrangements; the establishment of competent authorities with appropriate functions, and powers and mechanism for cooperation; and the arrangements to cooperate with other countries.

Kenya has taken steps towards improving its AML/CFT regime, including by parliamentary approval of the Finance Bill, which amends the FT offence; however, this is still awaiting Presidential assent. Despite Kenya's high-level political commitment to work with the FATF and ESAAMLG to address its strategic AML/CFT deficiencies, Kenya has not made sufficient progress in implementing its action plan within the agreed timelines, and certain strategic AML/CFT deficiencies remain. Kenya should continue to work on implementing its action plan to address these deficiencies, including by: (1) adequately criminalizing terrorist financing; (2) ensuring a fully operational and effectively functioning Financial Intelligence Unit; (3) establishing and implementing an adequate legal framework for the identification and freezing of terrorist assets; and (4) implementing an adequate and effective AML/CFT supervisory programme for all financial sectors. The FATF encourages Kenya to address its remaining deficiencies and continue the process of implementing its action plan.

The Role of Financial Institutions

The first step for financial institutions to contribute to the fight against organized crime and money laundering is to select and implement effective AML processes, considering the issues discussed above. While vendors and researchers work to increase sophistication of available technology, the financial institution is responsible for its own risk assessment, which forms the basis for selecting and implementing technology and systems suitable to the institution. They are also responsible for designing and implementing effective internal controls, based on the identified risks, and based on key due diligence requirements. Along with data collection and mining, suspicious transaction reporting, and proper preparation for examination, financial institutions can contribute to the fight against money laundering and organized crime.

Due Diligence

"Knowing your activities" has become a focus for due diligence requirements. The following are identified key due diligence processes that financial institutions should include in their processes from the Journal of Financial Regulation and Compliance (Wit 2007). Know Your Customer (KYC): "Understand who the customers are and what they do throughout the relationship with them"; Know the Transactions of Your Customers (KTYC): "Understand the transactions of the customer and have systems in place to spot any irregularities or suspicious activity"; Know the Customers of the Customer (KCYC): "This extra level of understanding of the customers activities allows for an extra level of the KYC process"; Know Your Business Partners (KYBP): "Understanding those the institution work with to avoid that indirectly the institution will be involved in unwanted activities" and Know Your Employees (KYE): "Criminal organizations need employees in the financial service industry to support them with illegal activities"

Some of the above processes relate to customer due diligence (CDD). CDD can be divided into two different stages: first, at the moment of customer relationship acceptance, and secondly, during the lifetime of the customer relationship. KYC processes should be present throughout both stages, as it "involves the assessment of the risk associated with each customer as banks continually monitor customers' behaviour based on their transactions." (Peggy 2007). FATF Recommendation 5 further stresses the importance of CDD, and states that a customer account should not be opened if the institution cannot comply with the Recommendation (Financial Action Task Force 2004). More specifically, there is greater emphasis on customer acceptance and customer identification (CID) processes. "There has to be no doubt about the identity of the customer, the representative and the ultimate beneficial owner. Further it will be very important to understand the business of the customer, the source of wealth and income." (Wit 2007).

2.4 Counterterrorism

Counterterrorism activities and operations are taken to neutralize terrorists, their organizations, and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals.

2.5 Multi-agent systems

In Multi-agent systems (MASs), a system is modeled as a collection of autonomous decision-making entities called agents. Each agent individually assesses its situation and makes decisions on the basis of a set of rules. The development of intelligent agents (IAs) and multi-agent systems (MASs) has recently gained popularity among IS researchers (Franklin and Graesser 1996). 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 (1995) 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 (Wooldridge 2002). 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 behaviour (Wooldridge 1999). 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 (Wooldridge 2002). 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 behaviours of other agents, to generate plans and to execute these plans.

There are three main attributes of an agent: (a) autonomy, which refers to the fact that an agent should run independently, with little or no human intervention, (b) temporal continuity, which signifies that an agent should run continuously rather than simply perform a task and finish, and (c) social skills, which signifies that an agent should possess some form of social skills, since the agent's advantages lie in its interactive communication with other agents. An agent can also be classified according to the following social behavior characteristics:

a. Pro-activeness: this refers to how the agent reacts to -and reasons about - its environment, and how it pursues its goals. The agent can directly react to stimuli in its environment by mapping an input from its sensors directly to an action, or it can take a purely planning, or goal-oriented, approach to achieve its goals. This last approach relies upon utilizing planning techniques.

b. Adaptability: this describes an agent's ability to modify its behavior over time. In fact, the term “agent” is often taken to implicitly mean “intelligent agents”, which combine traditional artificial intelligence techniques to assist in the process of autonomously performing tasks. This feature includes other sub-features such as learning and submission.
c. Mobility: this refers to the agents’ capability of transporting their execution between machines on a network. This form of moving can be physical, where the agent travels between machines on a network, or logical, where an agent which is running on a single machine is remotely accessed from other locations on the Internet.
d. Collaboration: collaboration among agents underpins the success of an operation or action in a timely manner. This can be achieved by being able to coordinate with other agents by sending and receiving messages using some form of agent communication language, and permits a high degree of collaboration, thus making social activities such as distributed problem solving and negotiation possible. Moreover, it is possible for agents to collaborate without actual communication taking place. The interaction of agents with resources and their environment may lead to the emergence of collaborative or competitive behavior.
e. Veracity: this refers to the agent’s ability to deceive other agents via their messages or behavior. An agent can thus be truthful in failing to intentionally deceive other players. Moreover, an agent that is untruthful may try to deceive other agents, either by providing false information or by acting in a misleading way.
f. Disposition: this refers to the agent’s “attitude” towards other agents, and its willingness to cooperate with them. An agent may always attempt to perform a task when asked to do so (benevolent), or may act in its own interests to collaborate with other agents only when it is convenient to do (self-interested), or it might try to harm other agents or destroy them in some way (malevolent) (Hector and Lakshmi 2005).

An agent makes a decision about what action to perform based on the history of the system that it has witnessed to date.

Multi-agent systems learning

The cognitive domain involves knowledge and the development of intellectual skills (Bloom 1956). This includes the recall or recognition of specific facts, procedural patterns, and concepts that serve in the development of intellectual abilities and skills. There are six major categories of cognitive and processes (Federal Reserve Bank of New York 1987).

a) Knowledge is the memory of previously learned materials such as facts, terms, basic concepts, and answers.
b) Comprehension is the understanding of facts and ideas by organization, comparison, translation, interpretation, and description.
c) Application is the use of new knowledge to solve problems.
d) Analysis is the examination and division of information into parts by identifying motives or causes. A person can analyze by making inferences and finding evidence to support generalizations.
e) Synthesis is the compilation of information in a new way by combining elements into patterns or proposing alternative solutions.
f) Evaluation is the presentation and defense of opinions by making judgments about information, validity of ideas, or quality of work based on a set of criteria.

2.6 Related Systems

Kariuki, at al, 2014, did a project research on a Multi-Agent Based Anti-Money Laundering System for use in a typical financial institution. The system is comprised of a group of software agents that work together to prevent and detect money laundering. It also provides a framework for reporting suspicious money laundering activities within a financial institution. Among the software agents are be the data collecting agents which gather internal and external data. The system also comprises of analyzing agents which use data collected by the data collecting agents to intelligently detect suspicious money laundering activities. If suspicious money laundering activities are detected, they would be sent to a reporting agent for a report to be compiled in a prescribed format.

This solution concentrated on anti-money laundering in one financial institution. It is therefore possible to transact a number of transactions in various financial institutions without any detection of money laundering since one financial institution do not have transactions from other financial institutions. The proposed solution also factored in a list of suspected individuals who are aiding criminal activities.

Gao and Xu, 2006, proposed a conceptual modelling and development of an intelligent agent-assisted decision support system for anti-money laundering

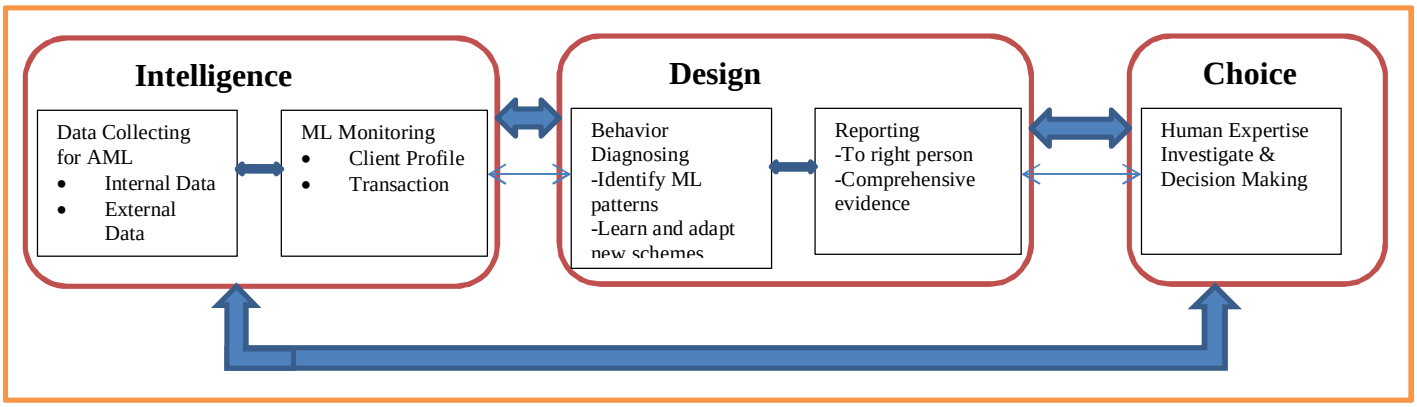

Figure 1: Decision Making/Problem-solving process model For AML adapted from Gao & Xu 2006

Above solution concentrates only on detecting and reporting money laundering whereas the proposed solution factored in how to use money laundering to reduce/eliminate terrorism.

Alvaro and Gareth, 2002 applies the MAS – CommonKADS methodology to the Flights Reservation Problem. We develop each model included in this methodology, illustrating the complete development of both the coordination and expertise models. We incorporate UML activity diagrams in the task model and use sequence diagrams to model communication between agents (human and software) and to detail the participation of each agent. We illustrate the implementation of the system using AGLETS, an agent building tool, and emphasize its integration with JESS, the Java Expert System Shell.

This work used the same methodology to solve a different problem from the one of the proposed system

2.7 The Proposed system

Though the project is working on anti-money laundering activities in financial institutions in Kenya, it focuses more on subset of clients (i.e. clients in watch list/Consolidated list). The proposed project will apply multi-agent technology to keep track of all transactions done by this subset of clients and detecting and raising alerts or stopping the transactions all together. To find the right subset clients, the proposed project applies the name matching algorithm.

Consideration has been taken into account to take care of clients' name and addresses against the watch list. In our case the watch list is the sanction names linked to terrorists or/and al-kaida network. The watch list is updated from various sources to a central database. In the proposed system, there is new client agent that will dynamically apply various pre-programmed rules against the client information provided. New client agent will output a report detailing the percentage of similarity of the client against the watch list. This output will then guide the financial institution user to take the necessary action i.e. whether to transaction with the client or to dismiss the client or/and report to security agencies. There is an agent (suspect agent x) in each and every financial institution keeping track of transaction of clients identified to be in the watch list. Update agent x will update a central database with all transactions done by clients in the watch list to be analyzed by AML agent to determine whether the transactions are ML. Such information, unless combined with large amounts of other data, offers few opportunities to identify suspicious transactions. Reporting agent will then report the transaction found to be ML to the relevant bodies. Refer to figure (i) below.

Patterns in Time and Locations

The need for temporal and spatial screening affects the necessary technical characteristics of a successful monitoring system. First, it emphasizes the importance of examining data from multiple locations and time periods, making localized analysis less likely to be effective—screening at a single bank or for limited time periods may identify relatively few money laundering schemes. Second, the need for temporal and spatial screening implies the need for certain types of databases and analysis tools, making them ill-suited for investigating money laundering (Federal Reserve Bank of New York1987).

Indeed, even these patterns of transactions can be made to resemble legitimate businesses. However, these data can be combined with other data in order to evaluate the suspiciousness of a pattern of financial transactions.

Below is guidelines from Security Council Committee Established Pursuant To UN Resolution 1267 (1999) Concerning Al-Qaida and The Taliban and Associated Individuals And Entities

The Consolidated List

(a) The Committee will update regularly the Consolidated List when it has agreed to include relevant information received from Member States or international or regional organizations either directly or through the Monitoring Team.

(b) Member States are encouraged to establish a national mechanism or procedure to identify and assess appropriate candidates to propose to the Committee for listing.

(c) Before a Member State proposes a name for addition to the Consolidated List, it is encouraged, if it deems it appropriate, to approach the State(s) of residence and/or citizenship of the individual or entity concerned to seek additional information. States are advised to submit names as soon as they gather the supporting evidence of association with Al-Qaida and/or the Taliban. A criminal charge or conviction is not necessary for inclusion on the List as the sanctions are intended to be preventive in nature. The Committee will consider proposed listings on the basis of the "associated with" standard described in paragraphs 2 and 3 of resolution 1617 (2005). When submitting names of groups, undertakings and/or entities, States are encouraged, if they deem it appropriate, to propose for listing at the same time the names of the individuals responsible for the decisions of the group, undertaking and/or entity concerned.

(d) Member States should provide a statement of case in support of the proposed listing that forms the basis or justification for the listing in accordance with the relevant resolutions. The statement of case should provide as much detail as possible on the basis for listing indicated above, including: (1) specific findings demonstrating the association or activities alleged; (2) the nature of the supporting evidence (e.g., intelligence, law enforcement, judicial, media, admissions by subject, etc.) and (3) supporting evidence or documents that can be supplied. States should include details of any connection with a currently listed individual or entity. States should indicate what portion(s) of the statement of case the Committee may publicly release or release to Member States upon request.

(e) Proposed additions to the List should be submitted using the cover sheet attached as an annex to these Guidelines and include, to the extent possible, relevant and specific information to

enable the accurate identification of the individual, group, undertaking or entity concerned by competent authorities, including:

- For individuals: family name/surname, given names, other relevant names, date of birth, place of birth, nationality/citizenship, gender, aliases, employment/occupation, residence, passport or travel document and national identification number, current and previous addresses, and current location;
- For groups, undertakings or entities: name, acronyms, address, headquarters, subsidiaries, affiliates, fronts, nature of business or activity, leadership, tax or other identification number and other names by which it is known or was formerly known.

(f) The Committee will consider expeditiously requests to update the List.

(g) Any modification to the List will be communicated to Member States immediately. For new entries to the List, the Secretariat shall include, upon the prior decision of the Committee, the publicly releasable portion of the statement of case in its communication. The updated List will be made promptly available on the web-site of the Committee. Unless the Committee decides otherwise, any new entry to the List will be transmitted to Interpol to request, where feasible, the issuance of an Interpol-United Nations Security Council Special Notice. Once the updated List is communicated to Member States, States are encouraged to circulate it widely, such as to banks and other financial institutions, border points, airports, seaports, consulates, customs agents, intelligence agencies, alternative remittance systems and charities.

2.8 Development Tools/Software

Windows 7

Boris .NET

Visual studio C#.NET 2012

MySQL Database

Figure 2 below summarizes the flow of the proposed system.

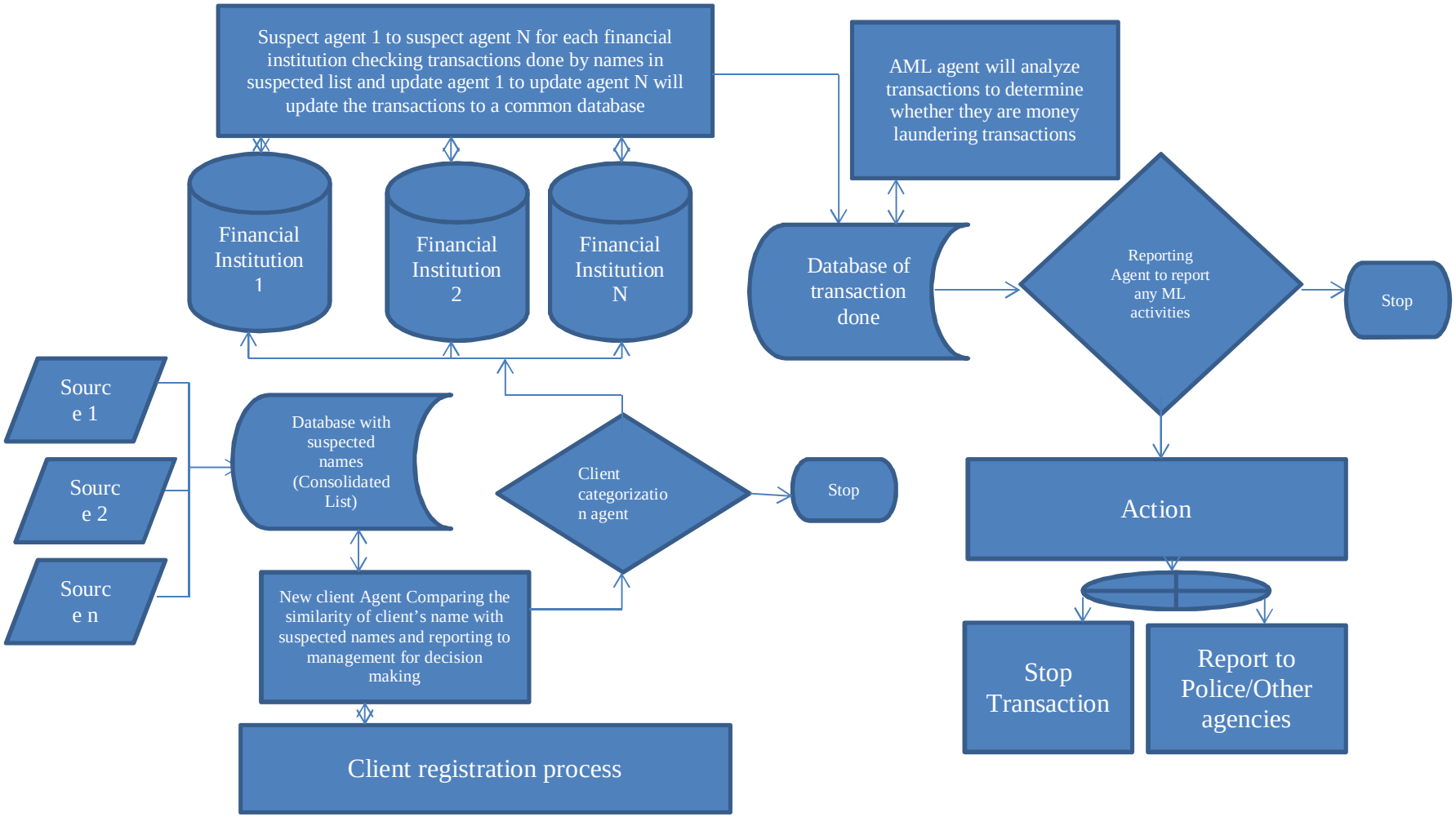

Figure 2: Architecture of the proposed system

CHAPTER 3: METHODOLOGY

3.0 Introduction

As agent technology has matured with the deployment of a variety of applications, particularly in open and dynamic environments such as the web, several methodologies and tools have been proposed to support software engineers during the development process of such systems.

3.1 MAS – CommonKADS methodology

This project proposes the **MAS – CommonKADS** methodology to counter terrorism. According to Iglesias et al. 1998 MAS-CommonKADS is based on the models of CommonKADS extended and adapted to agent modelling, including the definition of a new model, the coordination model, for describing agent interactions.

The software development life cycle in MAS-CommonKADS follows the phases described below:

- **Conceptualization**: Elicitation task in order to obtain a first description of the problem through the definition of a set of use cases that help to understand the system and how to test it.
- **Analysis**: The analysis phase determines the functional requirements of the system. It describes the system through the development of a set of models.
- **Design**: The design phase combines a top-down and bottom-up approach, reusing developed components and developing new ones, depending on the targeted agent platform. The design phase takes as an input the analysis models, which are then operationalized, that is, transformed into specifications (the design model) ready to be implemented. The internal architecture of every agent and the "network architecture" of the system are determined.
- **Development and testing**: Coding and testing tasks of the previously defined agents.
- **Operation**: Maintenance and operation of the system.

The methodology defines the following models (see figure 3 below):

- **Agent model** that specifies the agent characteristics: reasoning capabilities, skills (sensors/effectors), services, agent groups, and hierarchies.

- **Task model** that describes the tasks that the agents can carry out: goals, decompositions, ingredients, problem-solving methods, and so forth.
- **Expertise model** that describes the knowledge needed by the agents to achieve their goals.
- Organization model that describes the organization into which the MAS is going to be introduced and the social organization of the agent society.
- **Coordination model** that describes the conversations between agents, their interactions, protocols, and required capabilities.
- **Communication model** that details the human-software agent interactions and the human factors for developing these user interfaces. This model uses standard techniques for developing user interfaces.
- **Design model** that collects the previous models and consists of three sub-models: ***network design***, for designing the relevant aspects of the agent network infrastructure (required network, knowledge and telematic facilities); ***agent design***, for dividing or composing the agents of the analysis, according to pragmatic criteria and selecting the most suitable agent architecture for each agent; and ***platform design***, for selecting the agent development platform for each agent architecture.

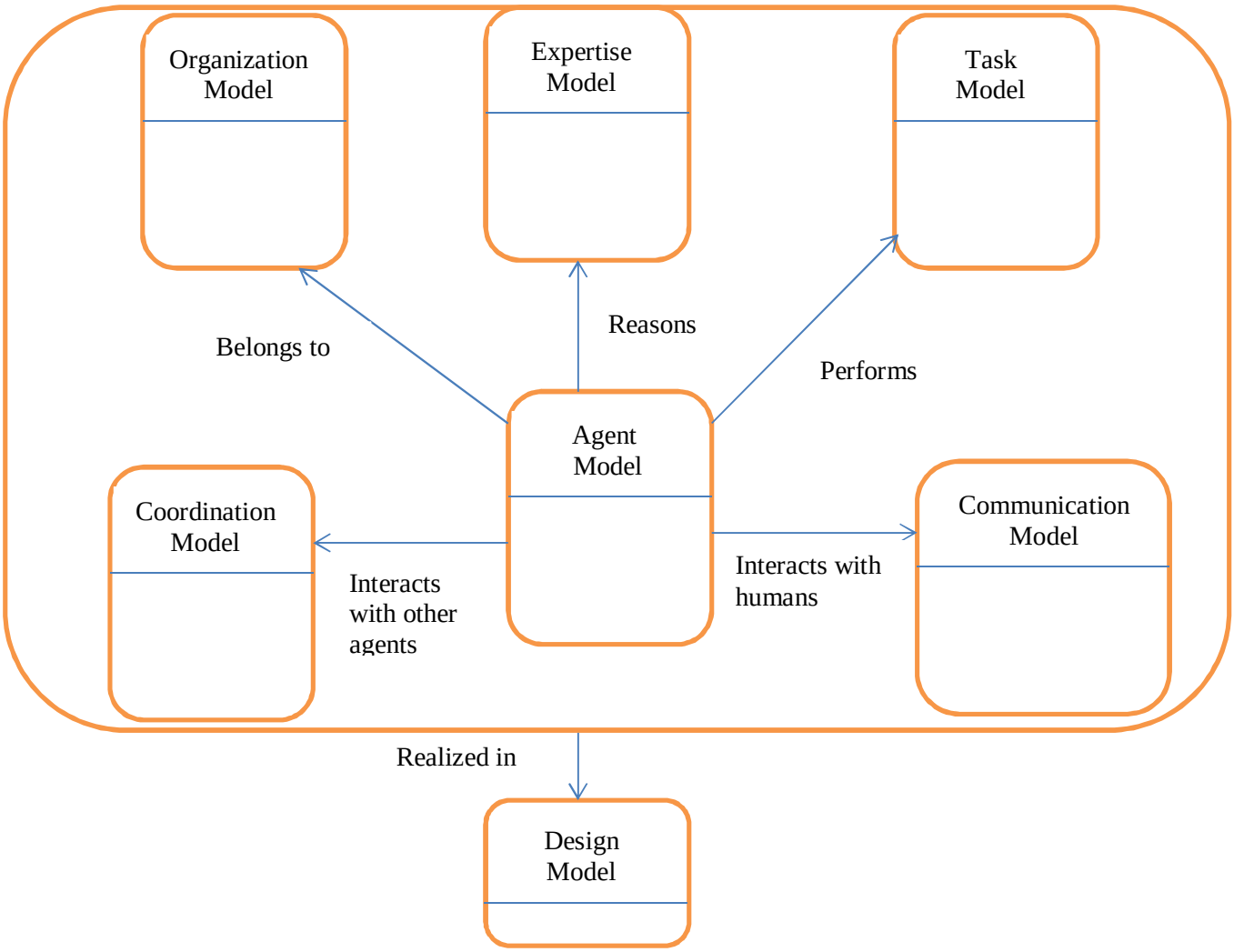

Figure 3: Models of MAS-CommonKADS

3.2 Conceptualization

The problem of conceptualization is the first step towards the identification of the functional requirements of a system. One of the most extended techniques for getting a first idea of the system is the Use Case technique. The technique consists in identifying the possible users of the systems and the possible user goals, describing ways of achieving these user goals. These textual descriptions are the use cases. Usually, different use cases can be combined with the relationships extend (if a use case is an extension of another one) or include (if a use case is a part of another one). This technique is very simple and intuitive and has been very successful for requirements elicitation and validation.

The use case technique can also be used for conceptualizing a multi-agent system. Nevertheless, autonomous agents are distinguished because they do not need a user that supervises their execution. So, while with use cases we have to answer the question, how is my system used? We could ask ourselves about other requirements of our system such as: When and how does my system act and react to the environment? (environment cases) and what are the goals of the system? (responsibility or goal cases).

In order to conceptualize an agent-based system, two general techniques are used in MAS-CommonKADS: the UER cases technique that deals with the identification of use, reaction, and goal cases of an agent or a multi-agent system, and the enhanced Class-Collaboration-Responsibility Cards technique that deals with the identification of responsibilities, plans, and collaborations of an agent. Both techniques are complementary. The UER technique can be used for both single-agent or multi-agent systems (for identifying use, reactive, and goal cases of the whole system). The enhanced CRC cards can only be used for conceptualizing multi-agent systems, since they guide the definition of collaborative scenarios. (Iglesias et al. 1998)

UER Technique

The User-Environment-Responsibility (UER) technique (Iglesias & Garijo, 1999) combines user, environment and responsibility-driven analysis for conceptualizing a system from an agent-oriented perspective. This technique can be used for conceptualizing a particular autonomous agent or the general requirements of a multi-agent system. The technique analyses the system from three complementary perspectives: the user perspective, the environment perspective, and the assigned responsibility perspective.

- **User-Centered Analysis**. The potential users (called actors) of the system are identified, together with their possible tasks or functions. The result of this analysis is the set of use cases. This analysis answers the question: What are the possible uses of the multi-agent system?
- **Environment-Centered Analysis**. Agents can be situated in an environment, and this environment needs to be modelled. In particular, we are interested in modelling how the system can act and react to this environment. The result of this analysis is the set of reaction cases. This analysis answers the question: How has the multi-agent system reacted to the environment?

- **Responsibility-Driven Analysis**. In contrast to usual software systems, multi-agent systems can act proactively. The user can desire that the system has some responsibilities, that is, the user can assign some goals or responsibilities to the system and the system carries out these responsibilities without a direct demand. This analysis answers the question: What are the goals of the system? The main difference of goal cases from the use cases is that the use cases show how the system gives an answer to a user request, while the goal cases show how the system behaves when some condition is fulfilled.

The application of the UER technique introduces some of the most relevant properties of an agent system, such as reactivity and proactiveness in the conceptualization of the system.

Enhanced CRC Cards and Internal Use Cases

The well-known Class Responsibility Collaboration (CRC) cards technique (Beck & Cunningham, 1989; Wirfs-Brock, Wilkerson & Wiener; 1990) provides a method for organizing the relevant classes for modelling a system. This technique was initially used for teaching object fundamentals in a collaborative environment. The technique consists of filling in cards. Each card has a class name and two columns. The left column shows the responsibilities of the class, namely, the tasks the class can perform or knowledge it has, and the right column show the classes that collaborate to achieve these tasks or obtain this knowledge.

This technique can be easily modified from an agent perspective. A CRC is filled for each agent class. Each CRC is divided into five columns (Table 1): goals assigned, plans for achieving these goals, knowledge needed to carry out the plans, collaborators in these plans, and services used in the collaboration. The back side of the CRC is used for annotations or extended description of the front side.

Table 1: Enhanced CRC cards

Agent:				
Goals	Plans	Knowledge	Collaborator	Service

3.4 Analysis

The results of this phase will be the requirements specification of the MAS through the development of the models previously described, except for the design model. These models are developed in a risk-driven way, and the steps are:

- **Agent Modelling**: developing initial instances of the agent model for identifying and describing the agents.
- **Task Modelling:** task decomposition and determination of the goals and ingredients of the tasks.
- **Coordination Modelling**: developing the coordination model for describing the interactions and the coordination protocols between the agents.
- **Knowledge Modelling**: modelling of the knowledge about the domain, the agents (knowledge needed to carry out the tasks and their proactive behaviour), and the environment (beliefs and inferences of the world, including the rest of the agents).
- **Organization Modelling:** developing the organization model. Depending on the type of project, it may be necessary to model the organization of the enterprise in which the MAS is going to be introduced for studying the feasibility of the proposed solution. In this case, two instances of the organization model are developed before and after the introduction of the MAS. This model is also used to model the software agent organization.

The Agent Model

The agent model acts as a link between the rest of the models of MAS-CommonKADS, since it collects the capabilities and restrictions of the agents.

MAS-CommonKADS proposes different strategies that can be combined in order to identify the agents of our problem. Some of these techniques are:

- Analysis of the actors of the use cases defined in the conceptualization phase. The actors of the use cases delimit the external agents of the system.
- Several similar roles (actors) can be mapped onto one agent to simplify the communication.
- Analysis of the statement of the problem. The syntactic analysis of the problem statement can help to identify some agents. The candidate agents are the subjects of the sentences,

the active objects. The actions carried out by these subjects should be developed by the agents as goals (with initiative) or services (under demand).

- Usage of heuristics. The agents can be identified by determining whether there is some conceptual distance: knowledge distribution, geographical distribution, logical distribution, or organizational distribution.
- Initial task and expertise models can help us to identify the necessary functions and the required knowledge capabilities, resulting in a preliminary definition of the agents. The goals of the tasks will be assigned to the agents.
- Application of the enhanced CRC cards.

Once the agents have been identified, every agent should be further described using textual templates that collect the main characteristics of the agents, such as its name, type, role, position, a description, offered services, goals, skills (sensors and effectors), reasoning capabilities, general capabilities, norms, preferences, and permissions. The process of filling in these templates helps the engineer to review his/her understanding of the problem and serves as a means of communication with the rest of the team.

The Task Model

The task model describes all the activities that should be performed in order to achieve a goal. Tasks are decomposed following a top-down approach and described in an "and/or" tree. The description of a task includes its name, its goal, a short description, input and output ingredients, task structure, its control, frequency of application, preconditions, and required capabilities of the performers.

The potential benefits of the development of this model are the documentation of the activities of the organization before and after the introduction of the multi-agent system.

The graphical notation of this model follows traditional tree decomposition or, alternatively, decomposition where optional and iterative tasks are indicated. It can be also be used to describe whether the tasks can be performed in a parallel or sequential way. Usually, the first versions of the model use just the sequential decomposition and refined versions of the model introduce gradually parallel tasks, optional tasks, or iterative tasks. Alternatively, the activity diagram of UML can be used for this model.

In case a task is knowledge intensive, it should be further developed in the expertise model. In the same way, if a task requires the agent interaction or human interaction, it should be further developed in the coordination model or communication model, respectively.

The Coordination Model

The coordination model specifies the interactions between the agents of the multi-agent system. The main components of the coordination model are the conversations between agents that are initiated to fulfill a goal in a cooperative way. Every conversation is composed of interactions (associated to speech acts) and follows a conversation protocol. In order to establish a conversation, there are some capabilities between the agents that maintain this conversation (capabilities and knowledge) that are specified in this model.

The coordination model has two milestones: (1) definition of the communication channels and building of a software prototype for testing purposes (as a mockup); and (2) analysis of the interactions and determination of complex interactions (with coordination protocols).

The Expertise Model

The expertise model, which is the focus of CommonKADS, is used for modelling the reasoning capabilities of the agents to carry out their tasks and achieve their goals. Normally, several instances of the expertise model should be developed: modelling inferences on the domain; modelling the reasoning of the agent; and modelling the inferences of the environment (how an agent can interpret the event it receives from other agents or from the world).

The expertise model consists of the development of the application knowledge (consisting of domain knowledge, inference knowledge, and task knowledge) and problem-solving knowledge.

The Organizational Model

This model shows the static or structural relationships between the agents, while the coordination model shows the dynamic relationships. The organization model is used for modelling both the human organization where the multi-agent system is going to be developed and the multi-agent society itself.

The main modelling steps are the description of agent (human and software) relationships, detailing the roles played in every relationship, and the study of the relationship of the environmental objects with the agents. In the case of software agent relationships, the model will collect the different use cases developed in the coordination model, while in the human-software

agent case, the system will collect the use cases developed in the communication model. As a result of this first analysis, the organization model will define the static and dynamic relationship between both human and software agents and the roles played by them in the different interactions (in addition to the required knowledge to be able to perform those interactions). During this process, inheritance and group relationships between software agents can be modelled as a result of the analysis.

3.5 Design

During the design phase, the design model is developed. This phase is extended for multi-agent systems and consists of the following phases:

- Agent network design: the infrastructure of the multi-agent system (so-called network model) is determined and consists of network, knowledge, and coordination facilities. The agents (so-called network agents) that maintain this infrastructure are also defined, depending on the required facilities. Some of these required facilities can be: Network facilities, Knowledge facilities and Coordination facilities.

  The result of the common facilities shared by the agents allows the efficient communication between the agents and is expressed by ontology, in the same way as service ontology.
- Agent design: the most suitable architecture is determined for each agent, and some agents can be introduced or subdivided according to pragmatic criteria. Each agent is subdivided in modules for user-communication (from communication model), agent communication (from coordination model), deliberation and reaction (from expertise, agent, and organization models), and external skills and services (from agent, expertise, and task models). The agent design maps the functions defined in these modules onto the selected agent architecture.
- Platform design: selection of the software (multi-agent development environment) and hardware that is needed (or available) for the system. The potential benefits of the development of this model are:
    - The decisions on the selection of a multi-agent platform and agent architecture for each agent are documented.
    - The design model collects the information of the previously developed models and details how these requirements can be achieved.

- The design model for multi-agent systems determines the common resources and needs of the agents and designs a common infrastructure managed by network agents. This facilitates modularity in the design.

Why this methodology

This methodology enables the developer to build agent-based systems while applying the experiences of pre-agent methodologies and employing familiar techniques and diagrams. MAS-CommonKADS also takes into account reusability at all levels of the models, making it easy to reuse analyses and designs from previous projects.

The design model for multi-agent systems determines the common resources and needs of the agents and designs a common infrastructure managed by network agents. This facilitates modularity in the design.

CHAPTER 4: SYSTEM ANALYSIS, DESIGN AND IMPLEMENTATION

Applying MAS-commonKADS methodology, the models mentioned above will be developed in analysis and design phases;

4.1 Conceptualization

Here we obtain a general description of the problem as described by the users. The aim is to achieve user expectations at the end of offering the solution. Conceptualization will rely heavily on user requirement. Below is some of the key user requirements relied upon on analyzing this project.

What records are we expected to maintain?

- The name, physical and postal address and occupation of the person conducting the transaction or the person on whose behalf the transaction is being conducted.
- The nature, time and date of the transaction
- The type and amount of currency involved.
- The type and identifying number of any account with financial institution

Tell- signs of a suspicious transaction?

- A customer attempts to make frequent or large deposits of currency, insists on dealing only in cash equivalents or asks for exemptions to the firm's policies relating to the deposit of cash and cash equivalents;
- A customer engages in multiple transfers of funds or wire transfers to and from countries that are considered bank secrecy or "tax havens" that have no apparent business purpose or are to or from countries otherwise considered by the firm to be high-risk;
- A customer deposits multiple third party cheques or securities registered to third parties;
- For no apparent reason, a customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers;
- Making over payment for a policy then asking for a refund
- Where you suspect the relationship between a policy holder and the beneficiary is unusual.
- A customer whose main concern is the cancellation terms and not the benefits of the policy.
- Unusually large payments using cash, money orders or travelers cheques

- An individual purchasing a policy and making a claim shortly after.
- A customer who usually purchases small policies suddenly requests a large lump sum contract.
- A customer who wishes to fund his/her policy from a 3rd party
- Premium being paid into one policy from various sources

Monitoring and reporting obligation

- Staff is expected to examine the background and purpose of all complex, unusual, suspicious or large transactions and set out the findings of the same in writing.
- The company will maintain and file reports for all cash transactions exceeding US$ 10,000 or its equivalent in any other currency.
- The company will then forward the same findings to the Financial Reporting Center, to the regulators and/or to the auditors.

Conceptualization is carried out to using user-centered approach to determining the scenarios to help in understanding the user needs and also assist in determining whether the system meets the user expectation. Use cases are used to illustrate the identified roles and interactions are formalized using MSC (Message Sequence Charts)

Example below illustrates the financial institution officer registering new client; role is new customer. New client is register by capturing the client's details e.g. name, date of birth, National Identification number, passport number, nationality, etc.

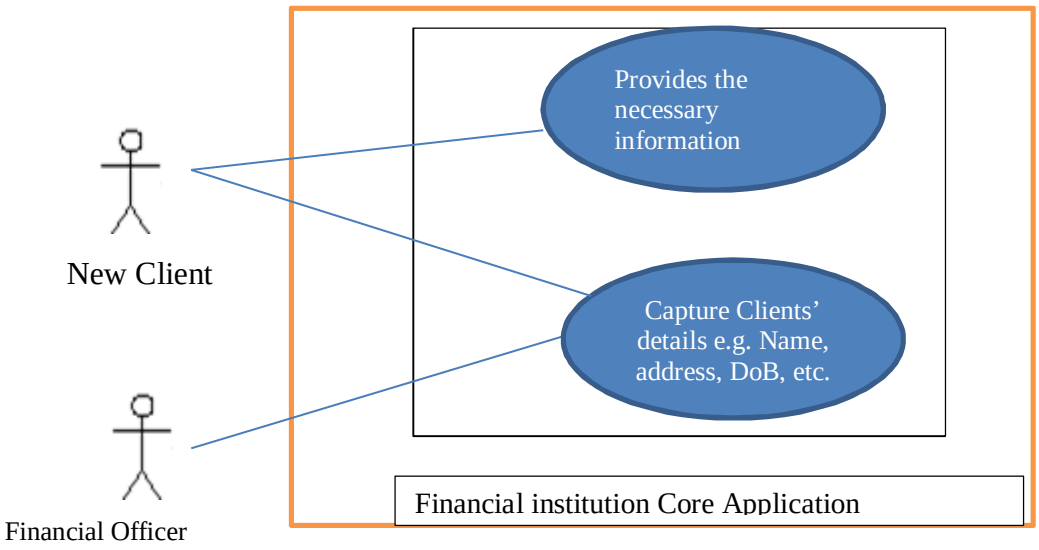

Figure 4: Use case diagram

Applying Know Your Customer policy and requirements needed to open an account, new account is opened or reason is given to the client to meet the necessary requirements. Therefore two scenarios are identified, new account is generated or reason is provided.

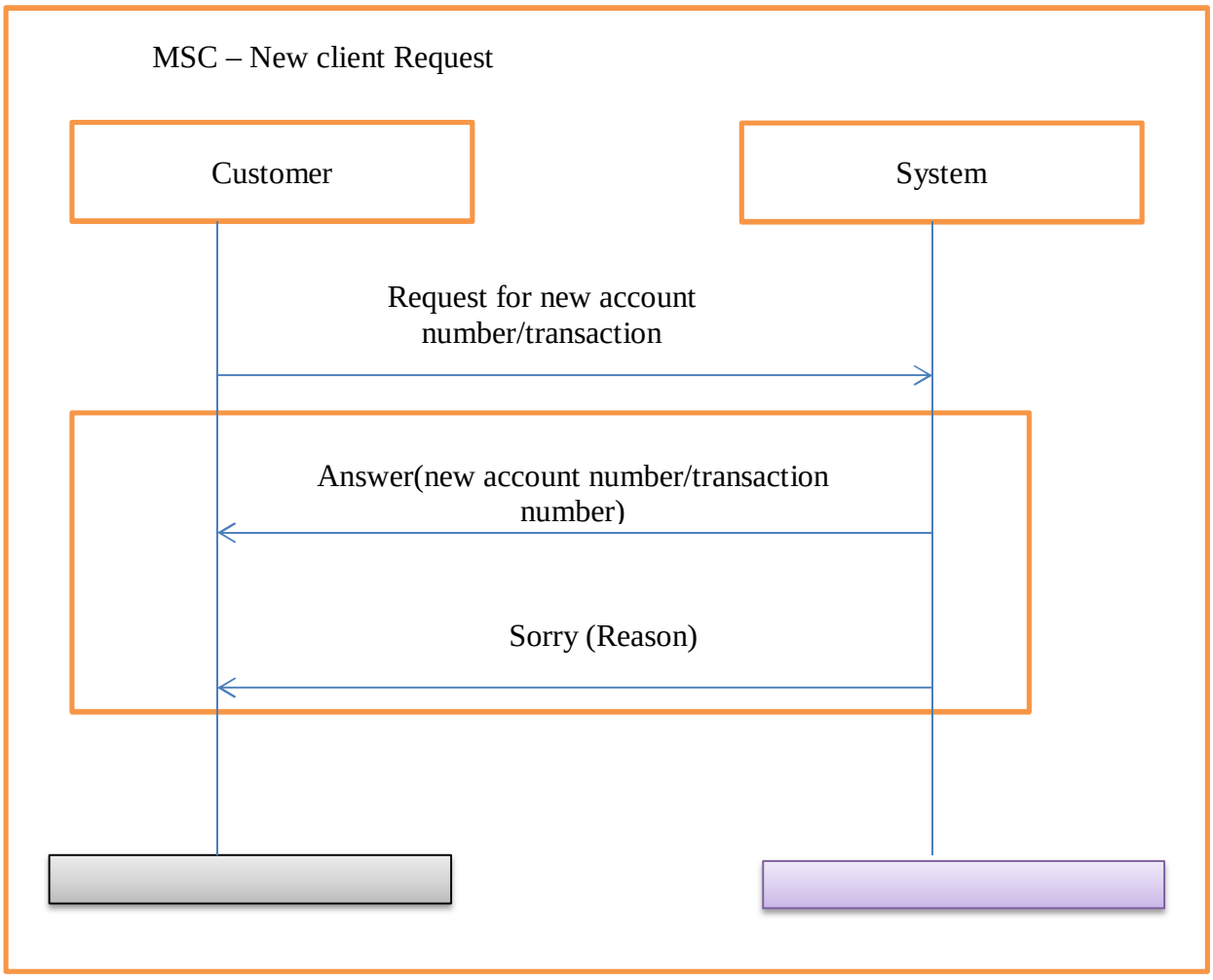

Figure 5: Message Sequence Charts for New client

MSC diagram describes the basic communication between entities and give iteration where need be and decision made.

The table below describes the actors required and identifies corresponding use cases.

Table 2: Actors and use cases

Actor	Description	Use case
client agent	Human interacting with system by registering new customers	Introduce new record/client
Client categorization agent	Software agent to categorize new clients based on their details	Categorize the new client, give recommendations
Watch list Database	List of clients associated to terrorism	Give information of names linked to terrorism

Based on the table above we come up with descriptions of actors and use cases. Example from above is 'categorize new client use cases for actor user agent'.

Table 3: Categorize client use cases for staff agent

Summary: Capture the new of new client and determine whether the clients is associated with terrorism based on watch list database **Actors**: staff and watch list database **Preconditions**: watch list is updated with name of individuals/groups associated with terrorism

During this phase, we also need to factor in activities being executed by financial institution. We shall also seek to understand the banking business processes and the flow of operations. Since we are working on reducing/eliminating terrorism, it is important to find factual data of individuals or organizations listed as suspected by credible institutions e.g. UN sanction list.

Owing to sensitivity and privacy of data information held by financial institutions, this project is guided by data simulation. This project mainly concentrates on those transactions that constitute to anti-money laundering.

To achieve proper agent interactions, below functionalities are key on financial institution to demonstrate anti-money laundering

a) Capture of new clients
b) Obtaining list of suspect individual and organizations aiding terrorism
c) Capturing bank transactions

d) Detect money laundering
e) Reporting suspicious transaction.

From these functionalities, structures necessary were identified (see appendix A)

4.2 Analysis

In analysis, we apply the first six models of MAS – CommonKADS methodology to capture requirement specification of the multi-agent system

Agent model - this model specifies the characteristics of an agent (e.g. skills and roles) and acts as reference point to other models. An agent is an entity either software or human capable of executing an activity. Identification of agents is based on use case diagrams developed in Conceptualization stage. Agents identified in this stage are:

- Client agent- human agent interacting with the system to capture details of new clients
- Watch list agent – software agent that provide information of names associated with terrorism activities
- Source agent –human agent updating the watch list
- Client classifier agent – software agent to categorize clients based to information kept in watch list database
- Transaction agent – agent to keep track of transaction of suspected clients in financial institutions.
- Anti-money laundering agent – software agent to analysis transactions done by suspected clients to determine whether the transactions constitute to money laundering.
- Reporting agent – software agent to either report the money laundering transactions to relevant bodies and/or to stop the transactions altogether.

This methodology defines textual templates for each constituent in order to describe it e.g. table below describes client categorization agent

Table 4: Client classifier agent textual template

Agent: Client Classifier
Name – client classifier **Type** – software agent **Role** – categorize new clients been register to financial institution **Location** – inside agent society **Description** – determines the similarity of the new clients with the names in the watch list database **Exceptions** – use of alias names which are not in the watch list. **Input parameters** – New clients details e.g. name, identification number, address, passport no etc. **Expertise** – this agent must know the details of the information of suspects in the watch list. It should also be able to categorize new clients based on the similarities with the watch list. **Coordination** – coordinate with watch list agent **Communication** – findings should be communicated to suspect agent

Task model – this model describes all activities that should be performed to achieve desired goal. Task is further described by inputs and outputs, the goal of the task, features and control/environmental constrains. Unified Modeling Language (UML) is used to represent the flow of activities. The Unified Modeling Language (UML) is a general-purpose visual modeling language that is used to specify, visualize, construct, and document the artifacts of a software system. It captures decisions and understanding about systems that must be constructed. It is used to understand, design, browse, configure, maintain, and control information about such systems (Rumbaugh, Jacobson and Booch 1999).

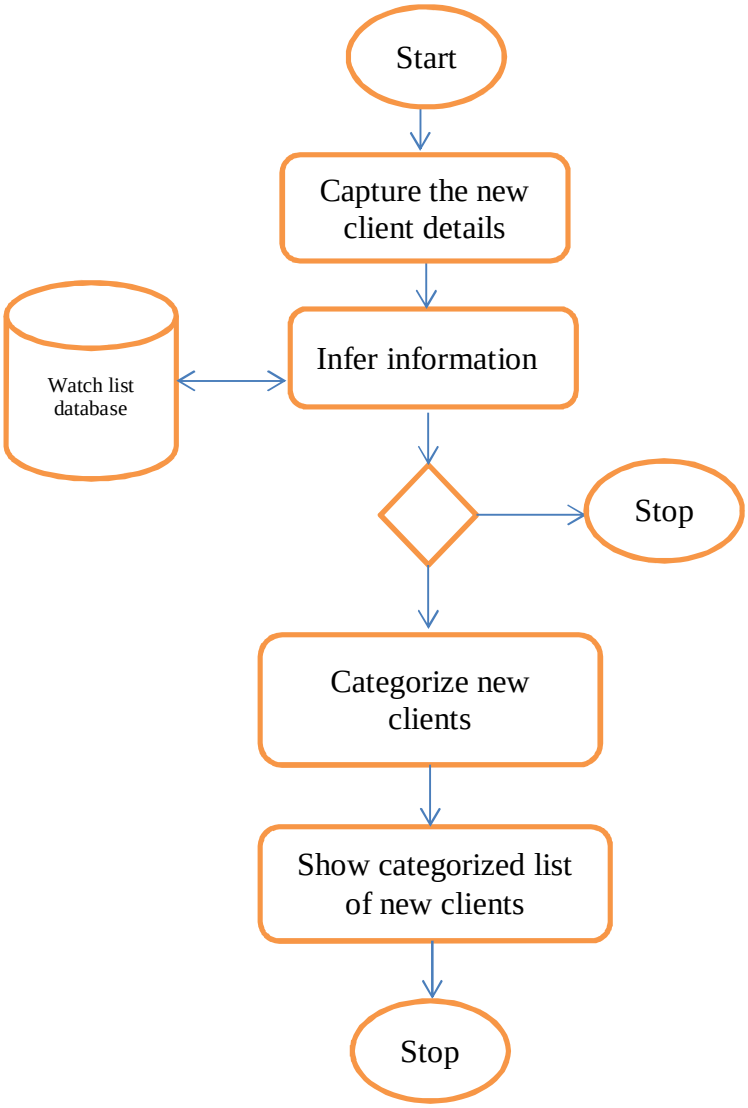

Figure 6: Client categorization agent activity diagram

Table 5: Client categorization agent activity's textual template

Task: infer information
Objective - compare the information of new clients provided by new client agent to information provided by watch list agent Description – have the information from new client agent and information from watch list agent with an aim of categorizing new clients based on this information. Ingredients – client details i.e. name, address, place of birth, etc. Constrains – use of alias names not provided by watch list agents Exceptions – None
Task: Categorize new clients
Objective – flag the client as suspect or non-suspect Description – having compared the similarities of new clients with information in watch list, categorization agent will then categorize new clients having considered pre-determined set rules. Ingredients – name similarities and pre-determined set rules Constrains –None Exceptions –None

Expertise model – describes the knowledge needed by agents in order to carry out their tasks. In order to determine application knowledge, we define the task knowledge which specifies the knowledge needed by a task to accomplish its goal. We define all the agents, generic tasks and knowledge needed by each agent to achieve its goal. We also define the inference knowledge which represents the steps needed to solve a problem.

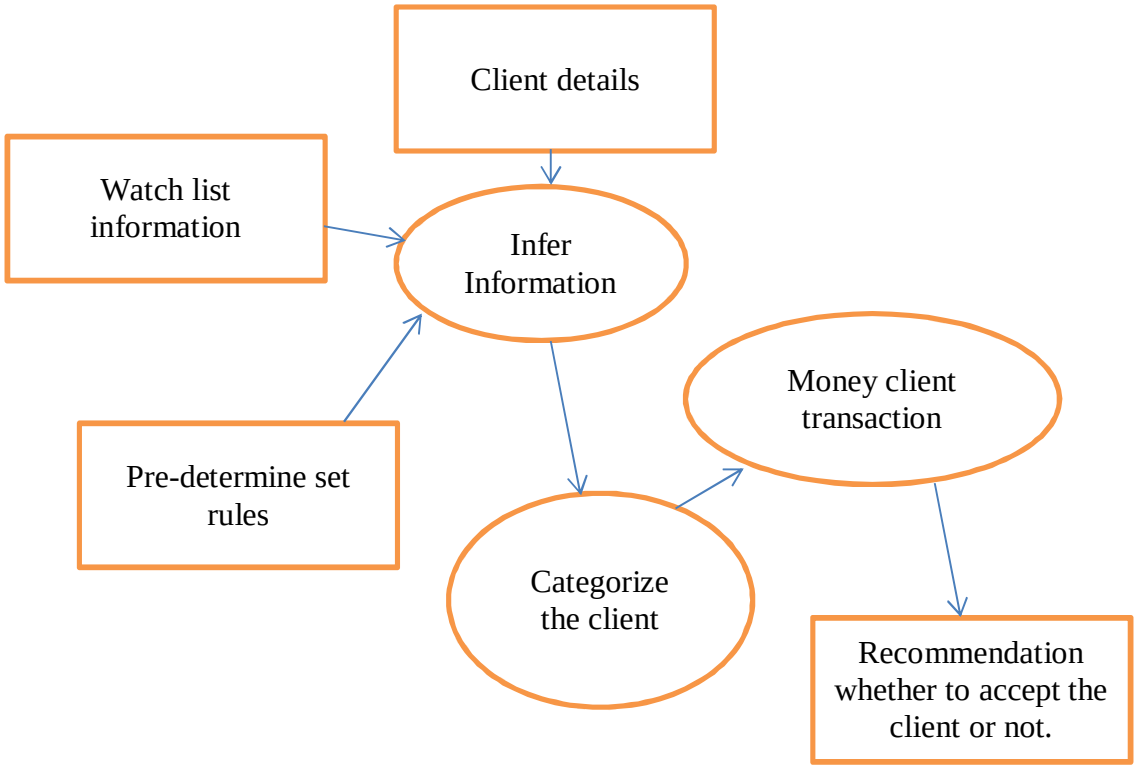

Figure 7: Client Categorization task inferences diagram

The pre-determine set rules are factors that will guide the agent to flag the new client as a suspect or non-suspect.

In the proposed project the naming algorithm is applied to determine the similarities of new clients with names in the watch list. The table below describes the pre-determined set rules

Table 6: Pre-determined client categorization rule.

Client details	Client Categorization Rule
Passport number Identification number Address Occupation …	If the passport number is similar to the name in watch list then check other details

Organization model – it shows structural relationships between the agents.

ConnectorAgent is the main agent; it will be receiving all the communications from all the agents.

Other agents will be beneath it as showed in the diagram below;

Table 7: Organization Model

ConnectorAgent		
TransSniffer Agent		
MoneyLounderAgent		
…		

Coordination model -describes the conversations between agents i.e. their interactions, protocols and required capabilities. The conversations are identified, taking as input the results of the techniques used for identifying agents.

Communication model

Client agent who is a human agent will initiate a transaction on banking system. BankAccountSniffer Agent will sniff the transaction and update the TransSniffer Agent & ConnectorAgent of the new client.

4.3 Design

Application Design

At this phase we take output from analysis as an input the analysis models and transform them into specifications. Detailed description of each agent and it function with a flow diagram.

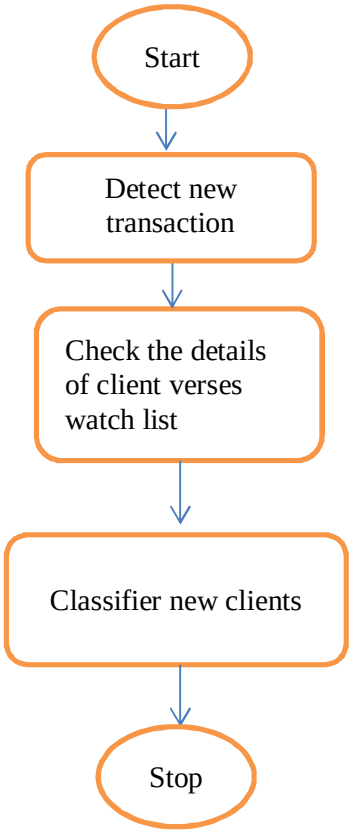

Figure 8: Flow diagram of client classifier Agent

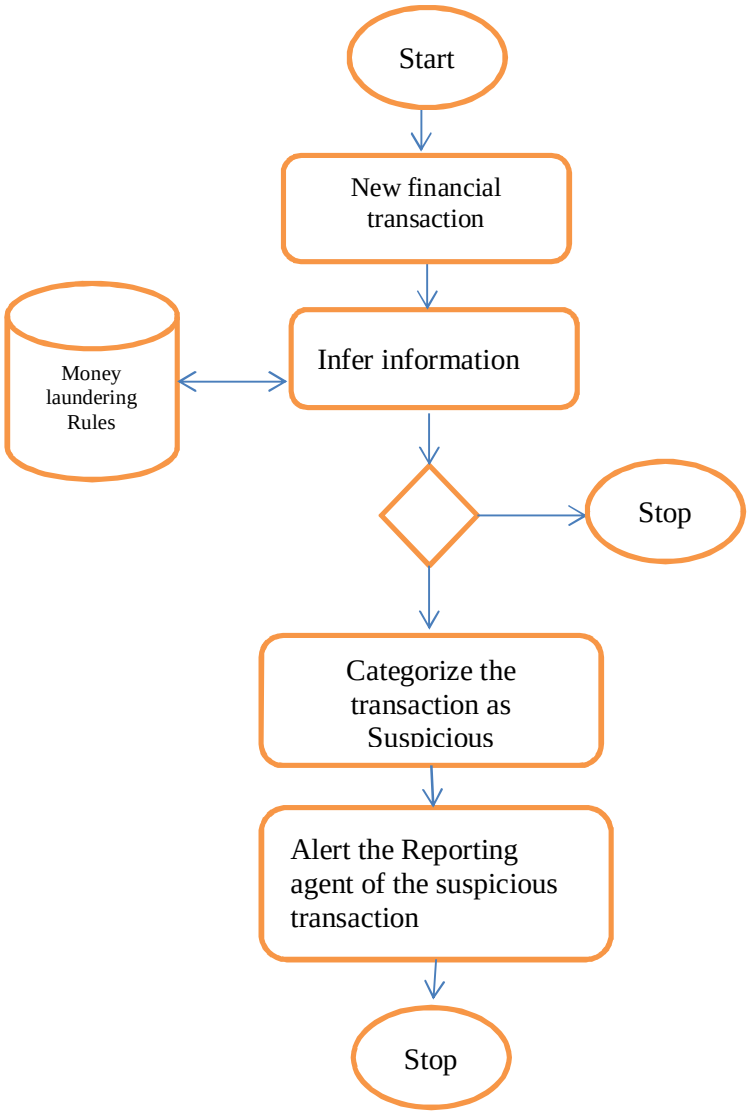

Figure 9: Flow diagram of Money Laundering Agent

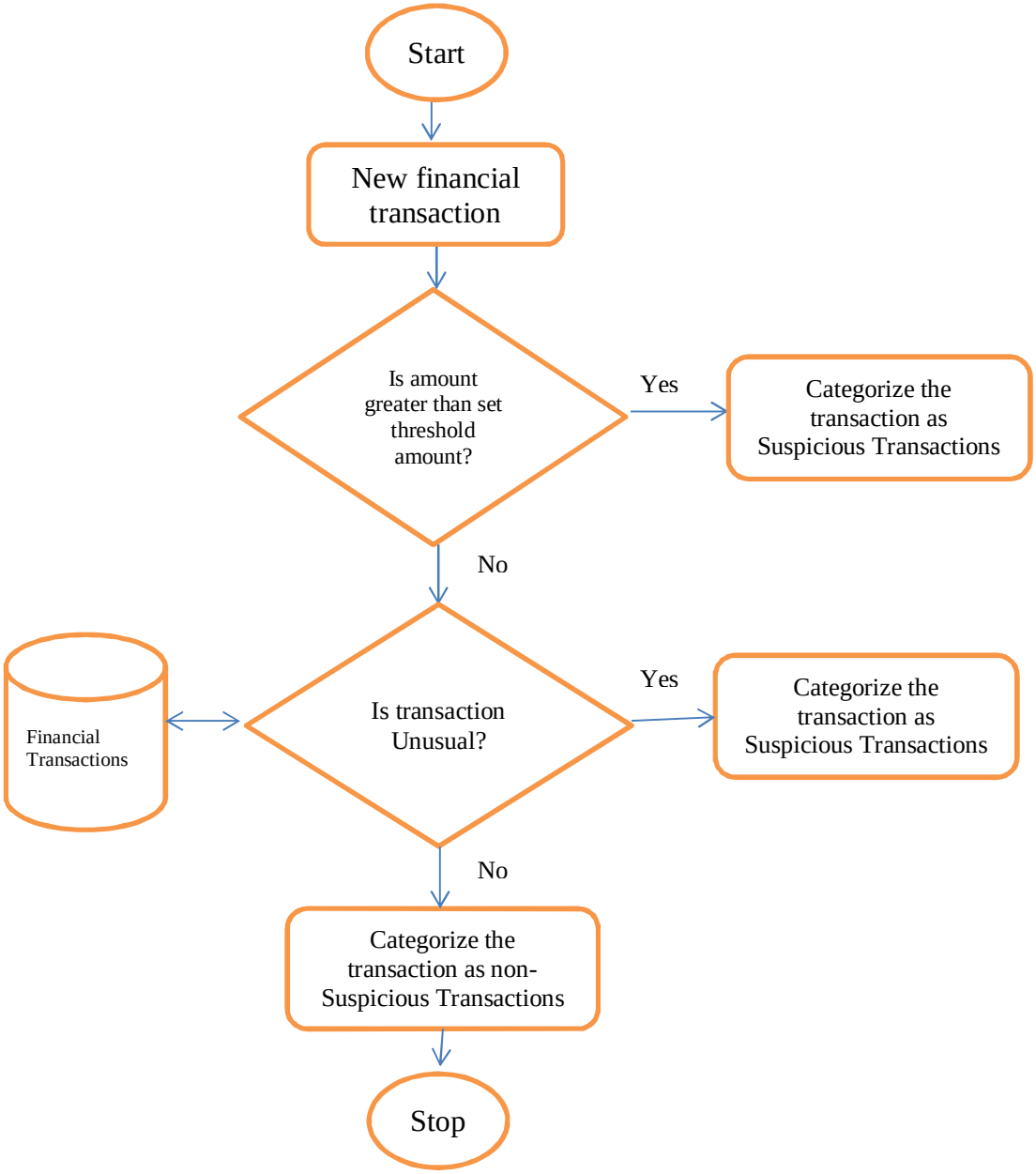

Figure 10: Flow diagram of Money Laundering Rules

Architecture design

Here we concentrate on designing the relevant aspects of the agent network. It captures the overview structure of the project and the major stakeholder/factors that determines the output of the system. Database connectivity was implemented through ODBC

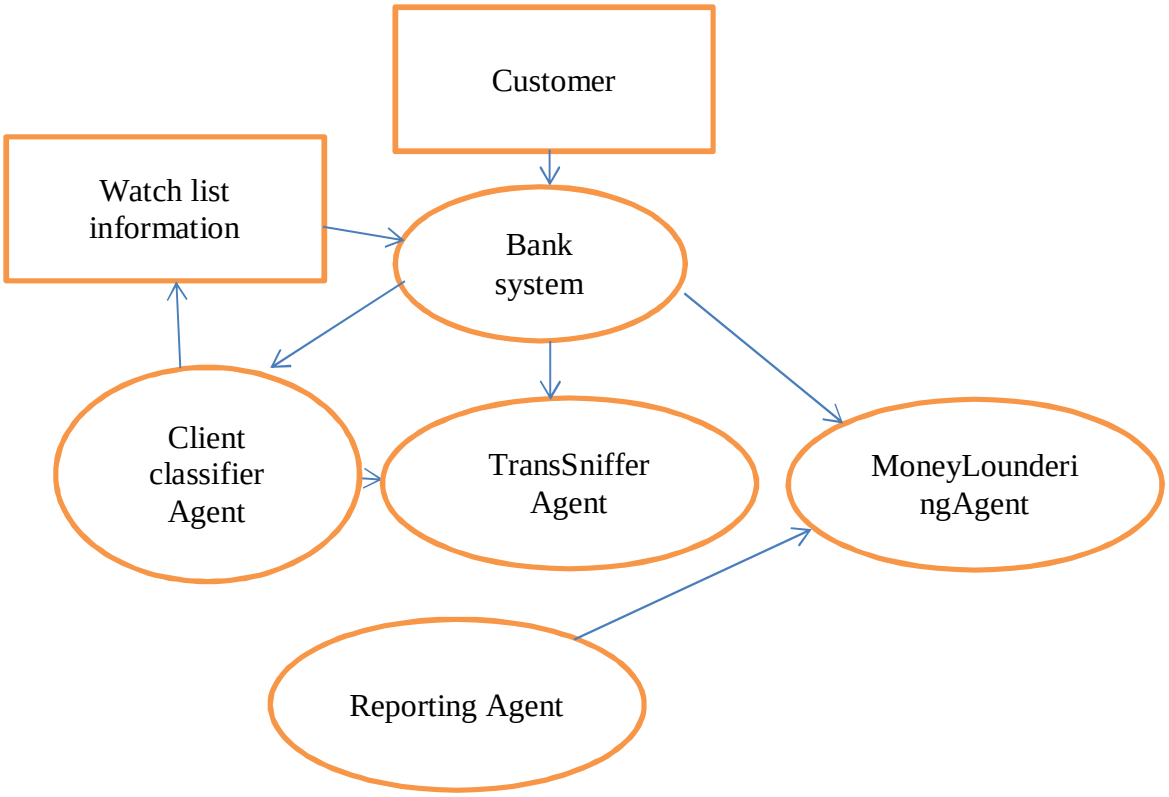

Figure 11: Design Diagram displaying the interaction of agent

Platform design

Here we determine and select the agent development platform for each agent architecture. Graphical User Interface (GUI) was implemented using Windows forms in Visual Studio 2012 (C#.NET 2012); Boris .NET was used to depicts agents' interactions and communication i.e. Multi-agent system; and MySQL database will used to store relevant information.

4.4 Implementation

4.4.1 Implementation of the Model

Implementation involves coming up of user interface screens based on described models mentioned above. It will also involve test the output of the system based of pre-determined outputs.

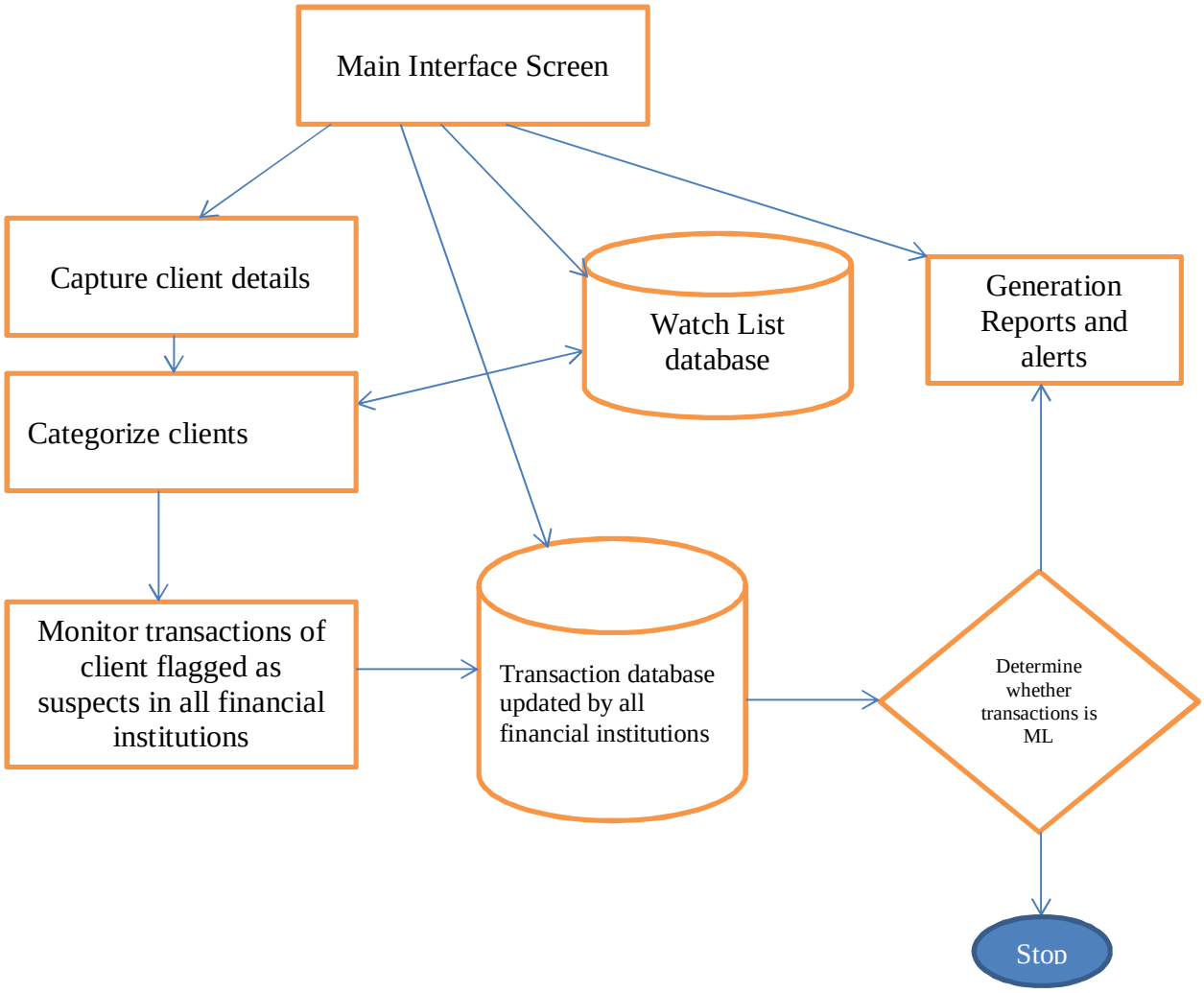

Figure 12: Proposed system interface flow diagram

4.4.2 Database implementation

Because data held by financial institution are private and confidential, data simulation is used as input into a prototype model to simulate real world environment. To perform this simulation, we create several database tables using MYSQL 5.6 Database Management System. Below is a list of tables in the database:

1) tblbankaccounts- used to store bank account details for financial institution clients.
2) tblbanktransactions– used for storing bank transactions.
3) tblwatchlist- used to store a list of suspected individuals and organizations

4) tblwatchlistbankaccounts – stores bank accounts operated by suspected individuals or organizations.

4.4.3 Key algorithms used

1. Matching algorithm: used to compare the similarity of new clients with details in the watch list.
2. Sniffing algorithm: continual monitoring of new clients versus details in the watch list and vice versa.
3. Classifying algorithm: used to classify suspected clients and suspicious transactions

4.4.4 Code Model

For sample code used to develop main functionalities, see Appendix B.

4.4.5 Deployment Mode

The project simulate the normal financial institution transactions including capturing the client details. As the transaction are being executed at the front and/or back office, agents Multi-Agent System will be interacting on the background.

4.5 System Evaluation

The evaluation of the system involved testing the developed model. Testing was broken down into three categories, namely;

a) Unit testing
b) Integration testing
c) System testing.

Unit Testing

At this stage, testing is aimed at verifying the modular functions of the system. It tests the connection of such modules to the database, reading and writing information from and to the database and displaying the results thereafter.

Table 8: The tasks in Unit Testing

Task	Description
UT_0	Running/starting the application
UT_1	Connect the application to the database using ODBC
UT_2	Capturing the details of financial institution clients
UT_3	Classifying the clients based on captured details
UT_4	Sniff the transactions done by suspected clients
UT_5	Classify the transactions (either to be suspicious or non-suspicious)
UT_6	Report the suspicious transactions

Integration Testing

At this stage, we test the interaction of various agents in the environment.

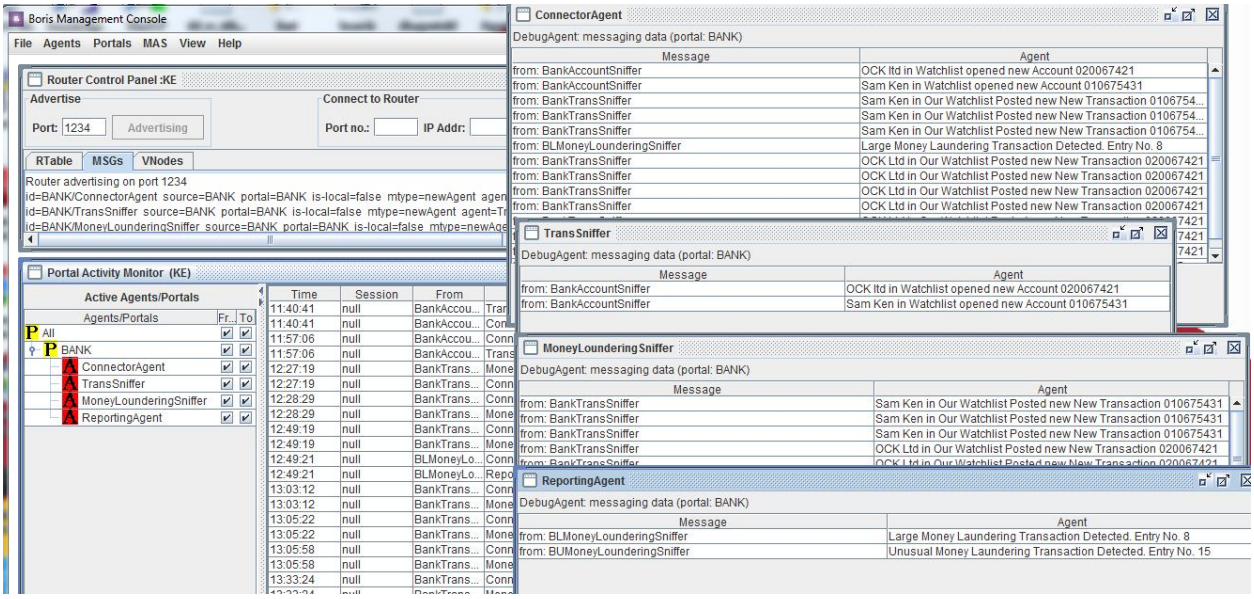

Figure 13: Diagram displaying Agent Interactions

System Testing

System testing was done to confirm that the system was producing expected results given the inputs and variables. Agents' communication was generated to confirm the system outputs.

CHAPTER 5: RESULTS AND DISCUSSION

Here I discuss and analyze the evaluation of the prototype to determine whether it was able to address our problem statement. Discussion has been broken into below categories;

a) Functionality of the prototype
b) Realism of the system

Functionality of the prototype

Outputs/results of unit and integration testing are done to determine whether the prototype model functions as required.

A list of watch list is captured and stored on a central database accessible by all financial institutions. Below table contains a sample list of individuals/organizations on watch list. This database is continuously updated by various bodies.

Table 9: Watch List table

Name	Client Type	Original Name	DoB	POB	AKA	Passport/ PIN No	Passport Date	Passport Place	IDNo	Place of Issue
Dav Charles	Individual	Koliech	10/29/1975	Kwale	Dalama	A12132423PL	10/29/2015	Kenya nairobi	3213124432	Nairobi
Jane Mercy	Individual	Mercy	10/29/1975	Kwale	Dalama	A12132423PLT	10/29/2015	Kenya nairobi	3213124432	Nairobi
OCK ltd	Organisation	Ock limited	3/3/2014		OCK	P012345678Q	3/3/2014	Kenya		Nairobi
Peter Paul	Individual	Mwangi	10/29/1965	Kwale	Dalama	D2234235345	10/29/2010	Kenya nairobi	212432543	Nairobi
Sam Ken	Individual	Samwuel	10/29/1965	Kwale	Dalama	D22342389F	10/29/2010	Kenya nairobi	21243254	Nairobi

Test: Capturing the details of financial institution clients considering KYC

Results: Clients details are captured by filling in all the mandatory fields.

Discussion & Analysis

Success capturing of client's details - Clients are classified by comparing similarities with those on watch list. BankAccountSniffer and InsuranceAccountSniffer agent sniffs new client details and report to TransSniffer agent

Agents were able to detect/sniff the opening of new accounts by individuals/organizations under watch list. Below are agents' communication pertaining the same.

Table 10: New clients on watch list

No	CommDate	Time	ID	From	To	Message
1	1/31/2016	11:40:42	1	BankAccountSniffer	ConnectorAgent	OCK ltd in Watchlist opened new Account 020067421
2	1/31/2016	11:40:42	1	BankAccountSniffer	TransSniffer	OCK ltd in Watchlist opened new Account 020067421
3	1/31/2016	11:57:06	1	BankAccountSniffer	ConnectorAgent	Sam Ken in Watchlist opened new Account 010675431
4	1/31/2016	11:57:06	1	BankAccountSniffer	TransSniffer	Sam Ken in Watchlist opened new Account 010675431
27	1/31/2016	14:00:21	1	InsuranceAccountSniffer	ConnectorAgent	Sam Ken in Watchlist opened new Account 001070178
28	1/31/2016	14:00:21	1	InsuranceAccountSniffer	TransSniffer	Sam Ken in Watchlist opened new Account 001070178

Below is pictorial communication between agents on new account opening.

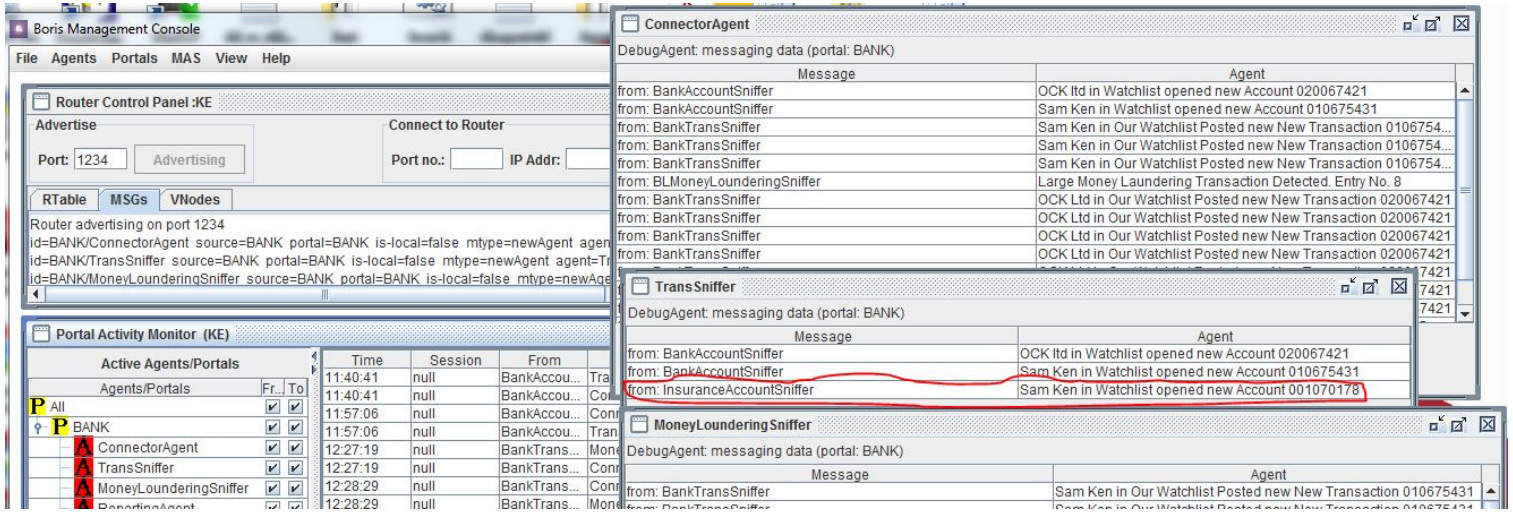

Figure 14: Agents' communication – New clients

This demonstrates that agents are intelligent and only sniff an account that belongs/hold by individuals on watch list.

Based on watch list, below accounts were tagged as watch list accounts and hence the need to monitor their transactions closely.

Table 11: Suspected Accounts

Institution	ClientType	AccountName	AccountNumber	Branch	DoB	Accountdate	Nationality	IDNo	Address	PassportNo	PassportPlace	Telephone	Status
BANK	Organisation	OCK Ltd	20067421	Ksm	1/6/2015	12/8/2015	Kenya	P012345678Q	Box 7 Ksm	P012345678Q	Nairobi		Active
BANK	Individual	Sam Ken	10675431	Kwale	1/4/1965	1/2/2009	Kenyan	21243254	Box 76 Kwale	D22342389F	Mombasa	030-00001	Active
INSURANCE	Individual	Sam Ken	1070178	Mombasa	1/4/1965	1/31/2016	Kenyan	21243254	Box 76 Kwale	D22342389F	Mombasa	030-00001	Active

A total of 40 transactions were transacted in various financial institutions to test the viability of this solution.

Below is the list of transactions both from banking and insurance institutions

Table 12: Financial Institution transactions

No	Institution	AccountNo	Account Name	Account Branch	Transaction Type	Amount	Transaction Date	Transaction Branch	Beneficiary AccName	Beneficiary AccNo	Beneficiary Bank	Beneficiary Branch	Beneficiary Country	Currency	Time
1	BANK	1000001	Charles Kip	Tombaya	Cash Deposit	5000	1/6/2016	Capital Hill	James Kip	7886454	Bank of India	Haile Silasi	Kenya	USD	12:22:24
2	BANK	10675431	Sam Ken	Kwale	Cash Deposit	6000	12/2/2015	Ksm	James Kip	55321	KCB	Kco	Kenya	USD	12:22:24
3	BANK	10675431	Sam Ken	Kwale	Cash Deposit	5000	12/2/2015	Ksm	Sam Kip	7886421	KCB	Ksm	Kenya	USD	12:22:24
4	BANK	5315312	Sam Imara	Thika	Cash Withdrawal	8000	1/12/2016	Embu	Philip Imara	7786341	Family	Nairobi	Kenya	KES	12:37:06
5	BANK	7785432	Ben Ban	Mks	EFT	8000	12/10/2015	Mlolongo	YYT ltd	676543	Equity	Machakos	Kenya	KES	12:37:06
6	BANK	7785432	Ben Ban	Mks	RTGS	87000	12/8/2015	Kitengela	Musyoka	887643	Rafiki	Machakos	Kenya	KES	12:37:06
7	BANK	7785432	Ben Ban	Mks	Cash Deposit	7600	12/11/2015	Kitengela	Peter A	878097	Co-op	Namanga	Kenya	KES	12:37:06
8	BANK	10675431	Sam Ken	Kwale	Cash Deposit	11000	12/11/2015	Mombasa	Osambe ltd	7754331	Ecq	Kakamega	Kenya	USD	12:37:06
9	BANK	20067421	OCK Ltd	Ksm	Cash Deposit	7000	12/1/2015	Kisumu	Ock ltd	6785796	Bank of Kigali	Capital hill	Korea	EURO	12:37:06
10	BANK	20067421	OCK Ltd	Ksm	RTGS	8000	12/9/2015	Kisumu	YYRU Ltd	67875	Equity	Uyt	Korea	EURO	12:37:06
11	BANK	20067421	OCK Ltd	Ksm	RTGS	7500	12/10/2015	Kisumu	YYRU Ltd	67875	Equity	Uyt	Korea	EURO	12:37:06
12	BANK	20067421	OCK Ltd	Ksm	Cash Deposit	9000	1/31/2016	Kitale	EREW ltd	9976537	UYG	IUU	Korea	EURO	13:32:01
13	BANK	20067421	OCK Ltd	Ksm	Bankers Check	8500	12/14/2015	Eldoret	EREW ltd	9977537	UYG	IUU	Korea	EURO	13:32:01
14	BANK	20067421	OCK Ltd	Ksm	Bankers Check	9500	12/15/2015	Eldoret	EREW ltd	9977537	UYG	IUU	Korea	EURO	13:32:01
15	BANK	20067421	OCK Ltd	Ksm	Bankers	29500	12/15/20	Kisumu	EREW ltd	9977537	UYG	IUU	Korea	EURO	13:32:

					Check		15								01
No	**Institution**	**AccountNo**	**Account Name**	**Account Branch**	**Transaction Type**	**Amount**	**Transaction Date**	**Transaction Branch**	**Beneficiary AccName**	**Beneficiary AccNo**	**Beneficiary Bank**	**Beneficiary Branch**	**Beneficiary Country**	**Currency**	**Time**
16	BANK	5315312	Sam Imara	Thika	Cash Withdrawal	80000	12/21/2015	Thika	Sam Imara	5315312	Equity	Thika	Kenya	KES	13:40:37
17	BANK	5315312	Sam Imara	Thika	RTGS	10000	12/21/2015	Thika	Tom Peter	778643	ECQ	Kco	Kenya	KES	13:40:37
18	BANK	20067691	ABDT Ltd	Nbi	Bankers Check	11000	12/22/2015	Tharaka	TYYY	554322	KCB	Kitui	Kenya	USD	13:44:37
19	BANK	20067691	ABDT Ltd	Nbi	Cash Deposit	9000	12/23/2015	Thika	TYYY	554322	KCB	Kitui	Kenya	USD	13:44:37
20	BANK	7785432754	Mark Peter	Mbs	Cash Deposit	7800	12/15/2015	Mombasa	Peter Jerry	7954312	ECQ	Kisumu	Kenya	KES	13:47:40
21	BANK	7785432754	Mark Peter	Mbs	Cash Withdrawal	10000	12/15/2015	Mombasa	Mark Peter	7.785E+09	ECQ	Mombasa	Kenya	KES	13:47:40
22	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	10000	8/4/2015	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:00:44
23	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	10000	9/4/2015	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:00:44
24	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	10000	10/5/2015	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:00:44
25	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	40000	12/4/2015	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:00:44
26	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	10000	1/6/2016	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:00:44
27	INSURANCE	2080001	KBT ltd	Nairobi	Cash Deposit	60000	1/31/2016	Nbi	KBT Ltd	2080001	Cic	CBD branch	Kenya	KES	14:43:42
28	INSURANCE	2080001	KBT ltd	Nairobi	Cash Deposit	60000	11/3/2015	Nbi	KBT Ltd	2080001	Cic	CBD branch	Kenya	KES	14:43:42
29	INSURANCE	2080001	KBT ltd	Nairobi	Cash Deposit	70000	9/7/2015	Nbi	KBT Ltd	2080001	Cic	CBD branch	Kenya	KES	14:43:42
30	INSURAN	2080001	KBT ltd	Nair	Cash	10000	1/7/2015	Nbi	KBT Ltd	2080001	Cic	CBD	Kenya	KES	14:43:

	CE			obi	Deposit	0						branch			42
No	**Institution**	**AccountNo**	**Account Name**	**Account Branch**	**Transaction Type**	**Amount**	**Transaction Date**	**Transaction Branch**	**Beneficiary AccName**	**Beneficiary AccNo**	**Beneficiary Bank**	**Beneficiary Branch**	**Beneficiary Country**	**Currency**	**Time**
31	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	1000	2/5/2015	Nbi	KBT Ltd	1070178	Cic	Mombasa	Kenya	KES	14:43:42
32	BANK	20067691	ABDT Ltd	Nbi	RTGS	10000	11/3/2014	Ngara	Audre ltd	6754375	Trans	Kunyak	Kenya	KES	14:51:56
33	BANK	20067691	ABDT Ltd	Nbi	RTGS	70000	11/4/2015	Ngara	Audre ltd	6754375	Trans	Kunyak	Kenya	KES	14:51:56
34	BANK	20067691	ABDT Ltd	Nbi	Cash Deposit	2000	1/3/2015	Nbi	ABDT ltd	20067691	Eq	Kile	Kenya	KES	14:55:26
35	INSURANCE	1070178	Sam Ken	Mombasa	Cash Withdrawal	70000	5/28/2015	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:59:43
36	INSURANCE	1070178	Sam Ken	Mombasa	Cash Withdrawal	40000	1/28/2016	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:59:43
37	BANK	5315312	Sam Imara	Thika	Cash Deposit	1000	1/31/2016	Thika	PULENI	997754	BOI	MUMBUA	India	USD	15:03:03
38	BANK	5315312	Sam Imara	Thika	Cash Deposit	1000	1/5/2016	Thika	Audre Ltd	78943	ECQ	Kigali	Rwanda	USD	15:03:03
39	BANK	1000001	Charles Kip	Tombaya	Cash Withdrawal	2000	10/1/2015	Kisii	Charles Kip	1000001	EQ	Tomboya	Kenya	KES	15:06:03
40	BANK	20067421	OCK Ltd	Ksm	Cash Deposit	9000	1/4/2016	Kisumu	Tyramid	668633	KCB	Moyale	Kenya	USD	15:08:08

Out of the many transactions above, below are transactions executed by through tagged accounts

Table 13: Tagged financial transactions

No	**Institution**	**Account No**	**Account Name**	**Account Branch**	**Transaction Type**	**Amount**	**Transaction Date**	**Transaction Branch**	**Beneficiary AccName**	**Beneficiary AccNo**	**Beneficiary Bank**	**Beneficiary Branch**	**Beneficiary Country**	**Currency**	**Time**
2	BANK	10675431	Sam Ken	Kwale	Cash Deposit	6000	12/2/2015	Ksm	James Kip	55321	KCB	Kco	Kenya	USD	12:22:24
3	BANK	10675431	Sam Ken	Kwale	Cash Deposit	5000	12/2/2015	Ksm	Sam Kip	7886421	KCB	Ksm	Kenya	USD	12:22:24

8	BANK	10675431	Sam Ken	Kwale	Cash Deposit	11000	12/11/2015	Mombasa	Osambe ltd	7754331	Ecq	Kakamega	Kenya	USD	12:37:06
9	BANK	20067421	OCK Ltd	Ksm	Cash Deposit	7000	12/1/2015	Kisumu	Ock ltd	6785796	Bank of Kigali	Capital hill	Korea	EURO	12:37:06
10	BANK	20067421	OCK Ltd	Ksm	RTGS	8000	12/9/2015	Kisumu	YYRU Ltd	67875	Equity	Uyt	Korea	EURO	12:37:06
11	BANK	20067421	OCK Ltd	Ksm	RTGS	7500	12/10/2015	Kisumu	YYRU Ltd	67875	Equity	Uyt	Korea	EURO	12:37:06
12	BANK	20067421	OCK Ltd	Ksm	Cash Deposit	9000	1/31/2016	Kitale	EREW ltd	9976537	UYG	IUU	Korea	EURO	13:32:01
13	BANK	20067421	OCK Ltd	Ksm	Bankers Check	8500	12/14/2015	Eldoret	EREW ltd	9977537	UYG	IUU	Korea	EURO	13:32:01
14	BANK	20067421	OCK Ltd	Ksm	Bankers Check	9500	12/15/2015	Eldoret	EREW ltd	9977537	UYG	IUU	Korea	EURO	13:32:01
15	BANK	20067421	OCK Ltd	Ksm	Bankers Check	29500	12/15/2015	Kisumu	EREW ltd	9977537	UYG	IUU	Korea	EURO	13:32:01
22	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	10000	8/4/2015	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:00:44
23	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	10000	9/4/2015	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:00:44
24	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	10000	10/5/2015	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:00:44
25	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	40000	12/4/2015	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:00:44
26	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	10000	1/6/2016	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:00:44
31	INSURANCE	1070178	Sam Ken	Mombasa	Cash Deposit	1000	2/5/2015	Nbi	KBT Ltd	1070178	Cic	Mombasa	Kenya	KES	14:43:42
35	INSURANCE	1070178	Sam Ken	Mombasa	Cash Withdrawal	70000	5/28/2015	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:59:43
36	INSURANCE	1070178	Sam Ken	Mombasa	Cash Withdrawal	40000	1/28/2016	Mombasa	Sam Ken	1070178	Cic	Kilifi	Kenya	KES	14:59:43

Test: The transactions execution (clients in watch list)

Results: Client transact with financial institution (Valid)

Discussion & Analysis

Success execution of transaction - BankTransSniffer agent sniffs all transactions done by suspected individuals/Organizations. MoneyLounderingSniffer is informed of the transaction.

Here is the communication agents' on transactions done by accounts tagged as watch list accounts

Table 14: Transactions by suspected individuals/Organizations

No	CommDate	Time	ID	From	To	Message
6	1/31/2016	12:27:20	1	BankTransSniffer	MoneyLounderingSniffer	Sam Ken in Our Watchlist Posted new New Transaction 010675431
8	1/31/2016	12:28:30	1	BankTransSniffer	MoneyLounderingSniffer	Sam Ken in Our Watchlist Posted new New Transaction 010675431
10	1/31/2016	12:49:19	1	BankTransSniffer	MoneyLounderingSniffer	Sam Ken in Our Watchlist Posted new New Transaction 010675431
14	1/31/2016	13:03:12	1	BankTransSniffer	MoneyLounderingSniffer	OCK Ltd in Our Watchlist Posted new New Transaction 020067421
16	1/31/2016	13:05:23	1	BankTransSniffer	MoneyLounderingSniffer	OCK Ltd in Our Watchlist Posted new New Transaction 020067421
18	1/31/2016	13:05:59	1	BankTransSniffer	MoneyLounderingSniffer	OCK Ltd in Our Watchlist Posted new New Transaction 020067421
20	1/31/2016	13:33:24	1	BankTransSniffer	MoneyLounderingSniffer	OCK Ltd in Our Watchlist Posted new New Transaction 020067421
22	1/31/2016	13:34:55	1	BankTransSniffer	MoneyLounderingSniffer	OCK Ltd in Our Watchlist Posted new New Transaction 020067421
24	1/31/2016	13:35:24	1	BankTransSniffer	MoneyLounderingSniffer	OCK Ltd in Our Watchlist Posted new New Transaction 020067421
26	1/31/2016	13:36:02	1	BankTransSniffer	MoneyLounderingSniffer	OCK Ltd in Our Watchlist Posted new New Transaction 020067421
30	1/31/2016	14:08:56	1	InsuranceTransSniffer	MoneyLounderingSniffer	Sam Ken in Our Watchlist Posted new New Transaction 001070178
32	1/31/2016	14:09:11	1	InsuranceTransSniffer	MoneyLounderingSniffer	Sam Ken in Our Watchlist Posted new New Transaction 001070178
34	1/31/2016	14:09:35	1	InsuranceTransSniffer	MoneyLounderingSniffer	Sam Ken in Our Watchlist Posted new New Transaction 001070178
36	1/31/2016	14:10:10	1	InsuranceTransSniffer	MoneyLounderingSniffer	Sam Ken in Our Watchlist Posted new New Transaction 001070178
40	1/31/2016	14:35:09	1	InsuranceTransSniffer	MoneyLounderingSniffer	Sam Ken in Our Watchlist Posted new New Transaction 001070178
42	1/31/2016	14:50:26	1	InsuranceTransSniffer	MoneyLounderingSniffer	Sam Ken in Our Watchlist Posted new New Transaction 001070178
44	1/31/2016	15:02:02	1	InsuranceTransSniffer	MoneyLounderingSniffer	Sam Ken in Our Watchlist Posted new New Transaction 001070178
46	1/31/2016	15:02:30	1	InsuranceTransSniffer	MoneyLounderingSniffer	Sam Ken in Our Watchlist Posted new New Transaction 001070178
48	1/31/2016	15:09:21	1	BankTransSniffer	MoneyLounderingSniffer	OCK Ltd in Our Watchlist Posted new New Transaction 020067421

Below is pictorial representing agents' communication

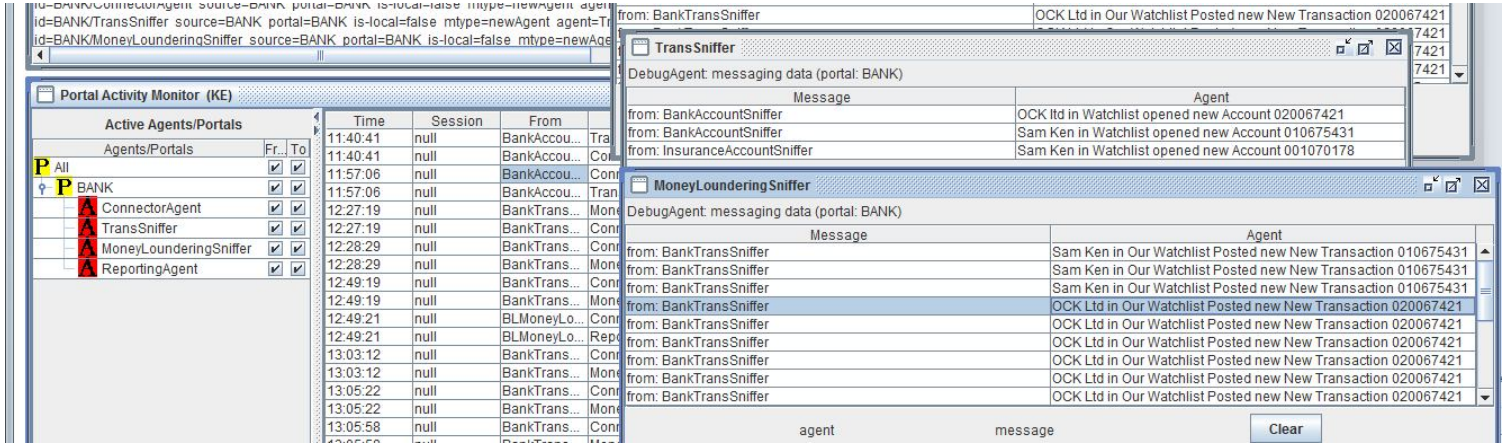

Figure 15: Agents' communication – tagged transactions

Test: The transactions execution (either to be suspicious or non-suspicious)

Results: Client transact with financial institution (Valid)

Discussion & Analysis

Money laundering agents determine whether the transaction meets the threshold to be considered as money laundering transaction. Transaction will be classified and if it amounts to Money laundering, ReportingAgent is informed of suspicious transaction.

Transactions that amount to money laundering are supposed to be reported as suspicious transactions. MoneyLounderingSniffer agent was able to detect and report these transactions to reporting agent for actions as demonstrated below.

Table 15: Suspicious Transactions

No	CommDate	Time	ID	From	To	Message
12	1/31/2016	12:49:22	1	BLMoneyLounderingSniffer	ReportingAgent	Large Money Laundering Transaction Detected. Entry No. 8
38	1/31/2016	14:10:13	1	IUMoneyLounderingSniffer	ReportingAgent	Unusual Money Laundering Transaction Detected. Entry No. 25

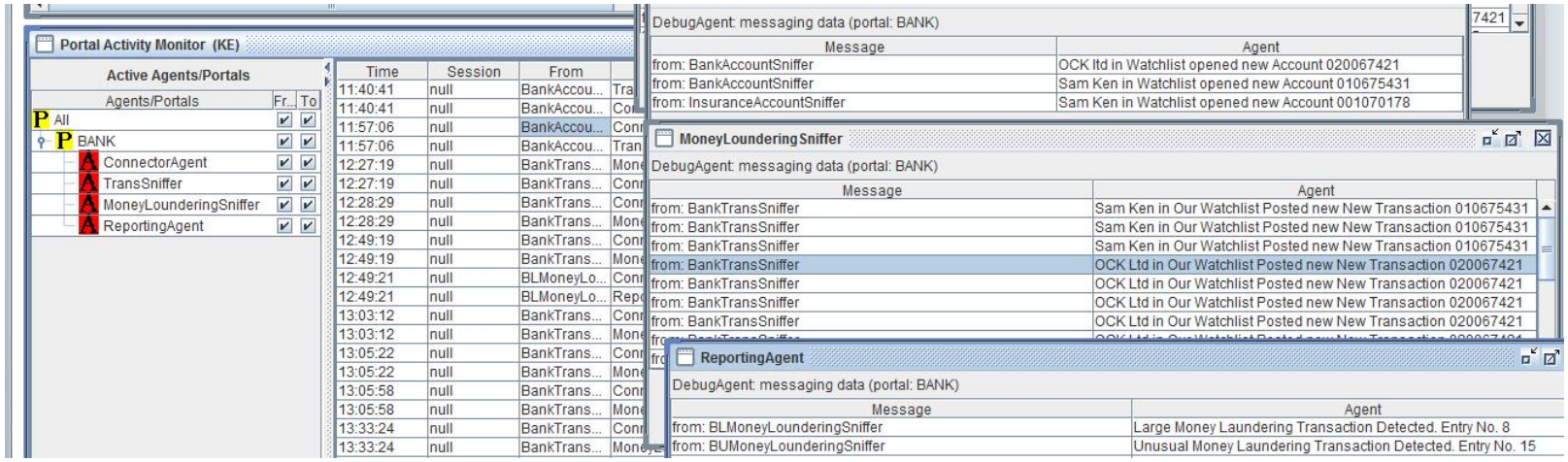

Figure 16: Agents' communication –Suspicious transactions

The first instance was large amount beyond threshold being transacted. The second instance is unusual transaction based on historical transactions done through the specified account.

Test: Agents interaction

Results: Sniffer agents sniff new transaction and communicated the same to other agents (Valid)

Discussion and Analysis

a) Agents were able to detect suspicious transactions

b) Each agent works autonomously to achieve its task.

c) All agents interact and cooperate to achieve a common goal

Realism of the system

Here we determine whether the model can be applied in the real world. Having discussed earlier that the main source of funds for terrorist is through money laundering and due to complex nature of money laundering in financial institutions, the proposed system seeks to reduce and/or eliminate terrorism by detecting money laundering activities.

System functionality discussed above demonstrates the workability of the proposed system in real world environment. New clients accounts opened and new transactions are detected on real time basis by sniffer agents.

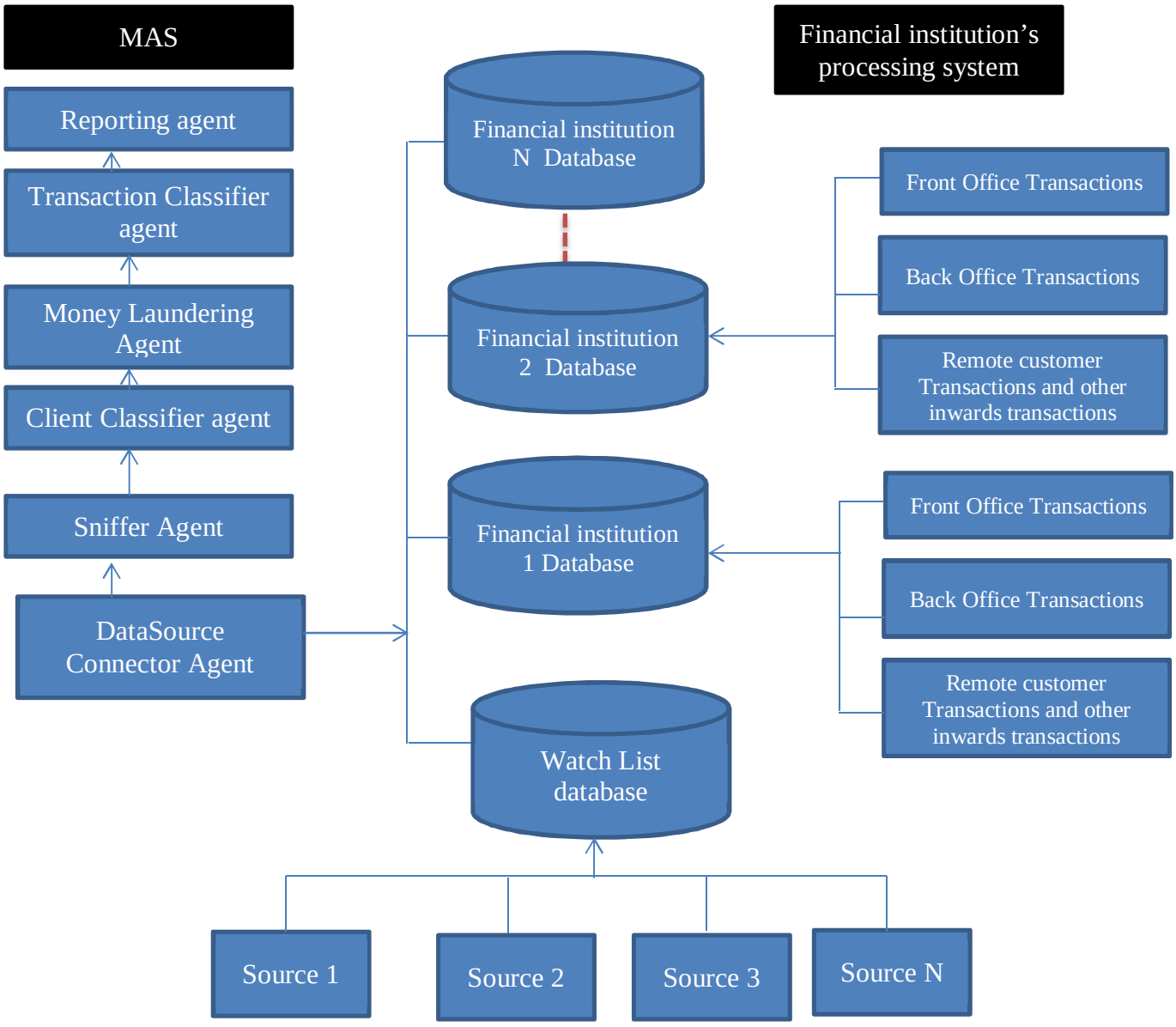

Figure 17: Deployment Mode Diagram

DataSource Agent – Generate a connection to various databases, namely watch list database and financial institution's databases (i.e. from 1 to N)

Sniffer Agent – monitor new transactions

Classifier agent A – will classify the financial institutions' clients at the time of registration or at any given time when watchlist database is updated.

Classifier agent B - will classify the transaction transacted by or in favour of individuals/organizations in watchlist database.

Reporting agent – will report suspicious transactions.

See sample demonstration on Appendix C

CHAPTER 6: CONCLUSION, RECOMMENDATIONS AND FUTURE WORKS

6.1 Conclusion

Money Laundering and terrorism financing pose a serious threat of stability and integrity of national states, Kenya included. Money launderer keep on inverting new ways of laundering illegally acquired funds/money and injection them into the economy. Complex and dynamic measures and mechanisms are therefore needed to stop or eliminate the menace. This is project is a multi-agent solution and is capable of handling sophisticated mechanisms using intelligent and autonomous agents on real time bases.

In line with FATF recommendation that stipulates that all financial institution to submit Suspicious Transaction Reports (STR) to relevant regulatory bodies, quality reporting will dependent on the effectiveness of controls put in place. If the proposed system is implemented, the central center will be in a position to detect suspicious transactions on real time basis. Since time is of essence in detecting money laundering, such bodies will be able to investigate the suspicious transaction and take necessary actions in good time.

Eliminating/controlling money laundering which forms that main source of income to terrorist will reduce the amount of funds on their disposal hence reduction in terrorism activities.

6.2 Recommendations

In Kenya, FRC the central Centre whose main objective is to assist in the identification of the proceeds of crime and the combating of money laundering is relying on financial institutions to send them suspicious transactions. I recommend this solution to be used by such institutions since the agents involved are intelligent enough to sniff for suspicious without much manual intervention.

6.3 Future works

- Sophisticated agents tools can be employed in future to display and publish suspicious transactions on almost real time.
- To eliminate terrorism regionally or globally, this model can be expanded in future to regional states.

References

1 Kariuki, O.K., Opiyo, E.T.O. and Okello, O. (2014). *Multi-Agent Based Anti-Money Laundering System*, Trends in Distributed Computing Applications.

2 Simon, H.A. (1977). *The new science of management decision*, Englewood Cliffs, N.J., Prentice-Hall.

3 Franklin, S. and Graesser, A. (1996). Is it an agent, or just a program*?* in: J. Muller, M. Wooldridge and N. Jennings, Eds., *Intelligent agents III: agent theories, architectures, and language::* ECAI'96 Workshop (ATAL), Budapest, Hungary, August 12-13, 1996 proceedings, Springer-Verlag, Berlin, 1997, 1 – 20.

4 Gao, S. and Xu, D. (2006). Conceptual Modelling and Development of an Intelligent Agent-Assisted Decision Support System for Anti-Money Laundering. In: The 11th Annual Conference of Asia Pacific Decision Sciences Institute (APDSI 2006). *The 11th Annual Conference of Asia Pacific Decision Sciences Institute (APDSI 2006)*, Kowloon, Hong Kong, (241-244). 14-18 June, 2006.

5 Wooldridge, M. & Jennings, N.R. (1995). *Intelligent agents: theory and practice*, Knowledge Engineering Review, 10(2), 115 – 152.

6 Wooldridge, M. (1999). Intelligent agents, in: G. Weiss, Ed., *Multiagent systems: a modern approach to distributed artificial intelligence*, Cambridge, MA, the MIT Press, 27 – 77.

7 Wooldridge, M. (2002). *An introduction to multiagent systems*, Chichester, England, J. Wiley.

8 Hector, A.; Lakshmi Narasimhan, V. (2005). *A New Classification Scheme for Software Agents.* Proceedings of the Third International Conference on Information Technology and Applications (ICITA'05), pp. 191 – 196, ISBN: 0-7695-2316-1, Sydney, Australia, July 2005, IEEE Computer Society, Washington, DC

9 Grabosky, P. (1995). Counterproductive regulation, *International Journal of the Sociology of Law*, vol.23, pp. 347-69.

10 Financial Action Task Force. (2004). The 40 Recommendations.

11 Wit, J. d. (2007). A risk-based approach to AML. Retrieved June 20, 2011, from Journal of *Financial Regulation and Compliance*: http://proquest.umi.com.proxy.lib.uwaterloo.ca/pqdweb?index=18&did=1344340421&Sr

chMode=2&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1309544465&clientId=16746

12 Peggy Bresnick Kendler. (2007). *Anti-Money Laundering. Bank Systems & Technology*, 44(10), 38.

13 Financial Action Task Force. (2004). The 40 Recommendations. Retrieved June 20, 2011, from FATF: http://www.fatf-gafi.org/document/28/0,3343,en_32250379_32236930_33658140_1_1_1_1,00.html

14 Wit, J. d. (2007). A risk-based approach to AML. Retrieved June 20, 2011, from Journal of Financial Regulation and Compliance

15 Bloom, B.S. (Ed.). Engelhart, M.D., Furst, E.J., Hill, W.H., Krathwohl, D.R. (1956).Taxonomy of Educational Objectives, Handbook I: The Cognitive Domain. New York: David McKay Co Inc.

16 Federal Reserve Bank of New York. (1987). *A Study of Large-Dollar Payment Flows Through CHIPS and Fedwire*.

17 Ekkart, R., Jens, G., and Peter, G. (1996). Tutorial on message sequence charts (MSC). *In Proceedings of FORTE/PSTV'96 Conference*.

18 Bjorn, R., Michael, A. and Johan B. (1996). A hierarchical use case model with graphical representation. *In Proceedings of ECBS'96, IEEE International Symposium and Workshop on Engineering of Computer-Based Systems*.

19 Iglesias, C., Garijo, M., Centeno-Gonzalez J. & Velasco J. R. (1998). Analysis and Design of Multiagent Systems Using MAS-CommonKADS. *Agent Theories, Architectures, and Languages. Lecture Notes in Artificial Intellegence.* Vol. 1365, pages 313-326. Springer-Verlag.

20 Rumbaugh, J., Jacobson, I. & Booch, G. (1999).*The Unified Modelling Language Reference Manual.* Addison Wesley

21 Alvaro, E.A. and Gareth, B. (2002). 'Applying the MAS-CommonKADS Methodology to the Flights Reservation Problem: Integrating Coordination and Expertise', *Proceedings of the Fifth Joint Conference on Knowledge-Based Software Engineering (JCKBSE 2002)*. No 39, Vol. 234, pp. 1-10.

22 Beck, K. & Cunningham, W. (1989). A laboratory for teaching object-oriented thinking. In *OOPSLA'89 Conference Proceedings*, New Orleans, LA, USA (Vol. 17, pp. 1-6).

23 Wirfs-Brock, R., Wilkerson, B. & Wiener, L. (1990). *Designing object-oriented software*. Upper Saddle River, NJ: Prentice-Hall

Appendices

Appendix A – Table structure

New clients

ClientType – Individual or organization

AccountName – Account holder name

Branch – financial institution branch

DoB – Date of Birth

Accountdate – Date when account was opened.

Nationality - Nationality

IDNo – National Identification number

Address -

PassportNo – passport number

PassportPlace - place of issue

Telephone - Telephone

Status – Active or Dormant

Watch List

Name – Name of the person or Organization

OriginalName – Original name

Title – title of the person

Designation

DoB – Date of Birth or registration

PlaceofBirth

GoodQuality – also known as

LowQuality – also known as

Nationality

PassportNo

PassportDate

PassportPlace

IDNo

IDPlaceofIssue

Address

DateListed

OtherInformation

Status

Bank Transaction

Institution

AccountNo

AccountName

AccountBranch

TransactionType

Amount

TransactionDate

TransactionBranch

BeneficiaryAccName

BeneficiaryAccNo

BeneficiaryBank

BeneficiaryBranch

BeneficiaryCountry

Currency

TransactionTime

Appendix B – Sample Code

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.Data.Odbc;

namespace WindowsFormsApplication1
{
    public partial class frmMainAgent : Form
    {
        private int childFormNumber = 0;

        public frmMainAgent()
        {
            InitializeComponent();
        }

        private void ShowNewForm(object sender, EventArgs e)
        {
            Form childForm = new Form();
            childForm.MdiParent = this;
            childForm.Text = "Window " + childFormNumber++;
            childForm.Show();
        }

        private void OpenFile(object sender, EventArgs e)
        {
            OpenFileDialog openFileDialog = new OpenFileDialog();
            openFileDialog.InitialDirectory =
Environment.GetFolderPath(Environment.SpecialFolder.Personal);
            openFileDialog.Filter = "Text Files (*.txt)|*.txt|All Files (*.*)|*.*";
            if (openFileDialog.ShowDialog(this) == DialogResult.OK)
            {
                string FileName = openFileDialog.FileName;
            }
        }

        private void SaveAsToolStripMenuItem_Click(object sender, EventArgs e)
        {
            SaveFileDialog saveFileDialog = new SaveFileDialog();
            saveFileDialog.InitialDirectory =
Environment.GetFolderPath(Environment.SpecialFolder.Personal);
            saveFileDialog.Filter = "Text Files (*.txt)|*.txt|All Files (*.*)|*.*";
            if (saveFileDialog.ShowDialog(this) == DialogResult.OK)
            {
                string FileName = saveFileDialog.FileName;
            }
        }
```

```
        private void ExitToolsStripMenuItem_Click(object sender, EventArgs e)
        {
            this.Close();
        }

        private void CutToolStripMenuItem_Click(object sender, EventArgs e)
        {
        }

        private void CopyToolStripMenuItem_Click(object sender, EventArgs e)
        {
        }

        private void PasteToolStripMenuItem_Click(object sender, EventArgs e)
        {
        }

        private void ToolBarToolStripMenuItem_Click(object sender, EventArgs e)
        {
            toolStrip.Visible = toolBarToolStripMenuItem.Checked;
        }

        private void StatusBarToolStripMenuItem_Click(object sender, EventArgs e)
        {
            statusStrip.Visible = statusBarToolStripMenuItem.Checked;
        }

        private void CascadeToolStripMenuItem_Click(object sender, EventArgs e)
        {
            LayoutMdi(MdiLayout.Cascade);
        }

        private void TileVerticalToolStripMenuItem_Click(object sender, EventArgs e)
        {
            LayoutMdi(MdiLayout.TileVertical);
        }

        private void TileHorizontalToolStripMenuItem_Click(object sender, EventArgs
e)
        {
            LayoutMdi(MdiLayout.TileHorizontal);
        }

        private void ArrangeIconsToolStripMenuItem_Click(object sender, EventArgs e)
        {
            LayoutMdi(MdiLayout.ArrangeIcons);
        }

        private void CloseAllToolStripMenuItem_Click(object sender, EventArgs e)
        {
            foreach (Form childForm in MdiChildren)
            {
                childForm.Close();
            }
        }
```

```
        private void blackListContactsToolStripMenuItem_Click(object sender,
EventArgs e)
        {
            Form frmBlackList = new frmBlackListContants();
            frmBlackList.MdiParent = this;
            frmBlackList.StartPosition = FormStartPosition.CenterScreen;
            //form1.ShowDialog
            frmBlackList.Visible = true;
        }

        private void frmMainAgent_Load(object sender, EventArgs e)
        {
            //GlobalVar.MaConn();
            //GlobalVar.ConnAgent.Open();


        }

        private void accountHoldersToolStripMenuItem_Click(object sender, EventArgs
e)
        {
            Form myForm = new frmBankClientRegistry();
            myForm.MdiParent = this;
            myForm.StartPosition = FormStartPosition.CenterScreen;

            myForm.Visible = true;
        }

        private void transactionsToolStripMenuItem_Click(object sender, EventArgs e)
        {
            Form myForm = new frmBankTransactions();
            myForm.MdiParent = this;
            myForm.StartPosition = FormStartPosition.CenterScreen;

            myForm.Visible = true;
        }

        private void insuranceAccountsToolStripMenuItem_Click(object sender,
EventArgs e)
        {
            Form myForm = new frmInsuranceClients();
            myForm.MdiParent = this;
            myForm.StartPosition = FormStartPosition.CenterScreen;

            myForm.Visible = true;
        }

        private void moneyTransferAccountsToolStripMenuItem_Click(object sender,
EventArgs e)
        {
            Form myForm = new frmMoneyTransferClients();
            myForm.MdiParent = this;
            myForm.StartPosition = FormStartPosition.CenterScreen;
```

```
            myForm.Visible = true;
        }

        private void insuranceTransactionsToolStripMenuItem_Click(object sender,
EventArgs e)
        {
            Form myForm = new frmInsuranceTransactions();
            myForm.MdiParent = this;
            myForm.StartPosition = FormStartPosition.CenterScreen;

            myForm.Visible = true;
        }

        private void moneyTransferTransactionsToolStripMenuItem_Click(object sender,
EventArgs e)
        {
            Form myForm = new frmMoneyTransferTransactions();
            myForm.MdiParent = this;
            myForm.StartPosition = FormStartPosition.CenterScreen;

            myForm.Visible = true;
        }

        private void filterCriteriaToolStripMenuItem_Click(object sender, EventArgs
e)
        {
            Form myForm = new frmMoneyLaunderingSettings();
            myForm.MdiParent = this;
            myForm.StartPosition = FormStartPosition.CenterScreen;

            myForm.Visible = true;
        }

        private void blackListGroupsToolStripMenuItem_Click(object sender, EventArgs
e)
        {
            Form myForm = new frmWatchListAccounts();
            myForm.MdiParent = this;
            myForm.StartPosition = FormStartPosition.CenterScreen;

            myForm.Visible = true;
        }

        private void watchListTransactionsToolStripMenuItem_Click(object sender,
EventArgs e)
        {
            Form myForm = new frmWatchListTransactions();
            myForm.MdiParent = this;
            myForm.StartPosition = FormStartPosition.CenterScreen;

            myForm.Visible = true;
        }
    }
}
```

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using Boris;

namespace WindowsFormsApplication1
{
    public partial class frmMoneyTransferClients : Form
    {
        public frmMoneyTransferClients()
        {
            InitializeComponent();
        }

        private void btnSave_Click_1(object sender, EventArgs e)
        {
            if (string.IsNullOrEmpty(txtName.Text))
            {
                MessageBox.Show("Client Account Name must be filled in!", "Money
Transfer Accounts", MessageBoxButtons.OK, MessageBoxIcon.Exclamation);
                return;
            }

            if (string.IsNullOrEmpty(cboType.Text))
            {
                MessageBox.Show("Client Type must be filled in!", "Money Transfer
Accounts", MessageBoxButtons.OK, MessageBoxIcon.Exclamation);
                return;
            }

            if (string.IsNullOrEmpty(txtNationalID.Text))
            {
                MessageBox.Show("National ID Number must be filled in!", "Money
Transfer Accounts", MessageBoxButtons.OK, MessageBoxIcon.Exclamation);
                return;
            }

            if (string.IsNullOrEmpty(txtBankAccountNo.Text))
            {
                MessageBox.Show("Money Transfer Account Number must be filled in!",
"Money Transfer Accounts", MessageBoxButtons.OK, MessageBoxIcon.Exclamation);
                return;
            }

            if (string.IsNullOrEmpty(txtBranch.Text))
            {
                MessageBox.Show("Money Transfer Account Branch must be filled in!",
"Money Transfer Accounts", MessageBoxButtons.OK, MessageBoxIcon.Exclamation);
```

```
                return;
            }

            //Agent Confirm of the Black List Exists
            Boolean blackListAccountDetected = false;

            try
            {
                GlobalVar.LinkNestedString = "SELECT * FROM tblWatchList WHERE
PassportNo =   '" + txtPassportNo.Text + "' ";
                GlobalVar.NestedReadTable();

                if (GlobalVar.drNestedAgent.Read())
                {

                    blackListAccountDetected = true;

                    Portal p1 = new Portal("Liverpool");
                    MetaAgent AccountSniffer = new
MetaAgent("MTransferAccountSniffer");


                    p1.AddAgent(AccountSniffer);

                    p1.Connect("127.0.0.1", 1234);
                    //if (txtSendMessage.Text != "")

                    AccountSniffer.SendMessage("Sam",
GlobalVar.drNestedAgent["Name"].ToString() + " in Watchlist opened new Account " +
txtBankAccountNo.Text);
                    AccountSniffer.SendMessage("TransSniffer",
GlobalVar.drNestedAgent["Name"].ToString() + " in Watchlist opened new Account " +
txtBankAccountNo.Text);
                    //a1.SendMessage("Sam",
GlobalVar.drNestedAgent["EntryNo"].ToString());

                }
                GlobalVar.drNestedAgent.Close();
                GlobalVar.CmdNestedAgent.Dispose();

            }
            catch (Exception ex)
            {
                MessageBox.Show(ex.Message, "Money Transfer Account List",
MessageBoxButtons.OK, MessageBoxIcon.Exclamation);
                GlobalVar.drNestedAgent.Close();
                GlobalVar.CmdNestedAgent.Dispose();

            }


            try
            {
                string DOBDateString = dtpDOB.Value.Year + "-" + dtpDOB.Value.Month +
"-" + dtpDOB.Value.Day;
```

```
                //string PassportDateString = dtpPassportIssue.Value.Year + "-" +
dtpPassportIssue.Value.Month + "-" + dtpPassportIssue.Value.Day;
                string AccountDateString = dtpAccountDate.Value.Year + "-" +
dtpAccountDate.Value.Month + "-" + dtpAccountDate.Value.Day;

                GlobalVar.LinkString = ("INSERT INTO tblBankAccounts VALUES ('" +
"TRANSFER AGENT" + "','" + cboType.Text + "', '" + txtName.Text + "', '" +
txtBankAccountNo.Text + "', '" + txtBranch.Text + "', '" + DOBDateString + "', '" +
AccountDateString + "', '" + txtNationality.Text + "', '" + txtNationalID.Text + "',
'" + txtAddress.Text + "', '" + txtPassportNo.Text + "',  '" +
txtPassportPlaceOfIssue.Text + "', '" + txtTelephone.Text + "', '" + cboStatus.Text +
"')");
                GlobalVar.LinkTable();

                //Agent Insert Entry in Watch List Accounts
                if (blackListAccountDetected == true)
                {

                    GlobalVar.LinkString = ("INSERT INTO tblWatchListBankAccounts
VALUES ('" + "TRANSFER AGENT" + "','" + cboType.Text + "', '" + txtName.Text + "', '"
+ txtBankAccountNo.Text + "', '" + txtBranch.Text + "', '" + DOBDateString + "', '" +
AccountDateString + "', '" + txtNationality.Text + "', '" + txtNationalID.Text + "',
'" + txtAddress.Text + "', '" + txtPassportNo.Text + "',  '" +
txtPassportPlaceOfIssue.Text + "', '" + txtTelephone.Text + "', '" + cboStatus.Text +
"')");
                    GlobalVar.LinkTable();
                }


                MessageBox.Show("New Money Transfer Account saved successifully",
"Money Transfer Accounts", MessageBoxButtons.OK, MessageBoxIcon.Information);
                // Call ClearTxtBoxes(Me)
                //Populate the LV
                //PopulateLV();

            }
            catch (Exception ex)
            {
                GlobalVar.CmdAgent.Dispose();
                MessageBox.Show(ex.Message, "Money Transfer Accounts",
MessageBoxButtons.OK, MessageBoxIcon.Error);

            }
            return;
        }


         private void frmMoneyTransferClients_Load(object sender, EventArgs e)
        {

        }

        private void btnList_Click_1(object sender, EventArgs e)
        {
            Form myForm = new frmBankAccountList();
```

```
            myForm.MdiParent = this.ParentForm;
            myForm.StartPosition = FormStartPosition.CenterScreen;
            GlobalVar.GlobalFinancialInstitutionString = "TRANSFER AGENT";
            myForm.Visible = true;
        }


    }
}
```

Appendix C –System Demo

Launching the agents using Boris .NET. Here we register the key displaying agents, namely,

a) ConnectorAgent

b) ReportingAgent

c) MoneyLounderingSniffer

d) TransSniffer

The figure shows the agents just after the launch, note that there is no communication amongst the agents.

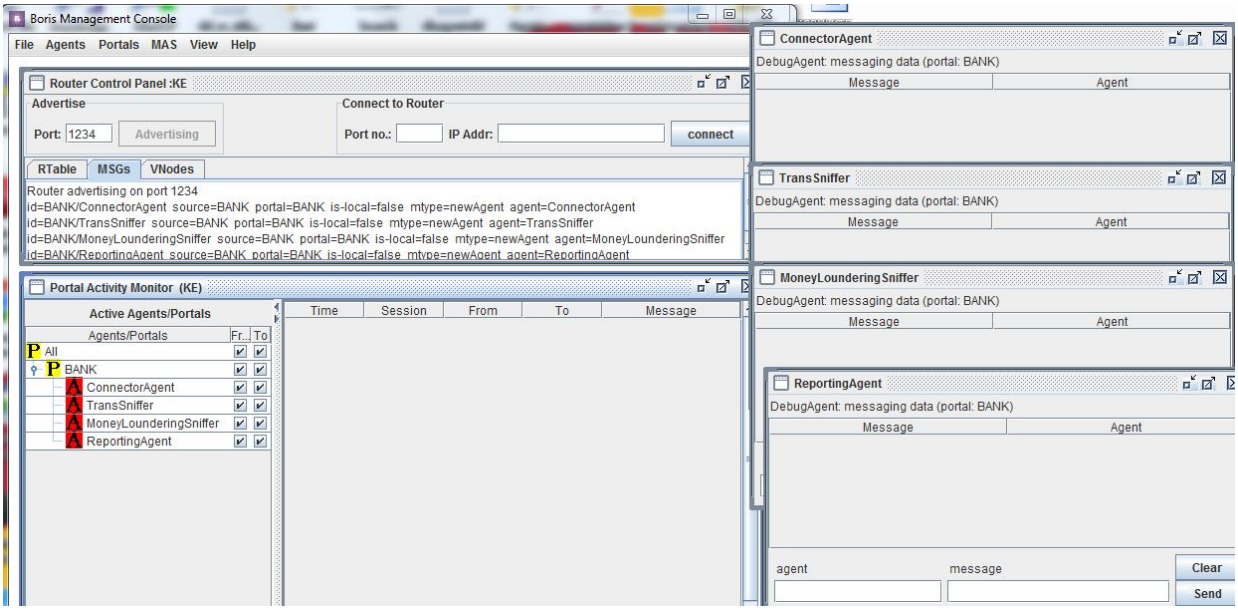

Figure 18: Screenshot of agents after launch

Simulated banking system is then started. It has a user interface for capturing/displaying the names of suspected individuals/organizations.

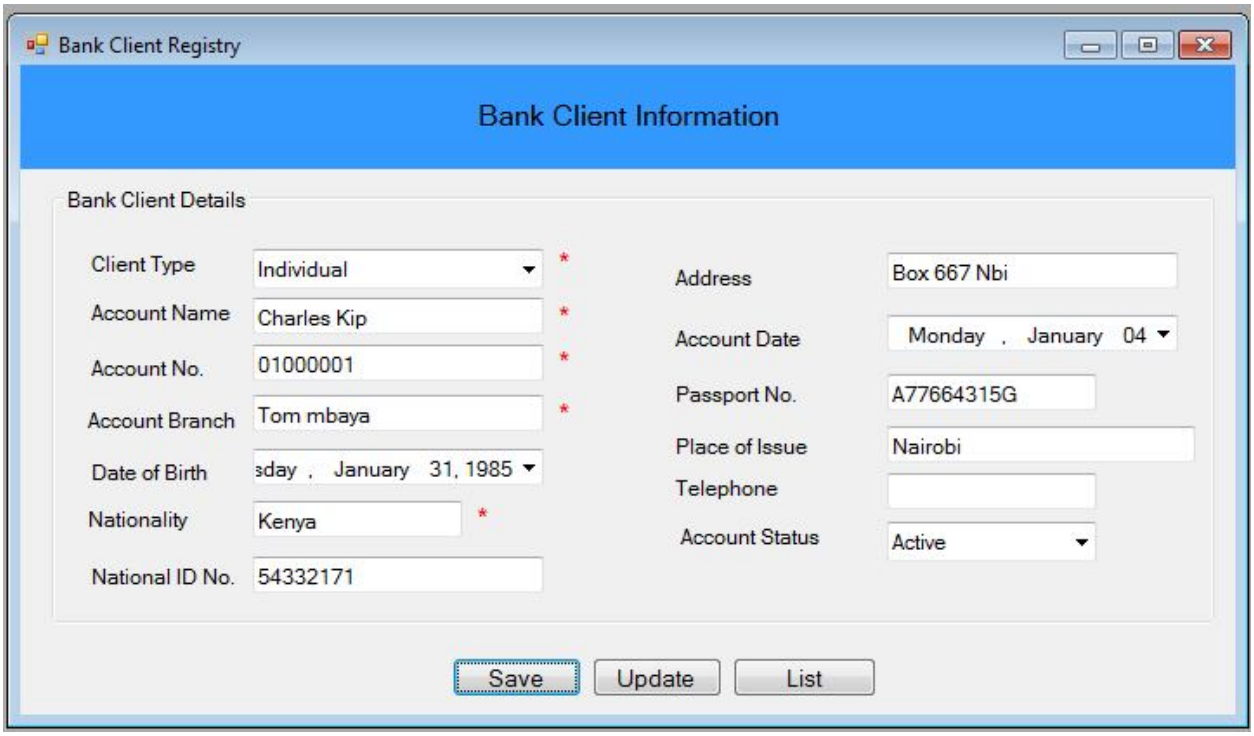

Figure 19: Registering bank client.

The details of the client are captured and stored in the bank database. If the client is in the watchlist, then the TransSniffer agent will raise an alarm – which the client registered is in watch list.

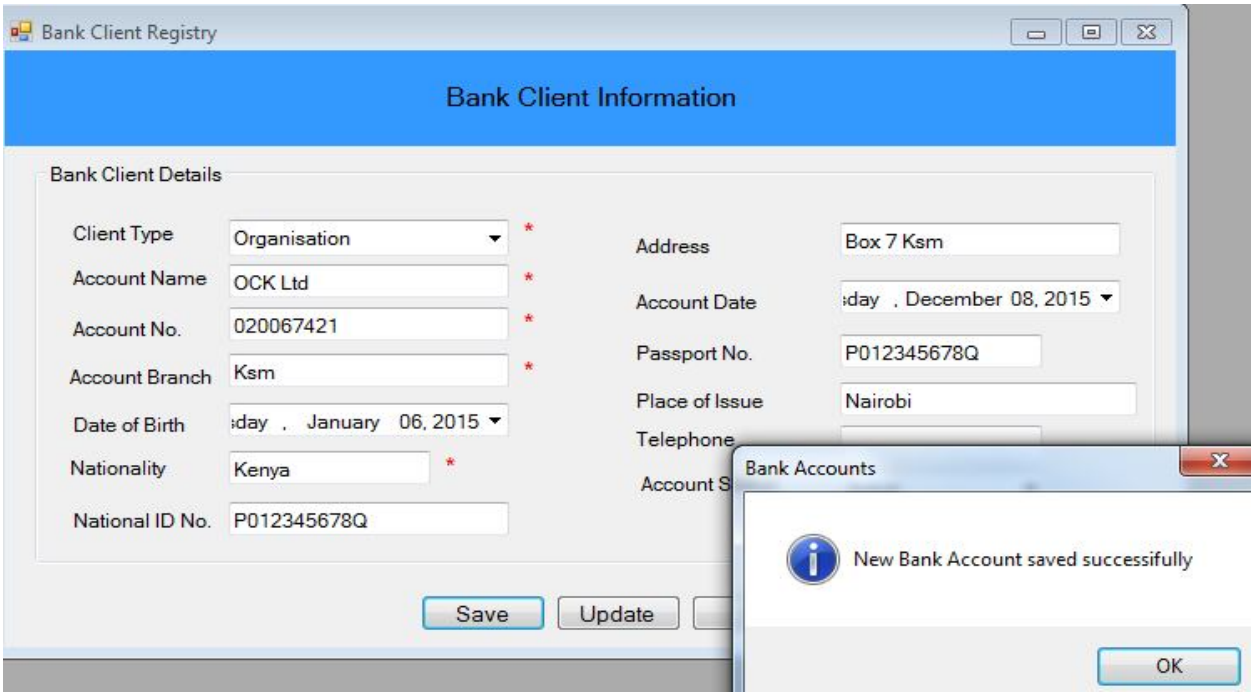

Figure 20: Bank client registration screen

Example above captures the details of a new client who happens to be in a watch list. This will prompt the BankAccountSniffer agent to send alert both ConnectorAgent and TransSniffer agent as shown below

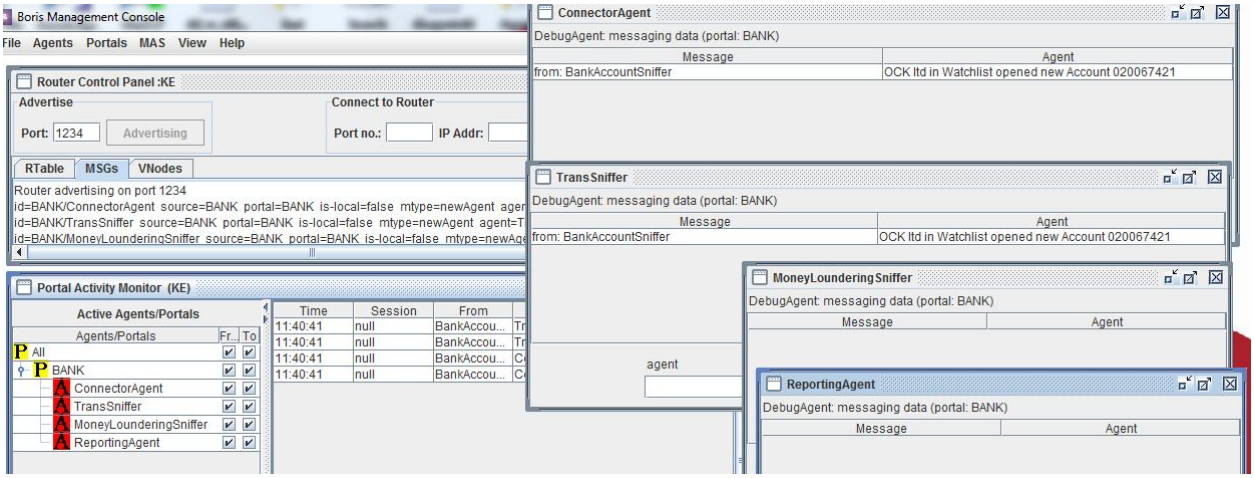

Figure 21: Agents' communication on new client

The BankTransSniffer will tag the account opened by individuals/organizations in the watch list and it will keep on monitoring the accounts i.e. it will monitor transactions done through such account. BankTransSniffer agent will alert MoneyLounderingSniffer agent whenever there is any transaction done by an account tagged.

Money Laundering Rules

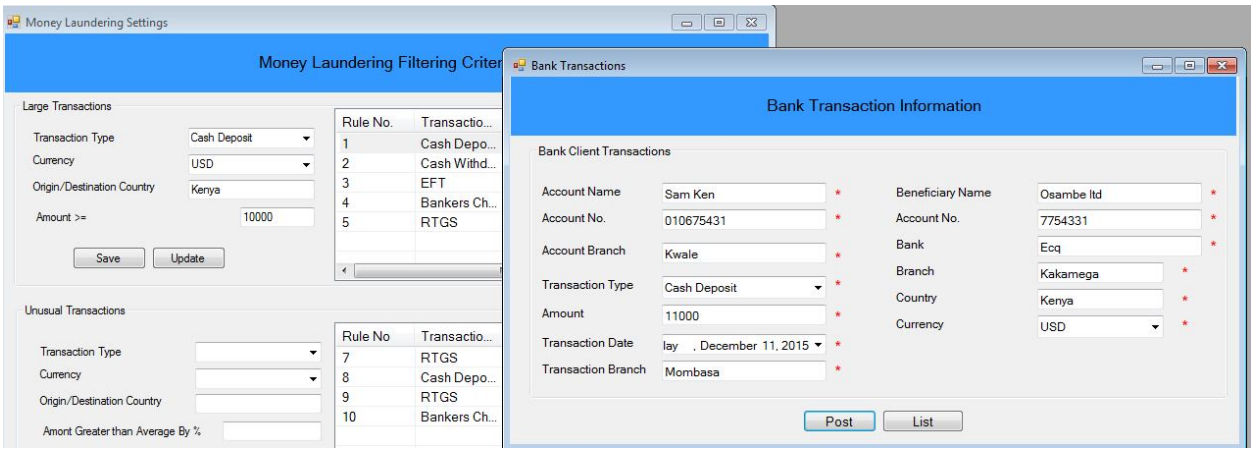

Figure 22: Money laundering rule setting

Figure above displays rule of threshold i.e. if the amount is greater or equals to 10,000 US dollar and transaction type is EFT and country is Kenya, then the transaction is treated is suspicious transaction and it should be reported.

To demonstrate the rule, Sam will transact an EFT of amount greater than 10,000 US dollars in Kenya.

Since the transact amounts to money laundering, the transaction is tagged as suspicious transaction and is reported to reporting agent. Below screenshot displays the communication to the ReportingAgent.

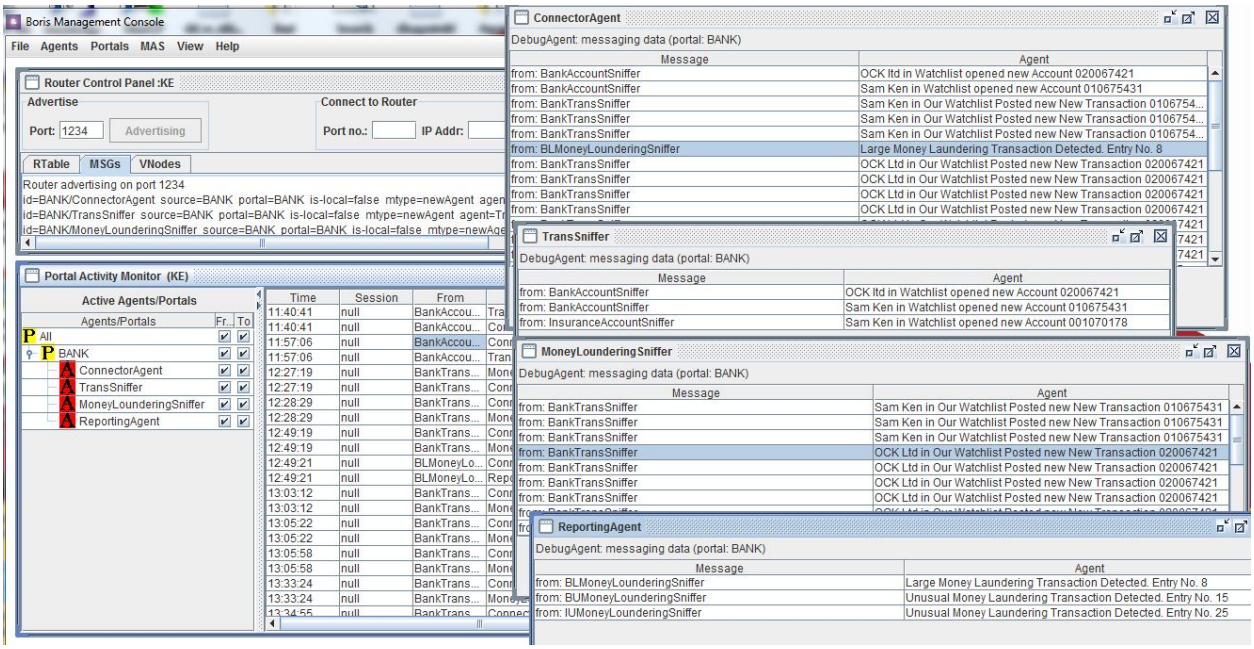

Figure 23: ReportingAgent communication