UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES

SCHOOL OF COMPUTING AND INFORMATICS

AGENT BASED FRAUD DETECTION AND REPORTING IN PUBLIC E-PROCUREMENT

BY

SIROREI JAMES K

A RESEARCH PROJECT REPORT SUBMITTED IN PARTIAL FULFILLMENT FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE IN COMPUTER SCIENCE OF THE UNIVERSITY OF NAIROBI.

AUGUST 2018

Declaration

This project report represents my original work and it has not been presented in any other institution for any award.

Sign: _____ Date: _____

James K Sirorei
P58/75906/2012

This project report has been submitted in partial fulfillment of the requirements for the Masters of Science in Computer Science of the University of Nairobi with my approval as the university supervisor.

Sign: _____ Date: _____

Dr. Elisha Opiyo
School of Computing and Informatics
University of Nairobi

Table of Contents

Abstract

Procurement fraud remains an endemic in most modern economies. E-Procurement fraud may manifest in different ways that can include collusion by parties involved in procurement as well as falsification of documents. A procurement officer might be induced through bribery to favor a particular supplier. For protection against procurement fraud, organizations have tried to implement some control measures, hoping such measures would discourage the fraud that is directed on institutions. Complex fraud does not revolve around the breaching of these controls, but bypassing them. In this research we set out to design and implement an e-procurement fraud detection tool for public entities using multi agent technologies. This was informed by contributions from various government employees who were interviewed, literature review and publications that indicate the presence of fraud in public offices attributable to procurement processes. A prototype of an e-procurement system is developed with the complete procure-to-pay functionality. This provides the environment for the agent based fraud detection tool to be implemented on. Fraud is then detected using rule set to determine suspicious activities and transactions in the e-procurement system. The agent based e-procurement fraud detection tool is able to detect and report fraud in situations where inflation of unit cost of items at requisition level and further upward adjustments are done while raising purchase orders. Upward adjustment of quantities on purchase orders after requisition approval is also picked as fraud by the agent detection tool. This is a scenario that requires approvals from approvers who may be compromised or fail to take note of the discrepancies. The proceeds from such fraud may be paid to the participants in the procurement chain as kickbacks (bribes).

Dedication

I dedicate this Project to my wife Loice Komen, daughter Sharon Jepkosgei and several family members and friends who continuously supported and encouraged me throughout the course of my studies. It is not possible to list all of you here. Many Thanks and God Bless you.

Acknowledgements

My appreciations go to the Lord Almighty for enabling me to get this far in my academic pursuit. I also extend lots of appreciation to my supervisor Dr. Elisha Opiyo and other panelists from the School of computing and informatics who guided me to successfully write this project.

Finally, my appreciation goes to my friends Bico Hamalah, Dawson Kiteto, Roseline and Perminus Gathanga who assisted me to understand and simulate an e-procurement system. Gratitude also goes to my employer and colleagues who gave me the invaluable time and support to take this course.

List of acronyms

AOSE: Agent-oriented software engineering.

E-GP: E-government procurement.

ICT: Information Communication Technology.

IFMIS: Integrated Financial Management Information System.

JADE: Java Agent Development Environment.

JDBC: Java Database Connectivity.

JDK: Java Development Kit.

JRE: Java Runtime Environment.

LAN: Local Area Network

MAS: Multi Agent System.

OECD: Organization for Economic Co-operation and Development.

PPOA: Public Procurement Oversight Authority.

UER: User-Environment-Responsibility.

WAN: Wide Area Network

Chapter One

1. Introduction

1.1 Background to the problem

Procurement fraud is as old as commerce and remains a problem to most developing countries/economies. The line between corporate hospitality and bribery is very thin.

E-procurement is the use of electronics to support the entire procure-to-pay process from requirements identification to the payment for goods, services or works including managing contracts (Davila et al., 2003).

Public Electronic Procurement is the use of e-Government infrastructure and electronic resources (internet and web applications) to purchase products and services from suppliers to organization's buyers.

E-Procurement fraud do manifest in various ways, from collusion by cartels to fiddling with procurement or payment documents. Often, an employee in the procurement chain may be bribed so as to look the other side or extend favors to a particular supplier.

The continued dominance of e-procurement due to digitization and automation raises the question on how this development continues to affect the openings available for perpetuating procurement fraud.

As a prevention measure against fraud in procurement, organizations have put in place certain controls and procedures, believing such would make it hard to circumvent thereby reducing fraud within their entities. Far from it, complex frauds do not revolve around the flouting of these controls, but their circumvention.

In the strategic plan of Public Procurement Oversight Authority (PPOA) for the period 2010-2014, it is highlighted that implementation and use of reliable public procurement system would enable the Government of Kenya achieve its goals

Such a system is one that ensures:

i) There is value for money to the government.

ii) There is minimum or no loss of funds in procurement.

iii) Optimization in resource allocation for the prioritized projects in government.

iv) Timely delivery of goods, works and services.

A reliable and efficient e-procurement system would yield benefits such as: reduced spending in government, discourages fraud, as well as promotes accountability in public procurement. It follows then that money will be available to fund other Government projects hence contribute to social-economic development and improve the living standards of the people.

It is therefore noted that e-procurement systems do not eliminate corruption on their own. It requires integrity on the part of every system user who plays a role in the procurement process.

Agents can play a critical role when successfully deployed to detect and report corruption. This though is a reactive approach.

1.2 Problem statement

The Kenyan government, despite having deployed ICT and an e-procurement system to manage procurement processes, corruption is still rampant. It means therefore, that there are loopholes in the current implementation that lead to procurement fraud and that ICT is not working in detecting fraud.

Public procurement fraud is a problem that is widespread in developing countries and it has serious negative effects to a nation. Some of the negative effects are: Hindrance to creation of wealth, increase government operational cost, wear-out the social structure and trust in government, and alter the ratio of government spending significantly increasing recurrent expenditure.

To overcome fraud related concerns in government e-procurement, technology can serve to inhibit fraud and promote good governance, Bertot, Jaeger & Grimes (2010).

It was published on the newspapers (Daily Nation, 2016) that the government of Kenya was looking at risk management on the (Integrated Financial Management Information System) IFMIS, by implementing mechanisms to identify fraud before money is lost. This came after a Cyber Security Report in 2015 indicating the loss of kshs.15 billion as a consequence of cyber-crime.

In the same article it was reported that a former devolution and planning cabinet secretary in mid 2015 reported an attempt to steal Ksh. 0.8 billion from NYS using compromised login credentials.

In January 2016, Transparency International (TI) released a report showing Kenya at position 139 out of 168 on corruption index.

Most of the deals are as a result of loopholes in the public procurement systems.

Since it is not possible to develop and run fraud detection agents on a live public e-procurement system due to authorization and security, there will be need to simulate such a system and embed agent prototypes for fraud detection

1.3 Purpose of the project/Goal

This project seeks to demonstrate how agents can play a critical role to detect corruption in public electronic procurement (specifically government) through reporting of fraud incidences.

Objectives

Specific Objectives

i. Identify possible fraud avenues in a public e-procurement system.
ii. Identify system variables and indicators that can help agents to detect likely incidences of corruption within the e-procurement system.
iii. Simulate a public e-procurement system.
iv. Design and implement a prototype based on agents to detect and report incidences of corruption.

v. Evaluate the detection agent.

1.4 Research questions

1. How agents can be used to monitor user activities within a public e-procurement system.
2. What database, system variables and indicators can be useful in detecting corruption in e-procurement platforms?
3. How agents can detect suspect activities in an e-procurement system.

1.5 Significance of the study

This research project is intended to assist the government (both national and county governments) to tackle the issue of corruption in a manner that goes beyond the deployment of ICT to automate processes. With the help of agents, It will be demonstrated how corruption will be detected at an early stage to give room for reactive action that can prevent loss of funds.

Integrity can be measured in Public procurement can looking at the number of cases an individual is reported as having attempted to perpetuate fraud.

Successful implementation of agents can reduce the number of internal and external auditors needed to scrutinize public e-procurement processes hence a cost saving.

Finally, more money will be available to the government to direct to real development projects devoid of corruption cases.

1.6 Assumptions

It is assumed that public e-procurement is deployed on systems that can store audit trails of system e-procurement activities (i.e. Oracle databases) and that those variables will be available for scrutiny to corruption detection agents.

1.7 Limitations of the research

Where Public procurement processes are not fully automated or where there is a hybrid implementation of electronic processes and manual processes it would be difficult to detect all cases of corruption owing to absence of important database variables and system variables that agents can track.

1.8 Definition of important terms

Agent - Russel & Norvig (1995) Are objects in the environment that perceive and react to states in the environment.

E-procurement - Procurement using electronic medium consisting of the internet and other ICT infrastructure.

Fraudulent practice - A misrepresentation to cause the purchase of goods or services or works or signing of a contract to the disadvantage of the procuring entity. It may involve collusion among tenderers before or after tender submission designed to fix tender prices and deprive the buying entity benefit of competitive bidding.

PPOA - Public Procurement Oversight Authority which is an independent regulatory body established under the Public Procurement and Disposal Act, 2005. The act was operationalized in January 2007 upon the publication of Public Procurement and Disposal Regulations, 2006.

Multi-agent system – Wooldridge (2002) is a system of agents that interact with one another through cooperation, competition, coordination or negotiation to accomplish some goal.

Modeling - A way of capturing ideas, relationships, decisions and requirements in a well-defined notation which can be applied to various domains.

Simulation - Experimenting with a simple imitation (on a computer) of an operations system as it progresses through time, so as to better understand and improve the system (Robinson Stewart, 2004).

Tender –A written offer by a candidate to supply goods, services or works at a price or to acquire or dispose items at a price, following an invitation to tender, request for quotation or proposal by a purchasing entity.

OECD - Organization for Economic Co-operation and Development.

Chapter Two

2 Literature Review

Procurement-related fraud is a deviant behavior, which involves manipulation of the procurement system to unfairly benefit a supplier. Rabl and Kuhl- mann (2009).

According to the World Bank (1998) manipulation of supply chain functions happen when tender documents are being drawn, publication of bids, opening, evaluating, approving, awarding contracts and executing them.

Sometimes, Supply chain officials bend rules governing bidding processes so as to favor some suppliers and design tenders with specific people or suppliers in mind. Some bidders are also joined in some unholy alliances with procurement officers who induce them to overstate project costs.

According to Ware and Noone (2003) bribery is the order of the day in third world countries. This is where a firm pays out a bribe to a public official who facilitated the award of the contract.

Fraud:

Fraud involves the misuse of public office for selfish personal gain, Amanda (1998). It is a bad practice that has been around since the beginning of time as Dike (2005) says as old as the world. The illegalities and fraud cases reported attest to it.

Transparency International (TI) presented an annual report that compared countries and showed the occurrence and size of fraud. Africa is ranking high compared to other continents.

TI presented a study on fraud using corruption perceptions index (CPI) that had some limitations.

TI relied heavily on a small number of country technocrats to conduct the research who overlooked socio-cultural elements, experiences, interests, freedom, and free will of the media. Sı´k (2002).

It also showed the country as perpetrator of fraud, overlooking the persons who committed the fraudulent acts. This results in the creation and implementation of bad public policies on fraud (Krastev 2004).

World Bank has also conducted an alternative study on fraud using the Business Environment and Enterprise Performance Survey (BEEPS). They conducted research on four thousand companies in 22 countries. This was done between the year 1999 and 2000 which looked at various dealings by companies and governments.

BEEPS was designed to produce comparative reports on matters relating to the quality of the business environment, fraud, state capture and lobbying (World Bank Institute & EBRD 2000). The research was able to describe fraud related to administration and state culture, but failed to bring out inherent fraud within the system(Hellman et al. 2000).

A decrease in fraud in traditional procurement can be improved through adoption of E-government procurement (Siriluck Rotchanakitumnuai, 2013). This was cited in a Thai survey that was conducted on public managers working in e-government procurement. Siriluck states ways on how to enhance governance in procurement. They include transparent processes, dedicated public officers, honest vendors, and adoption of specific policy guidelines and regulations.

There are advantages that accrue from a transparent e-procurement process. Such benefits include reducing collusion among suppliers of goods and services, good governance, cost effectiveness and being more accountable. Vendor honesty can determine the extent of collusion. There should be policy guidelines and regulations so as to make the law enforceable, realize cost effectiveness and accountability.

It is therefore noted that good governance can be realized by applying best practices in e-government procurement.

ADB (2004) defines good governance as both a structure and process that ensures prudent use and administration of resources. It is focused on transparency and maximization of benefits to ta

nation and its people.

Public sector procurement is the avenue for fraud between private entities and public sector (Warsta, 2004).

Padhi and Mohapatra (2011) suggested analysis of patterns to check for collusion. Other studies do not show much on correlation between e-procurement and the human factor. They do not bring out clearly the factors for determining good governance relative to e-government procurement.

The main objective of deploying e-government procurement is to minimize fraud. Implementation though is still a challenge. In Thai Government, it is common not to find a transparent tender process (Rotchanakitumnuai, 2012a).

Political influence and collusion with suppliers open fraud avenues for abusing public resources (Rotchanakitumnuai, 2012b). To implement good governance, one ought to identify elements of e-government procurement at various levels to gauge the best practices for electronic government procurement.

ICT helps to bring positive impact by shrinking the number of business processes steps and helping improve productivity.

E-procurement is a system that supports B2B transactions (Holmes, 2001). It rides on the Internet to decrease procurement time, reduce costs, change buying habits and enhance supplier relationships (Chopra et al. 2001)

Online IT is used in government e-government to procure goods, services and works for public organizations from other companies. E-procurement can be an avenue for value addition and also ensure the government save on cost (Iqbal and Seo, 2008; Rai et al. , 2006).

According to Harris and Rajora (2006), suppliers can be encouraged participate in public procurement. Moreover, it is effective in ensuring that political meddling is reduction (Heywood, 2002).

It is important to manage the procurement process so as to promote good governance. Proper development of requirements specification and the right choice of purchasing technique should be adopted (Hui et al., 2011). Some large-scale projects may require tendering through electronic auctioneering.

Kennedy and Deeter-Schmelz, (2001) argues that human resource is a factor for fraud. People at high level influence the use or adoption of e-procurement. They have a big say in the setting of procurement priorities. (Hardy and Williams, 2008).

Fraud is influenced by Politics where those elected to high offices seek to call shots (ADB, 2004 and Al-Zobi, 2008)

Public-private relations can lead to bias in procurement (Hui et al., 2011). Policy guidelines should be put in place to define the rules that guide e-procurement and help prevent fraud (Rotchanakitumnuai, 2010).

Procurement fraud has been around for a very long time and is problem affecting many developing countries.

E-Procurement fraud manifest in various forms such as: through cartels and falsification of procurement documents. A supply chain officer may be induced with bribes to favor a vendor.

As e-procurement becomes popular due to automation, its impact on the opportunities for procurement fraud using the same technology remains to be fully defined.

To protect themselves from procurement fraud, organizations have always sought to put in place certain controls and procedures, believing such would make it hard to circumvent locking out preying fraudsters. Far from it, complex frauds do not revolve around the flouting of these controls, but their circumvention.

According to Jon Hayton (Pricewaterhousecoopers), undetected fraud often begins from the first phases of tendering where those perpetuating: restrict suppliers invited to tender, develop a specification document that favors their friends or worse still ensure the participants receive a different specification document.

Why fraud opportunities exist

Most fraudsters know the internal operations of the organizations they are targeting very well. Some may have been former employees who were very much involved in the matters of supply chain. Their past roles in procurement means that they know how processes work and how they will be audited. They also know where an keen auditor will focus.

A fraudulent person can safeguard the interest of a particular supplier so as to be awarded a contract. This interference often is done at a point where auditors are unlikely to find or identify.

In today's business environment controls are designed to limit risk by containing fraud rather than eliminating it. Some organizations have realized that they are not have the tools to pre-empt fraud.

The most difficult thing with procurement frauds tracing the actual bribe including how and where it manifested A bribe extended to an employee will likely occur away work environment. It can be supplies to an individual's house or premises. Jon Hayton (Pricewaterhousecoopers).

To deter fraud, organizations have developed policies to handle conflict of interest. They are devised to help prevent fraud in early stages. Where there is possible proof it could be hard to infer the presence of material influence on the award of a contract.

Organizations must ensure they put in place measures to ensure their resources are well secured. Effective monitoring of risks rather than dependence on existing controls should be done.

In order to minimize exposure to procurement fraud organization's will have to look out for them within the entity.
Organizations need to look at all potential fraud avenues, identify weaknesses and use

intelligence possible fraudsters, rather than hoping the controls will work.

Sampling and auditing alone cannot not successfully detected fraud. It might occasionally stumble on a fraud, but that is just luck. Moreover, it is worth remembering that people perpetuate fraud and that their actions are not easily predicable.

It is therefore important to pose the question on how to effectively detect fraud in a modern business environment while minimizing disruption to business.

Detecting Procurement fraud

The widespread use of digital data storage and transmission has allowed investigators to be able to track and find cases of fraud. Electronic communication for example, leave behind an audit trail on any server through which it passes.

Data mining techniques are used to curb procurement fraud supported by availability of examinable pieces of information. Jon Hayton (Pricewaterhousecoopers).

Software agents can therefore be developed to seek out and deduce warning signals for fraud from such data.

A new dimension to fraud detection have been brought about by the use of SAP systems that enable investigators to identify who the purchaser within an organization is. The same information can be used similarly on credit card data to profile people thereby creating an account profile for every buyer. These profiles can be used to identify cases where vendors are favored. (Pricewaterhousecoopers).

Though firms find it difficult to quickly analyze information in an efficient way, it is still an efficient method. Since the required data has to be downloaded and analyzed detection will happen way after the procurement process has commenced.

E-procurement need to have real time detection as the procurement processes have become fully automated.

Network security breach patterns associated with fraud can be identified using intrusion systems. Artificial intelligence systems can profile users, learn their behavior and report anything unusual.

While organizations deploy online systems, websites and e-procurement, procurement processes are being changed significant.

Good Governance

The process of making decisions and the setting of formal and informal structures for the purpose of implementation (UNESCAP, 2007).

Transparency in public procurement is still problematic (Mitra and Gupta, 2007). Formal and informal structures are present in government.

Decisions in procurement and how to implement constitutes a formal structure. Informal structures uses undefined ways of making choices and involves use informal advisors which in many cases lead to fraud.

Good governance in supply chain involves: matters of accountability, transparency and integrity. It needs a fair process of transacting business. (Saxena, 2006).

Fraud therefore affects both the government and private business sectors.

The abuse of office for selfish gain constitutes an economic fraud. Political fraud on the other hand violates structured guidelines relating to distribution of resources for monetary benefit or partisan patronage (Ampratwum, 2008).

E-government can raise the performance of organizations hence making them more effective Hasan (2004). It is helps reduce fraud and bureaucracy while at the same time increasing transparency.

Research framework

A well defined e-procurement process should be able to safe on costs and help entities to realize monetary benefits (Subramaniam and Shaw, 2004).

Savings are realized by improving the purchasing processes. Such benefits are seen when more and more deployment of accurate automated procurement systems (Cox, 1999; Croom, 2000).

The level of transparency can be increased by adopting more ICT processes and ensuring they are properly used as per guidelines. (Subramaniam and Shaw, 2004).

Deployment of agents in e-government procurement will bring about accountability.

A clear procurement process ensures the best products or services are received within a reasonable price by public entities. (Evenett and Hoekman, 2005; Hui et al., 2011).

Siriluck Rotchanakitumnuai, (2013), Carried out a survey whose findings showed that a visible procurement process impact positively on cost and help minimize vendor collusion.

2.1 E-Procurement

In Kenya, Public procurement has undergone several reforms. It led to the enactment of Public Procurement and Disposal Act of the year 2005 and later the creation of an oversight body called the Public Procurement Oversight Authority. E-procurement for the public sector was the consequence of coming into effect of the e-government strategy paper of 2004.

E-procurement was to be implemented by June 2007, but was delayed. It was to allow the migration from a purely manual system that was error prone, slow, costly and by all standards.

Information Communication Technology in government offices has changed positively many public services (Aman and Kasimin, 2011). Public service delivery has improved following the

transition to e-government. It has been proven through research that internet has helped improve the speed in public sector service (NAO, 2014, Yusoff et al., 2010).

It has further helped in minimizing costs (Roman, 2013), and improving on accountability (Bertot et al., 2010, Krishnan et al., 2013).

There is a wide adoption and implementation of ICT in government procurement for goods, services and works (McCue and Roman, 2012).

Different countries have implemented different e-procurement models. They include: seller centric, buyer centric, e-market places or third party managed. These models can also be grouped as: public, mixed model and public private partnerships (Malela Akinyi, 2010).

According to Akinyi (2010) E-procurement is more than just providing a catalogue on the Internet. It may require several systems to be put in place so as to achieve results with sound strategy.

In August 2013, An electronic procurement and payment system was launched by Kenya's President Uhuru. He wanted to ensure Kenyans get quality services and that value for money was also derived. Public officers were therefore required to be transparent and accountable to the people.

He pointed out how Government was being overcharged for the procurement of goods, services and works. The government expected to stop the abuse of the procurement system by adopting e-procurement (Pscu 2013).

Government-supplier relationship can be made robust through e-procurement by providing easy access to information and simplifying the bidding process to ensure there is benefit accruing from cost reduction.

Integrated Financial Management Information System (IFMIS) ensures there is audit trail and identification of the actors in the procurement chain or transaction originators.

The implementation of this Procure-to-Pay system transitioned a new era to Government procurement.

Most of the e-procurement studies concentrate on the private entities. Angeles and Nath (2007) investigated difficulties the private sector experienced in e-procurement and came up with the following: standardization, system integration, and an immature e-procurement market.

Smart (2010) found out that the letdowns of implementing e-procurement are a result of process improvement, integration, adoption and change management.

More research work provide a wider analysis of the advantages of e-procurement (Tatsis et al., 2006; Puschman andAlt, 2005).

A few reports have focused on e-procurement in the public sector while looking at implementation benefits, risks and challenges (Croom, 2000).

Croom and Brandon-Jones (2007), Sought to comprehend the key difficulties of deploying e-procurement in the public sector. They focused on implementation and operation in public entities.

The following e-procurement areas were looked at: Specification, implementation, changes to organizational characteristics, changes in total acquisition costs, and changes to governance structures.

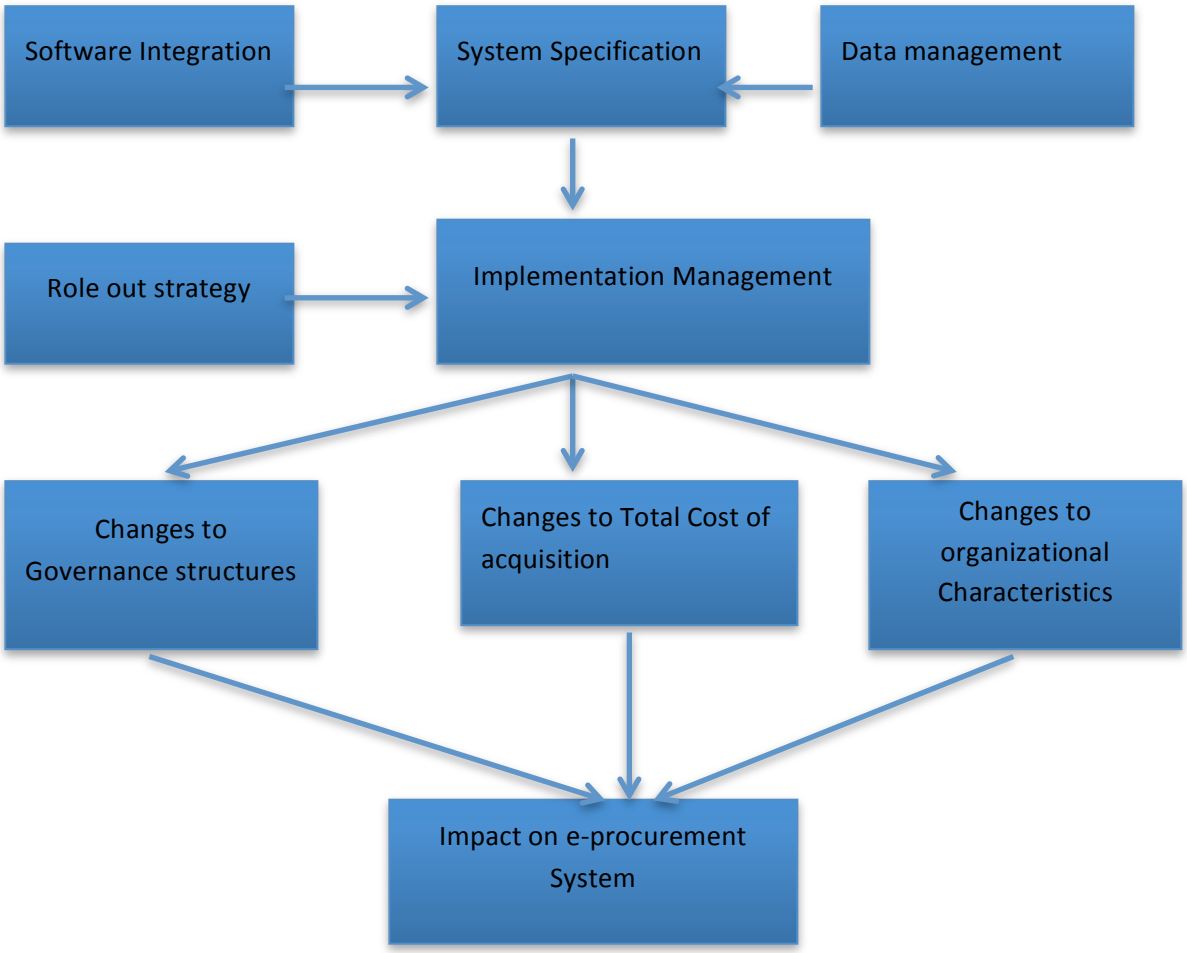
The e-procurement effects model by Croom and Brandon-Jones (2007) shows the cause and effect relationships in the implementation which are: system specification and implementation management. They show the impact of the variables on e-procurement by providing evidence of high supply availability, low search cost, and increased level of communication between clients

and vendors. They deduce the importance of system specification and implementation so as to impact e-procurement system in relation to governance structure, cost of acquisition changes and organizational characteristics.

They also bring out the importance of rollout strategy in software integration, implementation management, and data management. System specification problems and implementation management issues such as fraud are not discussed.

Understanding the challenges and limitations of e-procurement implementation in public sector is important due to the complexities of government policies and bureaucracy. Without a proper understanding the government will not maximize the gains from e-procurement system.

A framework is needed to solve the difficulties of e-procurement implementation in public sector such as fraud and assist in future system deployments. Agent technology can play a crucial role towards this objective.



Source: Croom and Brandon-Jones (2007)

Figure 2-1: Electronic-Procurement Effect Model.

Software integration links to suppliers and defines the customer's information infrastructure. Data management involves data capture and the employed scheme for coding. Issues in system specification include hardware, network and web server, where as issues in data management include limited information on expenditure, product and service specification.

2.2 Security of E-Procurement

The Government still needs to do much more before it can to take full advantage of e-commerce and e-procurement including getting the right technology. The following first need to be addressed:

Identification: Parties in a transaction should identify themselves to avoid spoofing. This means all actors in the procurement process use digital signatures to verify their identity on-line.

Synchronization: Since timing is important during occasions such as auction bidding and time stamping of transactions.

Confidentiality: A procurement system should put in place the necessary confidentiality measures.

Data Integrity: Requirement to ensure documents such as a tender specification or response submissions are not altered in any way.

Bandwidth: Bandwidth restrictions should improve as the service providers turn to B2B Internet commerce.

2.3 Fraud and public procurement

Fraud is abusing office for selfish personal gain. It is manifested through acts of bribery, embezzlement and state capture. Often, other illegal activities such as bid rigging, or money laundering are connected with it (OECD, 2014).

Arjun et al., 2012 in a paper that explored the ability of procurement systems to tackle fraud in the public procurement process, analyzed the risk factors of fraud procurement processes within government.

It looked at cases in third world countries and emerging economies while focusing on how to promote transparency and accountability. The outcome indicates that anti-corruption capabilities of public e-procurement brought about by automation and audit trail capabilities can increase transparency and accountability of government procurement process.

The government often seeks to buy the right goods and services at the right time with the right price and that is a key principle. The process should be transparent, open and objective.

Fraud leads to bottlenecks such as absence of accountability and transparency, lack of political control and auditing. To overcome fraud related challenges in the public procurement; ICT can be deployed. (Bertot, Jaeger & Grimes, 2010).

Fraud in public procurement is a big problem affecting most developing countries and with huge negative impact to a nation. It impedes wealth creation, it increases government expenditure, kills social fabric and trust in government, and also distorting government expenditure significantly increasing recurrent expenditure.

The price of corruption/fraud include loss of public funds through misallocation, high expenditure, poor quality of goods & services, and works (OECD, 2015). The people paying bribes attempt to get back their money by exaggerating prices, generating bills for work not done, performing sub standard work, diluting quality of work and supplying inferior goods/material.

Corruption in public procurement distorts competition, restricts the market and discourages foreign investors. Not surprisingly, many firms are demanding improved public procurement procedures. The 2014 Business and Industry Advisory Committee to the OECD (BIAC) Economic Survey shows that improving efficiency and transparency in public procurement is a key in public sector reforms

We have Integrity risks occurring in each of the stages in the procurement process as shown below:

During the year 2014/2015, a number of Ministries incurred expenditure adding to Kshs. 14 billion for which value for money could not be established. With no value in return, it is deemed to have been wasted (Auditor-General Report, 2014/2015).

ICTs can make a significant contribution to the fight against corruption. It can assist in information dissemination by government departments to citizens and vice versa. Technology can help to improve citizen participation and make the government more accountable (Chene, 2011). Such new technologies include the use of software agents.

Administrative abuses and fraud can be reported using technology. Whistle blowing can be done online using the web and mobile applications. (Sofia Wickberg, 2013)

There are many ways in which ICTs can contribute to the identification, reporting and exposure of fraud and bribery thereby decreasing their occurrence:

Innovations in ICT can drive governments to better public services, to improve communication and make information available to its citizens. It can also enhance public awareness on matters of corruption, abuse of office and monitoring government activities by citizens and civil society:

The role of ICTs in tackling corruption has created an opportunity for activism and civil demands by the techno servy people. Some ICT initiatives have been successfully implemented for monitoring and reporting purposes.

Governments information and services to citizens all over the world is increasingly being delivered over ICT to enhance the efficiency and increase citizen interaction. E-government has contributed to promotion of participatory and inclusive development and democracy (UNPAN, 2012).

Some e-government initiatives have been implemented successfully in the recent past are: e-procurement, e-taxation and e-judiciary.

2.4 Agents

Russel & Norvig (1995) define agents as objects in the environment that perceive and react to states in the environment.

An agent based system is one that is developed using agent. It may be made up of a single agent or multi-agents.

An agent based systems has the following features:

Autonomy: Agents that make independent decisions on what to do based on their internal states without a direct user input/influence.

Reactivity: Defines the ability of agents to sense the environment and respond quickly to the changes that happen.

Pro-activeness: Agents ability to exhibit some goal-directed behavior by initiating some action.

Social ability: Ability of agents to interact with other agents using an agent-communication language and participate in social activities like cooperation to negotiate or solve a problem so as to meet some goals.

Agents based systems are a new paradigm in software engineering because:

They are a natural metaphor: The agents can be conceived to be made-up of interacting, active and purposeful objects e.g. software agents that support online trading. Such software participants involved in online transactions as semi-autonomous agents.

Data control distribution: Overall control of software is distributed on several computers that may be geographically dispersed. They should be able to autonomously interact with each other.

Older systems can be incorporated into modern distributed systems by encapsulating them agents that allow them to interact.

Open systems: Open systems can be made to work effectively by incorporating the ability to engage in flexible autonomous decision-making.

There is low detection of fraud due to high personal gains or absence of serious prosecution or consequences when fraud is detected. This may induce some public servants to engage in corruption in procurement. National Integrity Survey (2002 , 2006)

According to a World Bank report (1998) over 90% of the fraud complaints received by the inspector general of Uganda relate to procurement.

2.5 Agent based Security issues

Mobile Agents have ability to move from computer to computer with ability to run from each of them. A network oriented environment pose a security challenge where neither the agent nor the computers can be trustworthy. An agent could harm a computer and gain access its resources.

The computer could as harm the agent and get private. They could both be maliciously programmed to harm the other

For mobile-agents, security is very important. Different approaches have been designed to address these problems. Ways should be sought to protect computers from being harmed by agents and vice versa. Very few systems deploy protection measures for agents.

In Tacoma, agents visiting other sites are treated as guests. The agents visiting foreign sites meet at an entry point in the new site. A firewall agent at the entry point can deal with, access control, authentication, accounting, and fault-tolerance to the guest agent (Johansen, 1995).

The firewall agent basically logs the agent code to disk. This provides accounting as the only security service provided. The agent code is first retrieved and be executed. At the endpoint, activation is done by the execution agent. This is meant to improve performance because firewall agents do not duplicate themselves but the execution agent do replicated (Johansen 1995).

In Agent Tcl, security issues relate to: protecting computers from agents, protecting agents from themselves, protecting agents from the computers, and protecting a group of computers from agents. In the latest implementation, The first two problems are addressed using authorization, authentication and enforcement in the latest version. Gray (1996a).

At authentication, Pretty Good Privacy technique is used. It encrypts a message using the a randomly chosen private key and IDEA private-key algorithm, encrypts the private key using the RSA public-key algorithm and the recipient's public key, and then sends the encrypted key and file to the recipient.

The agent registers with the server, and a request is digitally signed using the owner's private key, encrypted with the server's public key, and transmitted to the server which checks if the agent owner is allowed to register on that computer. Communication between the agent and the server is done using IDEA key to prevent malicious agents from masquerading as an existing agent during a particular session.

During migration, digitally signing of agents with the server's private key and encryption with the recipient server's public key is done.

Security in Telescript is done where the server seeks to be safeguarded from an incoming malicious agent. The agent also needs its information safeguarded while traversing from one

computer to another. In the system each stage has its own guidelines while every engine runs a system wide policy.

2.6 Conceptual Model

High level design architecture

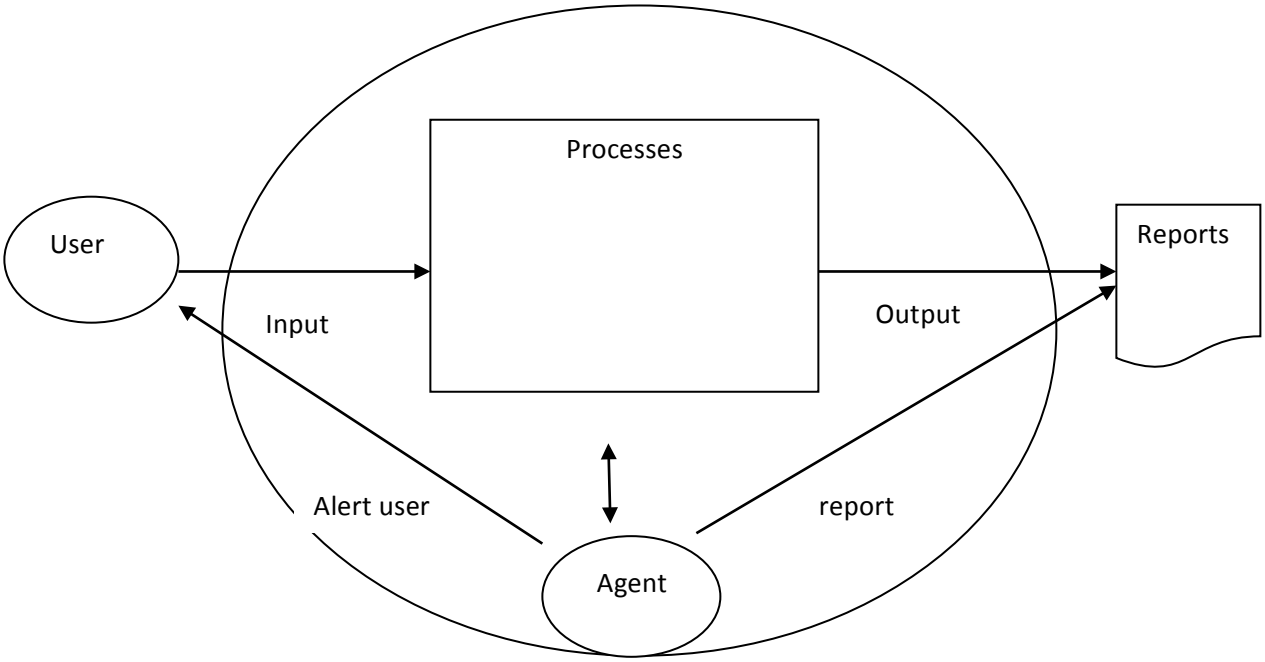


Figure 2-3: High level e-Procurement design model with agents

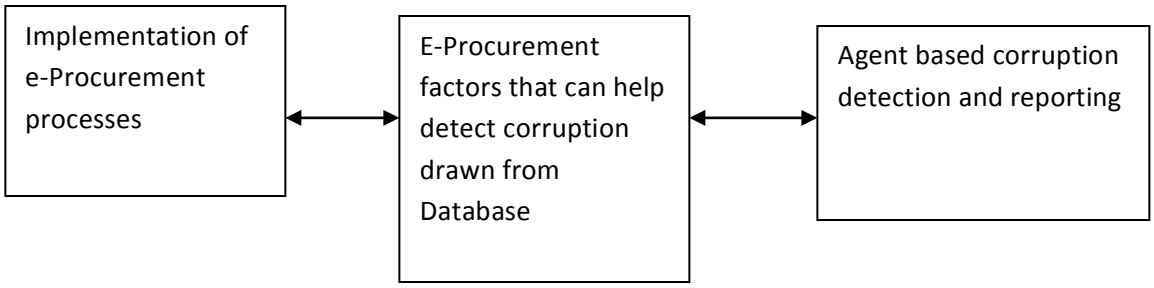


Figure 2-4: E-procurement processes and agents interaction with database

Chapter Three:

3 Methodology

A methodology is a step by step analysis of the method applied to an area of study. It involves analysis of the methods and principles associated with a branch of discipline.

For this project we have selected the MAS-CommonKADS methodology because it fits best this project.

3.1 Agent Methodology

Agent-based computing is a new software engineering paradigm that uses agent-oriented software engineering (AOSE).

Adequate abstractions are used in Agent methodologies to model and support agents and multi agent systems. They focus on an organized society of agents playing roles within a given environment while allowing agents to interact according to role based agent protocols.

3.1.1 The MAS-CommonKADS Methodology.

MAS-CommonKADS is an agent-oriented software engineering method to help in analyzing and designing multi-agent systems. It is composed of several design phases:

a. Conceptualization: where the multi-agent system is conceived and agent properties are identified. Definition of a use cases will help understand the system and thereby describe the problem.

b. Analysis: Involves developing different models for analyzing the system. This phase phase determines the functional requirements and come up with models.

c. Design: Uses both bottom-up and top-down approach in design. It may develop new components or reuse others based on agent environment. It uses analysis models to transform them into specifications for implementation. It also determines the internal and

network structure of the agent.

d. Development and testing: This is where the agents are developed and tested.

The methodology comes up with the following models:

- Agent model to show features such as: ability to reason, sensory skills, agent groups, and hierarchies.

- Task model that describes what the agent will do.

- Expertise model to define the knowledge needed by the agents in order to be able to achieve their goals.

- Organization model showing where the MAS is going to be introduced and the social organization of the agent society.

- Coordination model showing communication between agents, agent interaction, protocol, and their required capabilities.

- Communication model detailing human factors for developing user interfaces and human-software agent interactions.

- Design model that combines previous models consisting of the following sub-models: network design, for designing network infrastructure, agent design, for composing agents of the analysis and choosing the best agent architecture for each agent; and platform design, for choosing the platform for agent development.

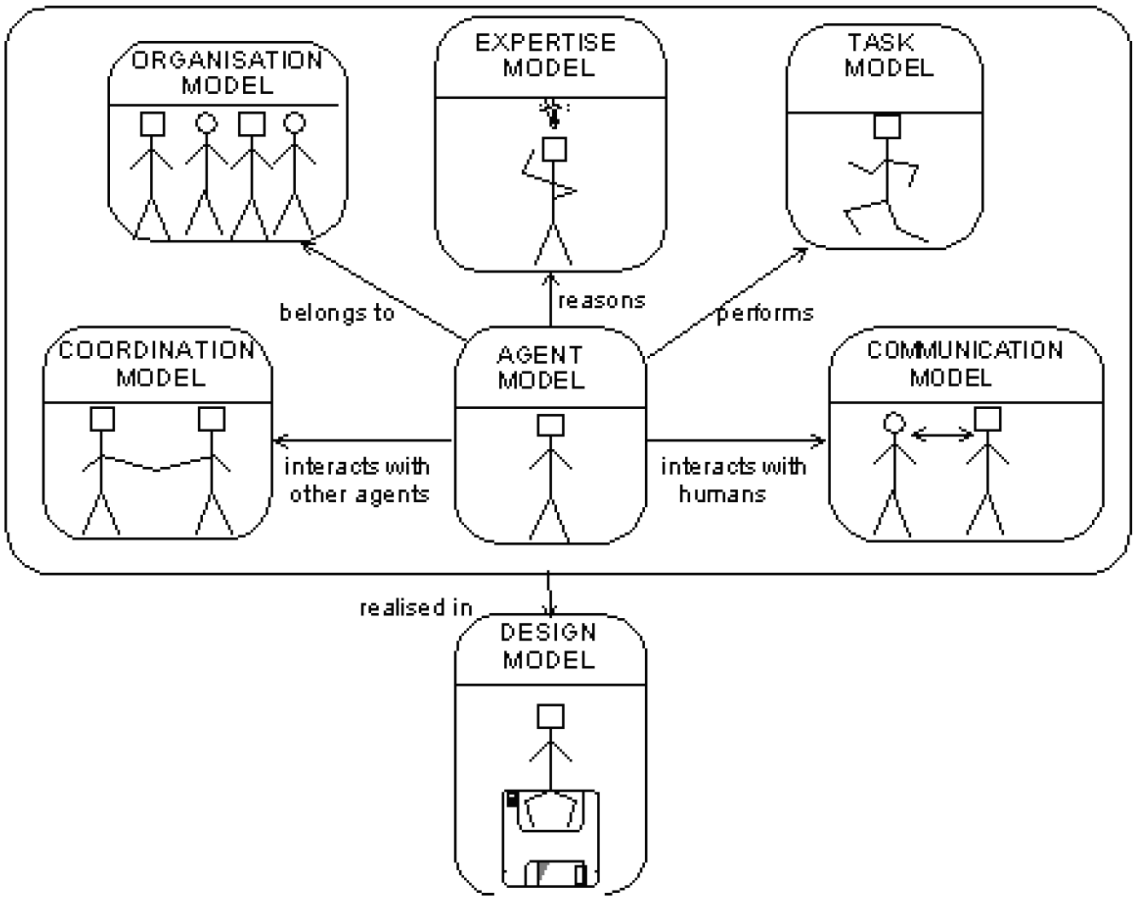


Figure 3-1: Model for MAS CommonKADS Methodology

Source: Idea Group (2005)

3.2 Data Collection

3.2.1 Sources of Data

We have used both primary and secondary data sources. Primary sources include literature review, interviews and observation, while secondary sources is input of data into the prototype to demonstrate the working of the system.

3.2.2 Data Collection Tools.

Interviews

The oral interviewing of national government employees was done in order to get the weak points of the IFMIS system that could be exploited as avenues for fraud. The key employees include: accountants, supply chain management officers (SCMO), internal auditors, IFMIS system requesters and ICT Officers.

Observation

Observation is one of the data collection methods we will use in this study. We will observe the way information flow in the IFMIS system in order to understand the kind of data that is collected and stored on the IFMIS database.

Prototype system

This method is very useful since it will not be possible to get authorization to experiment on the actual online IFMIS system. There will be no cause for security breaches since all data used will be test data.

Questionnaire

Questionnaires will be administered to those who will test the fraud detection agent so as to get feedback on its effectiveness at detecting and reporting fraud. It will also help get suggestions on what should be improved or added on a practical point of view.

Data Analysis

For analyzing the data in the simulated IFMIS databases, we will use SQL query commands and compare the variance of estimated unit cost of items and actual prices, check activity of users in the IFMIS system among other factors that can help detect fraud.

3.3 Prototype Implementation and Testing

The implementation of the prototype system will be done on a high-end computer (Simulating the IFMIS application server(online e-procurement)) and another computer simulating the front-

end interaction by users requesting for goods and services and getting procurement approvals.

Java Runtime Environment (JRE) and JADE will be installed

Oracle Database will also be installed and configured to implement the procurement modules.

Chapter Four:

4 Analysis and Design

4.1 Overview

The analysis and design of the system was guided by the MAS-CommonKADS agent methodology, which has been discussed in chapter 3. In this chapter we will look at how the methodology was used in analyzing and designing the system. As outlined by the MAS-CommonKADS Methodology, we will look at four major steps, which are: Conceptualization, Analysis, Design and Development and Testing.

4.2 Conceptualization

Functional requirements of our system are first identified. Use Case technique is used to elicit ideas of the system. The technique involves users of the systems and user goals identification, while stating how to realize them.

It is a very simple technique that is useful for eliciting and validating them.

To conceptualize an agent-based system, two techniques are used: the User-Environment-Responsibility cases technique dealing with identification of use, reaction, and goal cases of an agent or a multi-agent system, and the enhanced Class-Collaboration-Responsibility Cards technique dealing with the identification of plans, responsibilities and collaborations between agents. We will in our case use UER Technique.

User-Centered Analysis.

The actors who are potential users of the together with their possible tasks and roles are brought out. The outcome is a set of use cases. User centered analysis tries to define the possible uses of the agent based system.

Identify the Actors.

The roles played by the actors in this system are: Requester, Supplier, Approver and Fraud Detector. Each role is a different actor. There are human actors and agent actors.

- Identification of the Use Cases.

The process is carried out by: defining the tasks or functions are that are carried out by the actors, identifying the information acquired and those changed or generated or changed, checking for feedback from any actor on external changes in the system and identifying any unexpected changes that need to be communicated.

- Environment-Centered Analysis.

Here the relevant objects of the environment and possible actions and reactions of agents are identified so as to be used for sensor modeling. That is done by identifying objects in the environment, showing possible events coming from each object and determining hierarchy, defining the possible actions agents can perform in the environment, describing reactions coming from interaction with the environment, identify group-related reactive cases, and describing the reactive goal: its name, the activation/deactivation condition, and the success/failure condition.

- Responsibility-Driven Analysis.

This is a goal-driven analysis that involves definition of system requirements that should be fulfilled without the direct interaction with the user.

It has the following steps:

1. Identification of responsibilities or goals of the system that require action.

Involves looking at non-functional requirements, such as time and security.

Describe when an internal variable of an agent can achieve an undesirable value and actions to be carried out for example where there are too many processes.

Describe possible failure or an undesirable states in the system that should require action in order to avert.

2. Describe the proactive goal
3. Ensure the grouping of related goals using the relationships “extends” or “includes.”

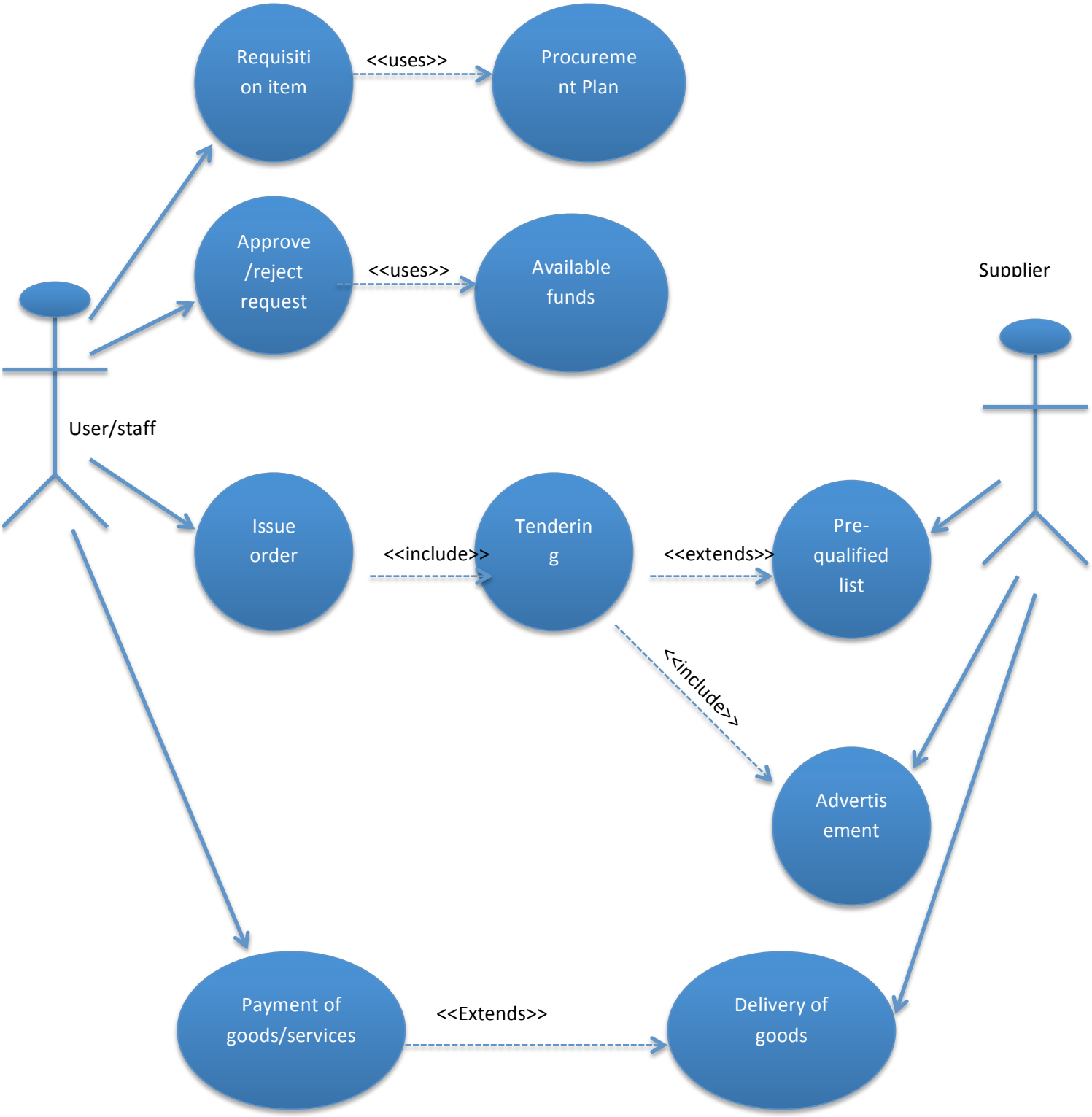


Figure 4-1: E-Procurement Use case diagram

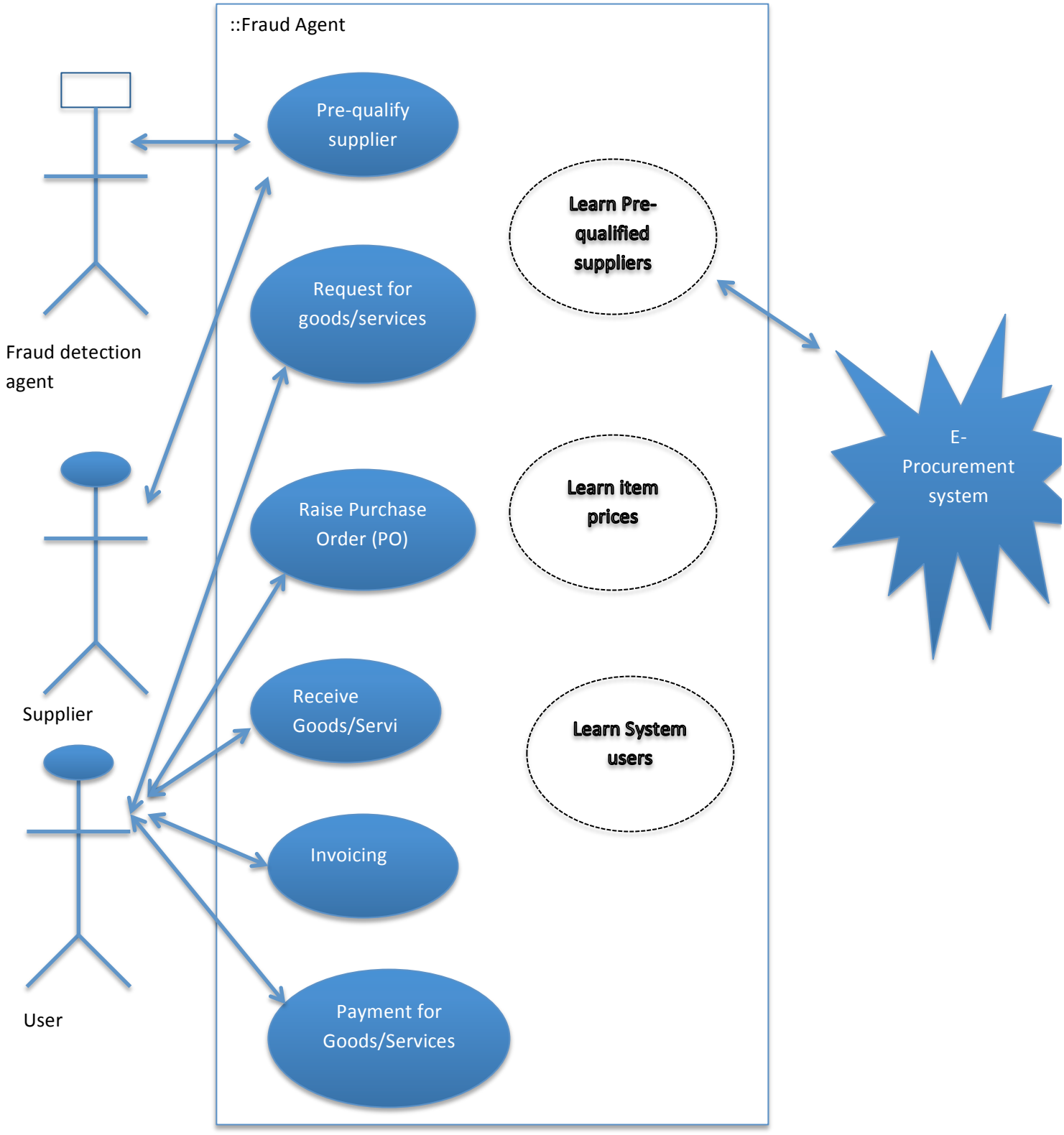


Figure 4-2: UER cases for the Public e-Procurement System

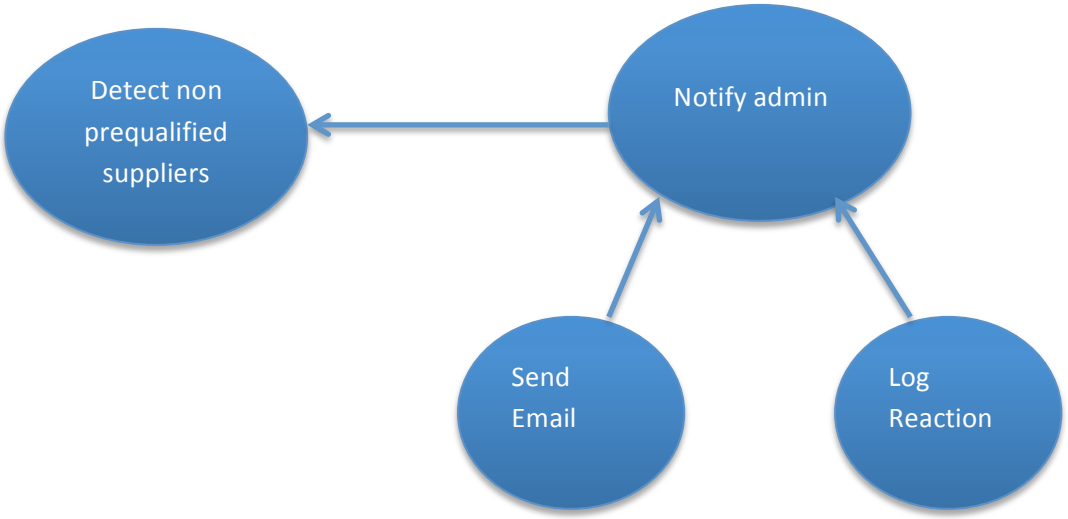


Figure 4-3: Reactive case relationship diagram depicting non prequalified suppliers

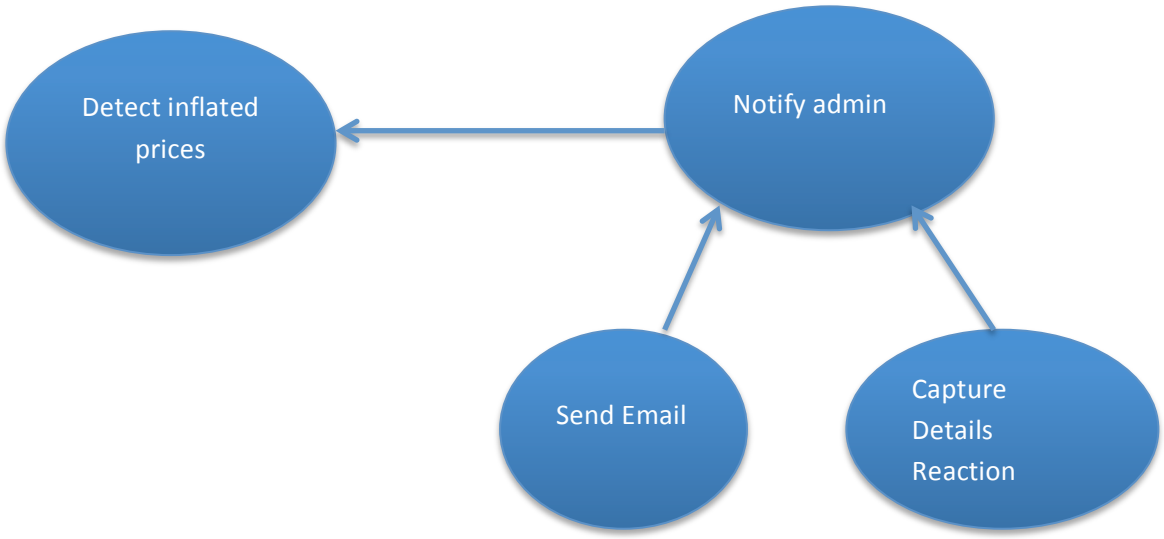


Figure 4-4: Reactive case relationship diagram depicting inflated prices

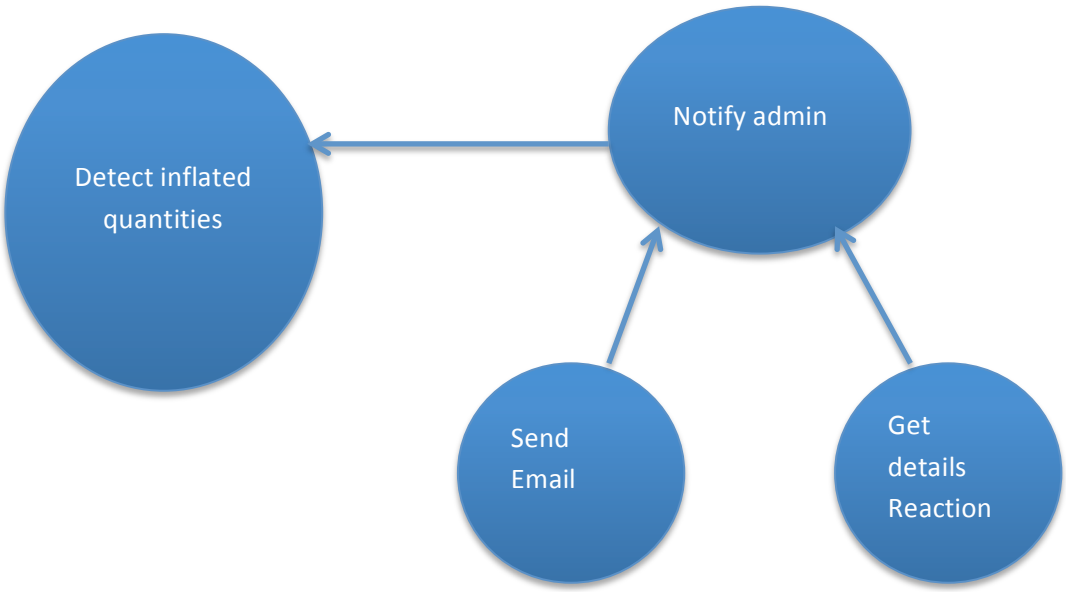


Figure 4-5: Reactive case relationship diagram depicting inflated quantities

4.3 Design

After analysis, a determination of agents is done. This involves coming up with a model.

The design model consists of:

- An agent network design which defines the architecture of the agent and consists of knowledge, coordination and network features. Agent supporting the features depending on what is needed such as:

  Network facilities such as agent name service, subscription service, security level,

encryption and authentication, transport/application protocol and accounting service.

Knowledge facilities defining ontology servers, knowledge representation language translators.

Coordination facilities describing available coordination protocols and primitives, protocol servers, group management facilities, facilities for assistance in coordination of shared goals, police agents for detecting misbehaviors and the control of the usage of common resources.

- Agent design: To help develop an appropriate architecture for each agent. Some agents can be introduced according to workable criteria. Each agent is subdivided in modules for user-communication, agent communication (from coordination model), deliberation and reaction (from expertise, agent, and organisation models), and external skills and services (from agent, expertise, and task models).

- Platform design: Which involves selection of the software and hardware that is needed for the system.

4.3.1 Database design

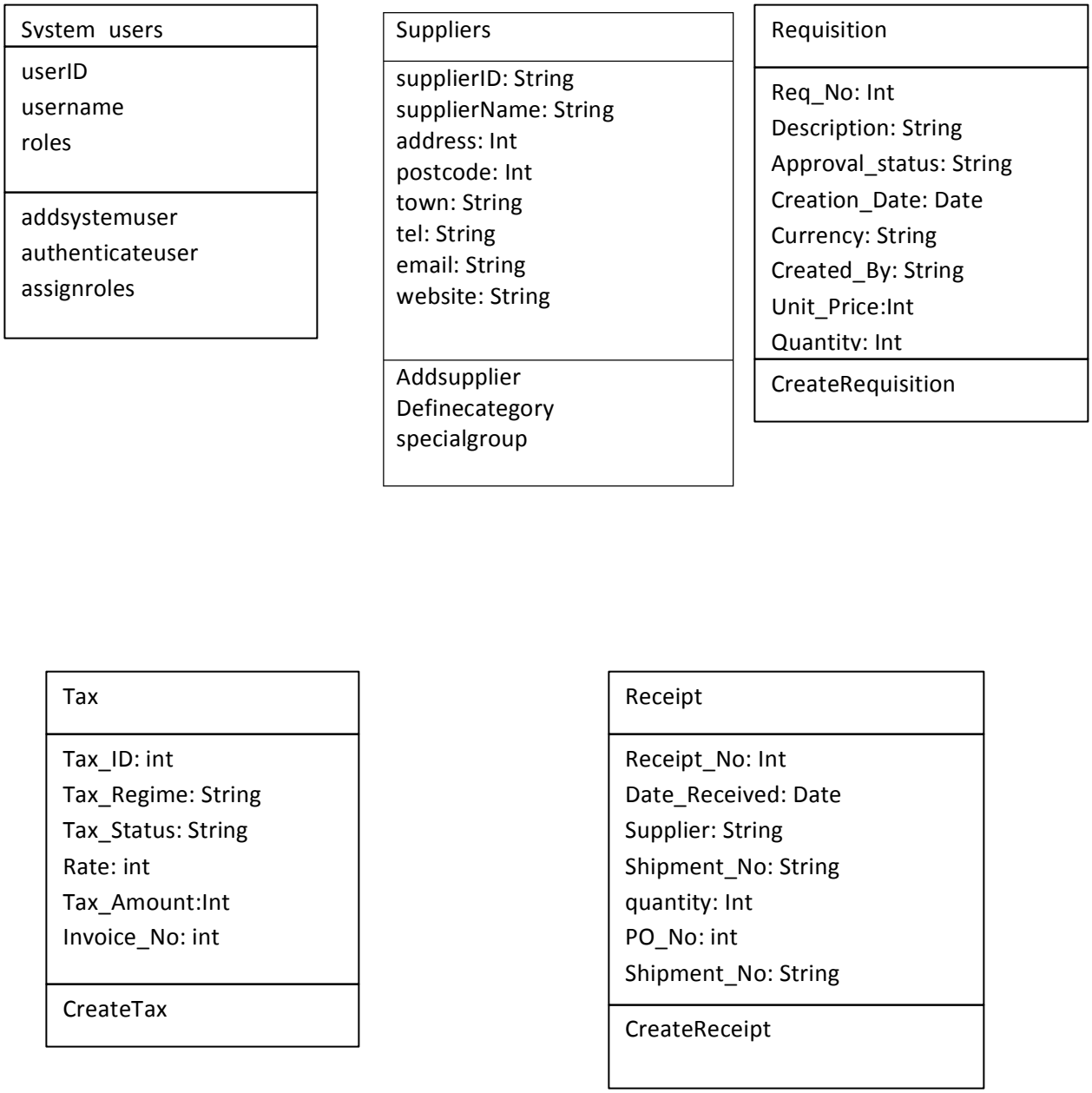


Figure 4-6: Database Design

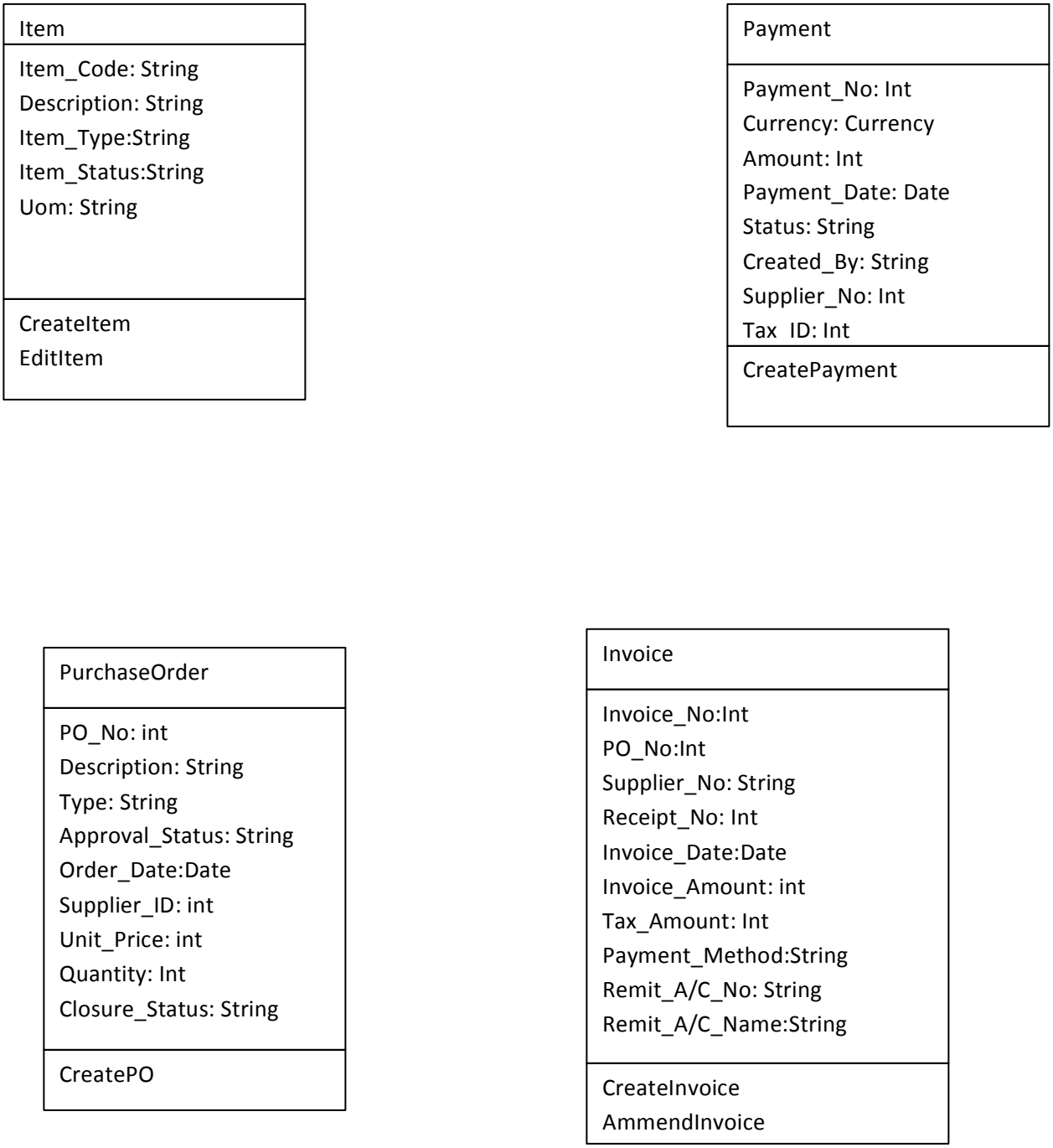


Figure 4-7: Database design

Table 4-1: E-Procurement Test Data

item code	Description	Item Unit price	Requisition Price	Requisition Quantity	PO Price	PO Quantity
AS20000	205 Digital Camera	5000	15000	2	15000	2
AS34300	HP ProLiant DL740 - Xeon MP 3 GHz	2000	2000	3	2000	3
AS35400	MS Exchange Email Server	8000	8000	1	8000	3
AS44400	President Model Desktop PC	1500	1500	4	1500	10
AS54111	Sentinel Standard Desktop - TP	1000	10000	2	10000	2
f11000	Desk - Capitalizable, taxable item	2500	2500	1	2500	2
CM00056	Battery Backup (DA-130)	450				
CM00057	Battery Backup (DA-290)	650				
CM08512	RAM - 512MB	1000				
CM10009	512 MEMORY	1000				
CM20571	Inks - Cartridge	100				

The above data will be captured onto the simulated public e-procurement system. The variation in unit price and quantities at various stages in the procurement process will be used to test the effectiveness of the fraud detection agent in picking out such malpractices and sending out notification to that effect.

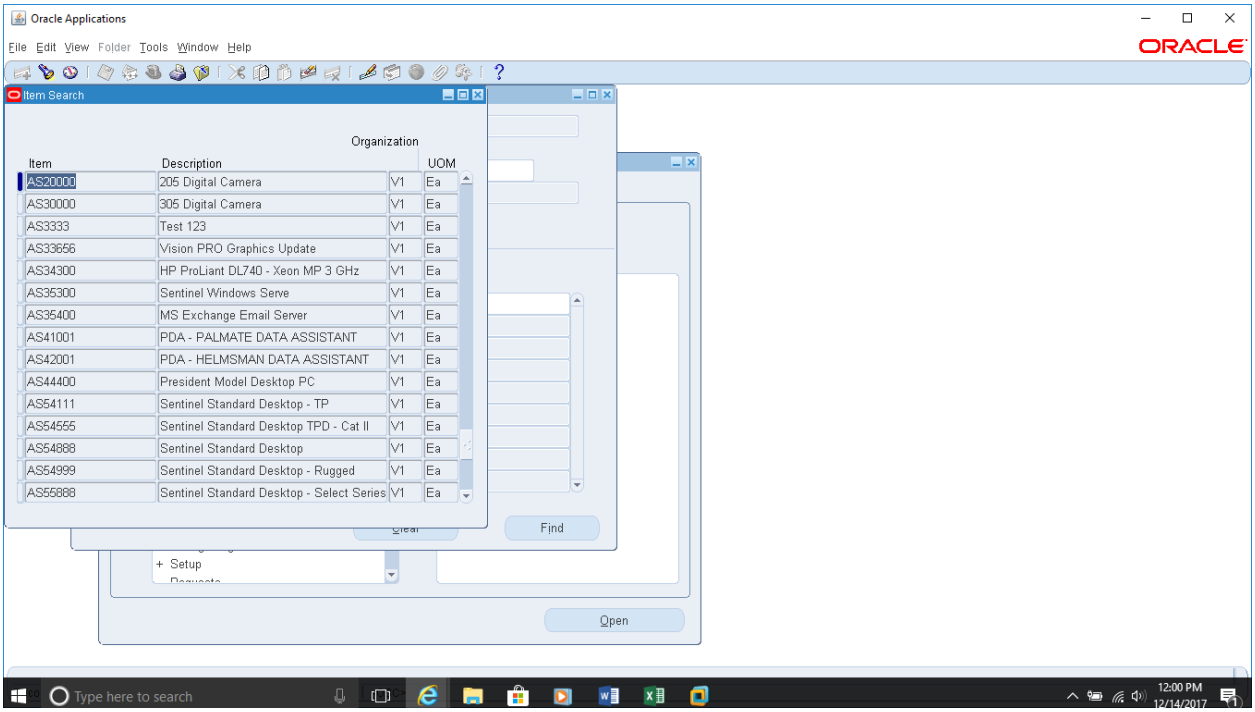


Figure 4-8: Item Master list

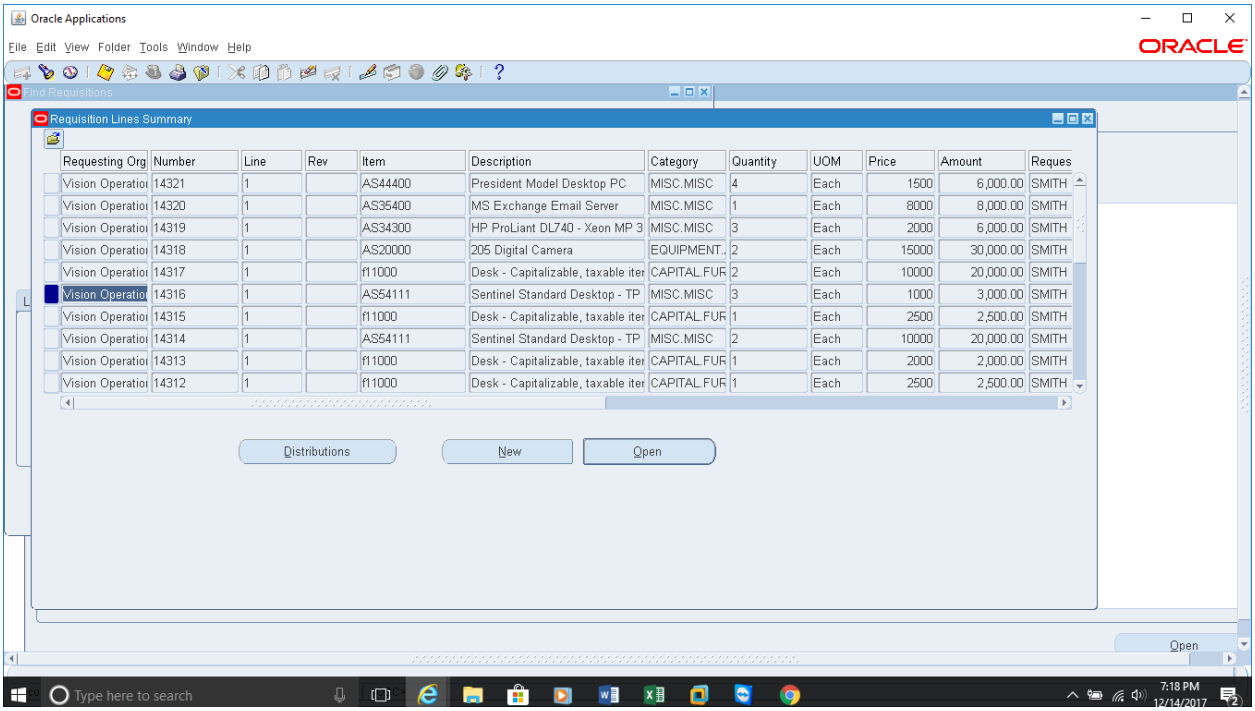


Figure 4-9: Requisition Simulation summary

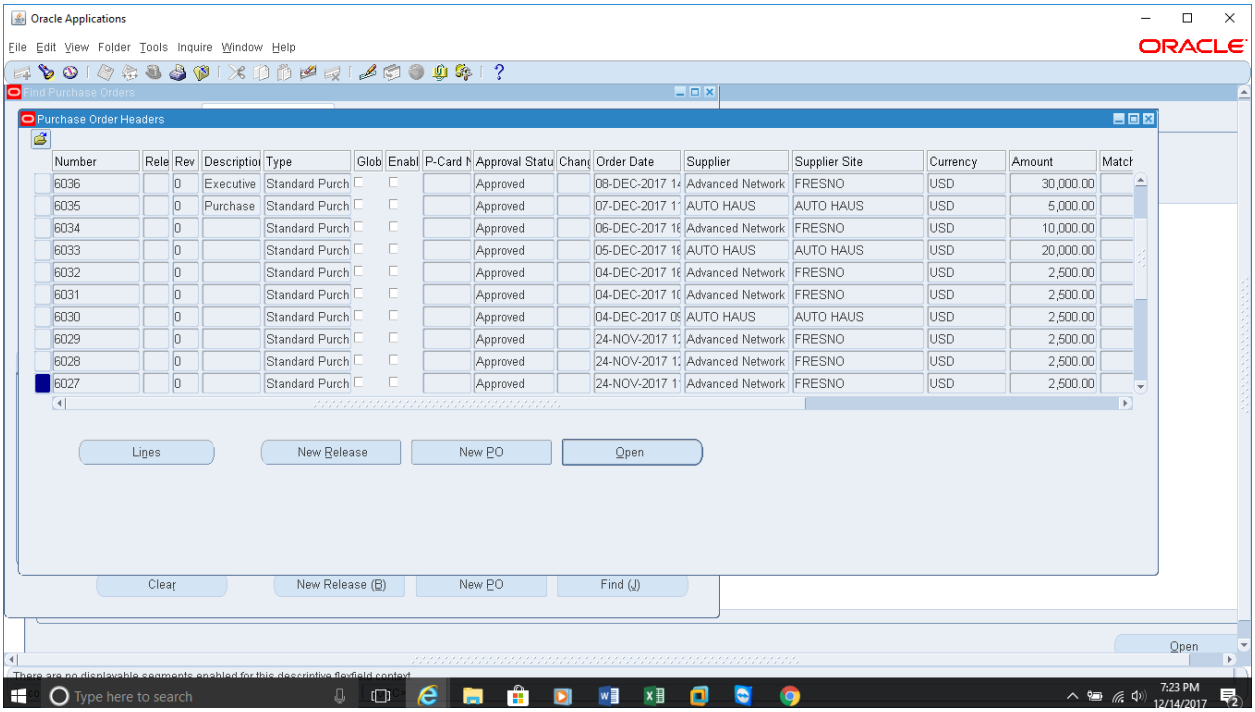


Figure 4-10: Purchase order summary

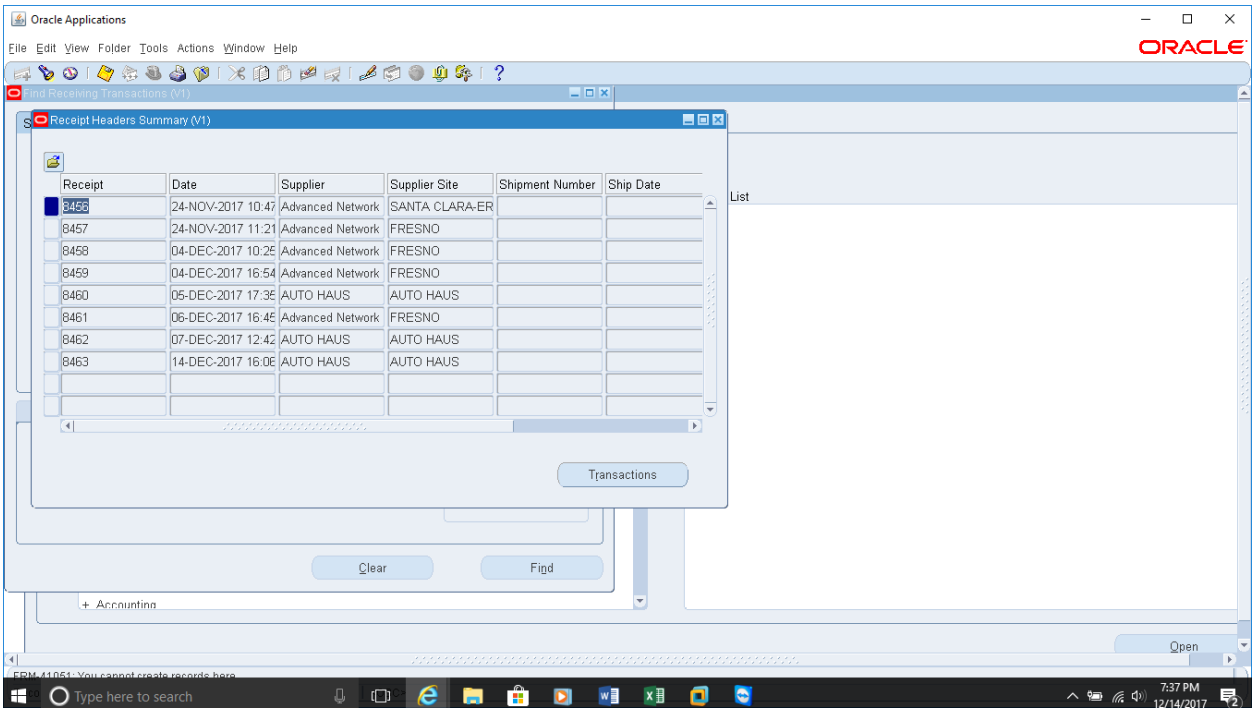


Figure 4-11: Receipts Summary

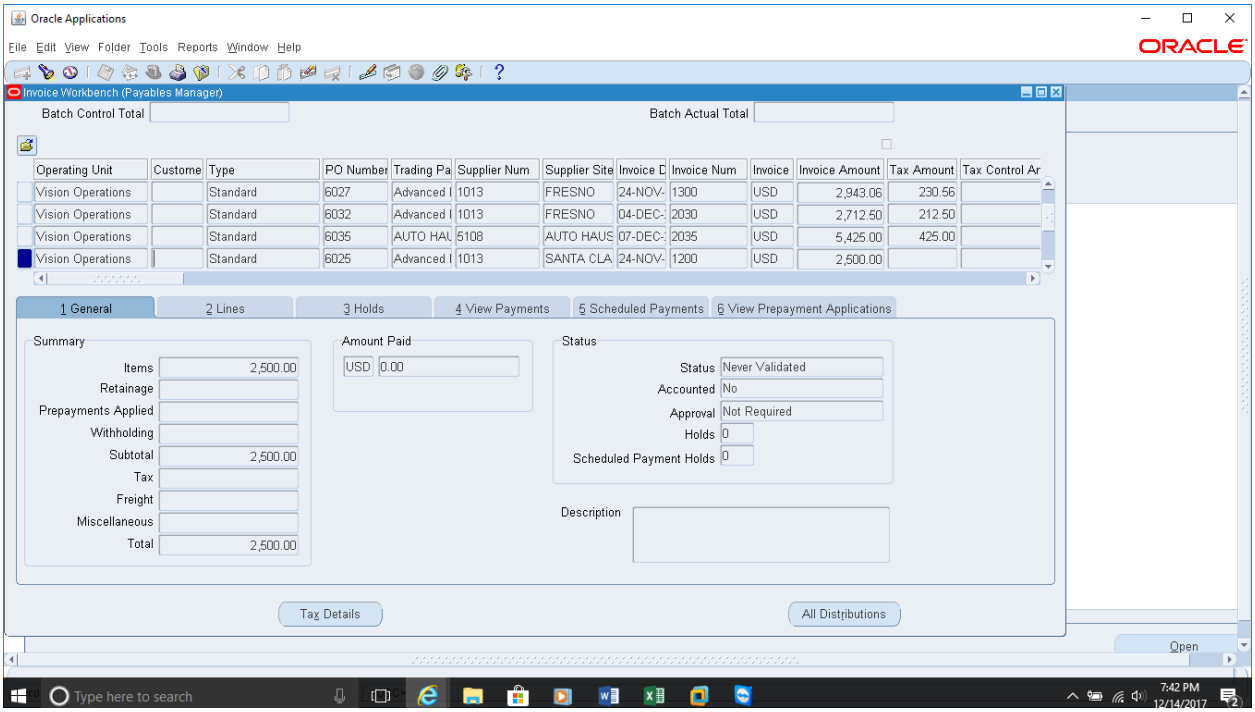


Figure 4-12: Invoice Summary

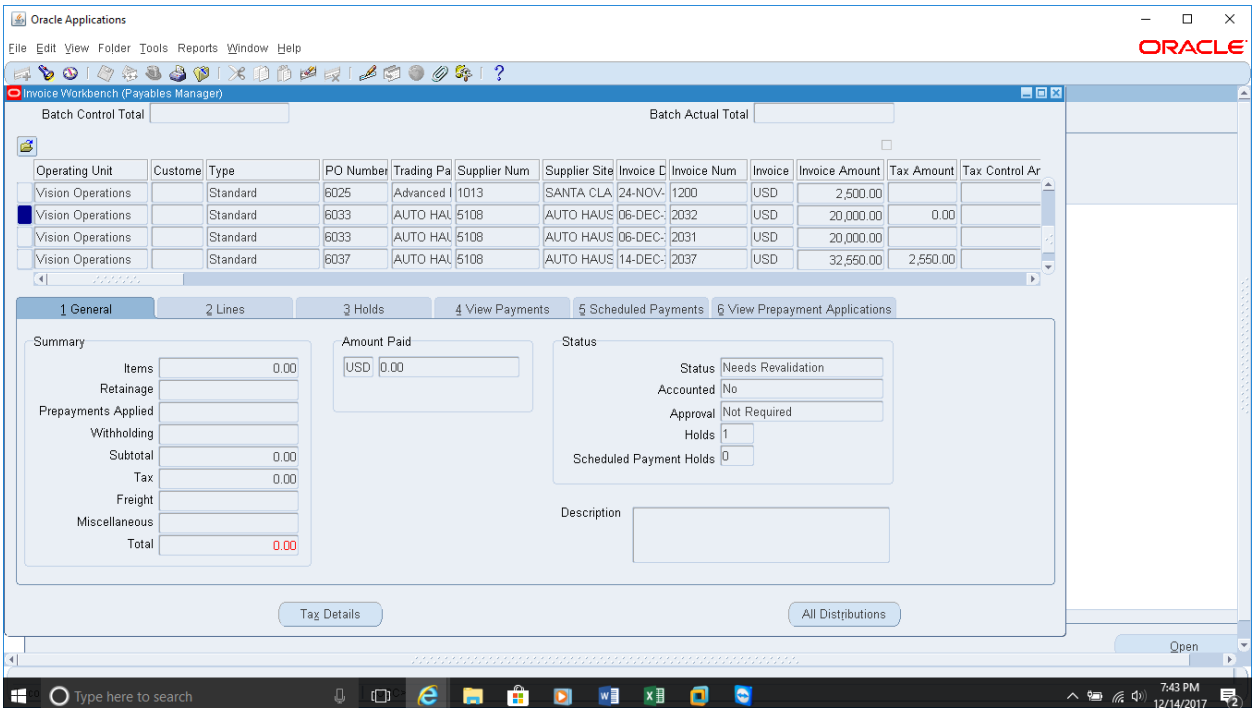


Figure 4-13: Invoice Summary

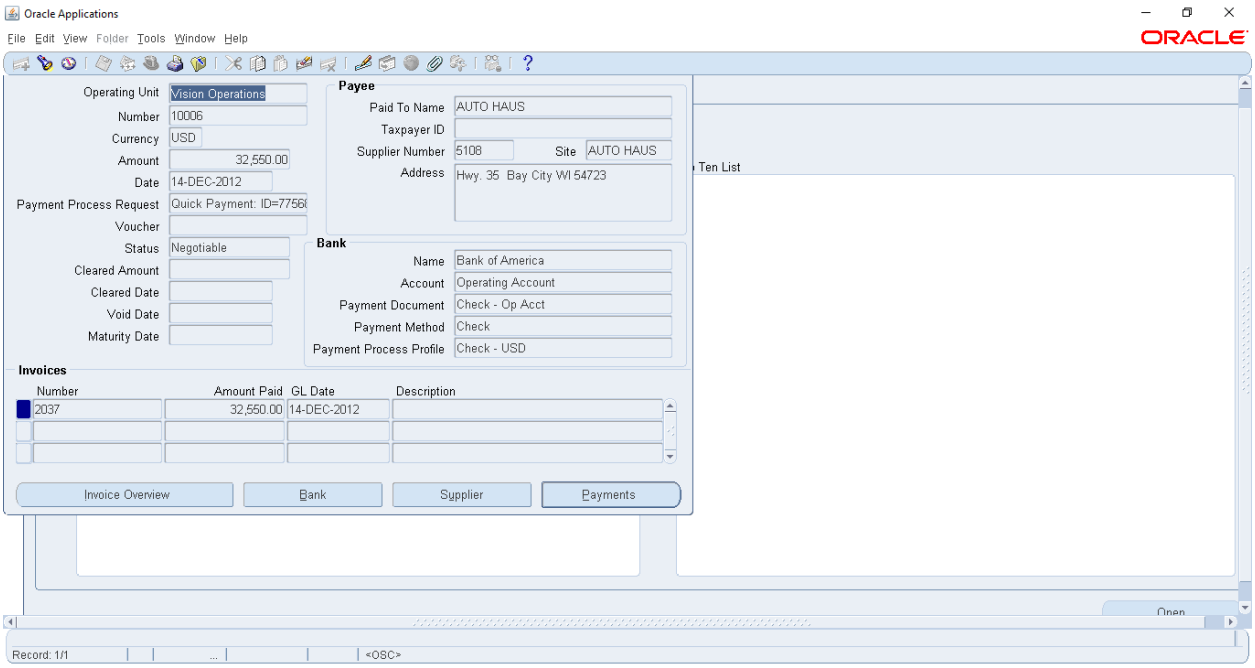


Figure 4-14: Payment report sample

Chapter Five:

5 Implementation

This chapter discusses the implementation process of the prototype and presentation of the results.

The system has been implemented using a combination of frameworks. The Multi –agent component has been implemented using JADE (Java Agent Development Environment) to monitor the activities of various processes (e.g. Requisitions, Purchase Orders, Receipts, Invoicing and Payments) and report where fraud is detected.

The user interface on the other hand is implemented using Eclipse. It is worth to note also that JADE in this implementation has been made to run within Java Eclipse.

5.1 Implementation Tools

A number of tools have been used to implement this system. The tools are as follows:

Eclipse Application-used to code and design agent diagrams.

Intelli J Idea- used to code the agent and establish connection to the database.

Java SE - Java Development Kit (JDK), Server Java Runtime Environment (Server JRE), and Java Runtime Environment (JRE). Contains library for extending java and which supports Eclipse.

Jade Framework -Provide Agent management system (AMS) , Directory facilitators (Df) and Remote management Access(RMA).Used as agent development environment

Databases – Oracle Database 11g is used to design and simulate the e-procurement system.

Web server computer -Installed with Redhat linux 7 and VMware.

Client computers -Installed with Windows 7 professional.

5.2 System testing

System testing was done in one national government ministry among existing IFMIS users who were willing to run and observe the behavior of the agent based fraud detection system.

Users were asked to give feedback in the form of a questionnaire highlighting positive and negative aspects of the agent program. They were also asked to suggest aspects that they think could be included to improve the fraud detection agent in future developments.

The first reaction was a positive evaluation of the system as being able to detect fraud relating to item price variations on both Purchase Orders and Invoices where authorization had been given on different unit costs at requisition level.

There was also a positive evaluation for quantity variations beyond what had been initially authorized.

The system was tested using a simulated e-procurement system where users where given an opportunity to requisition for items and attempt to commit fraud on the simulated system by excessively altering prices and quantities along the procurement process.

The agent was able to connect to the simulated system and continuously and autonomously scan for variations and entries that were suspect.

5.3 Discussion of results

5.3.1 Challenges facing e-procurement fraud detection agents

The system needs to be prompted by the user in order to start monitoring the activities of the public e-procurement system. A user can therefore deliberately disable the system to avoid such transaction monitoring.

A user can also disable the LAN or WAN infrastructure thereby disconnecting the link between the fraud agent system and the e-procurement system.

Agents have to be granted access privileges to a database in order to be able to scrutinize the activities in a database environment. When such privileges and rights are denied an agent like any other user will not be able to establish a connection.

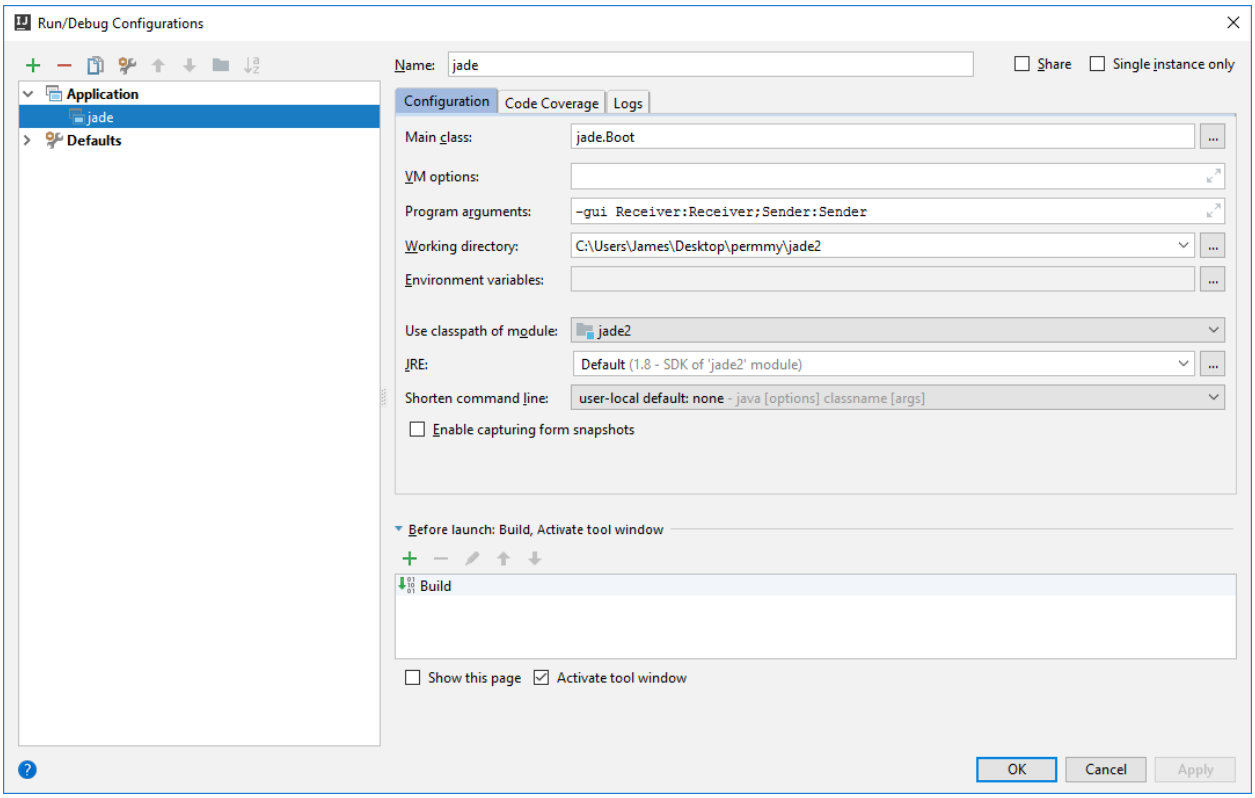


Figure 5-1: Jade Agent Configuration

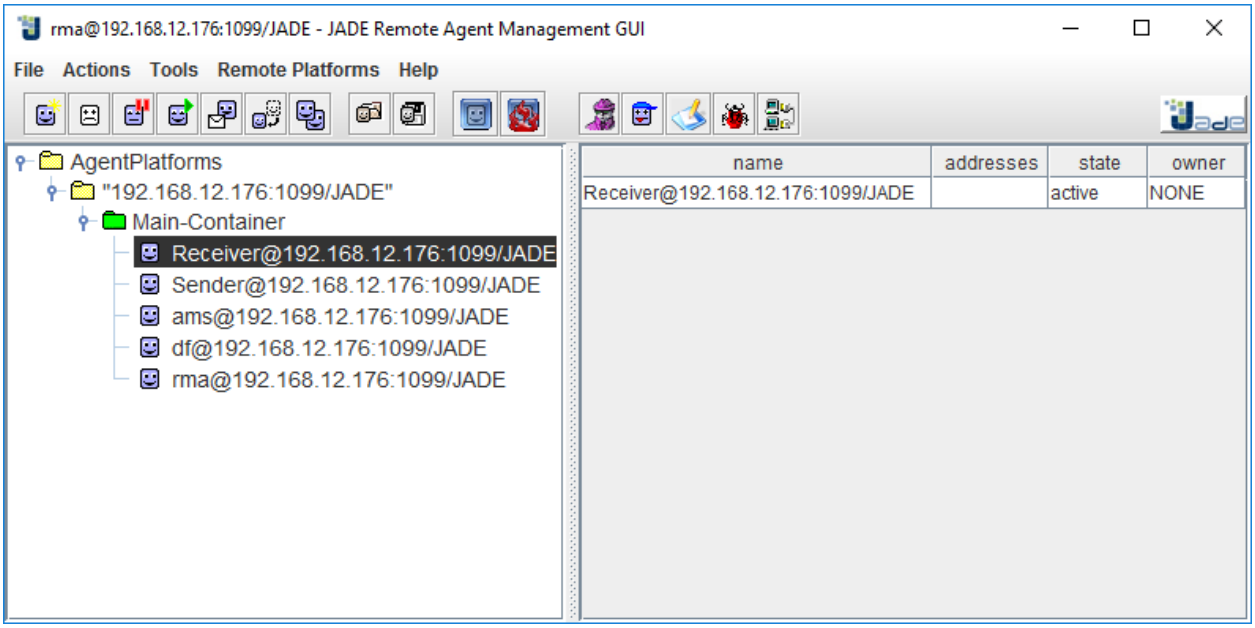


Figure 5-2: Fraud agent communication architecture

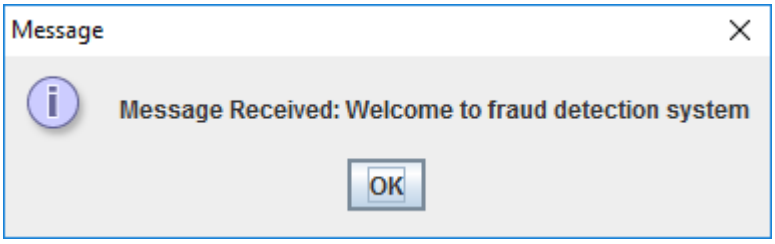


Figure 5-3: Agent receiver notification

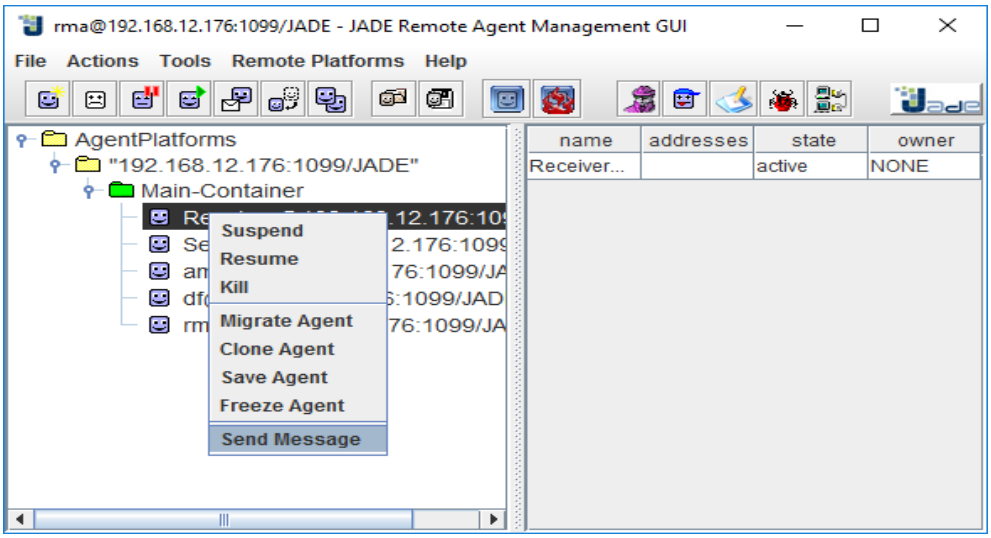


Figure 5-4: Agent messaging

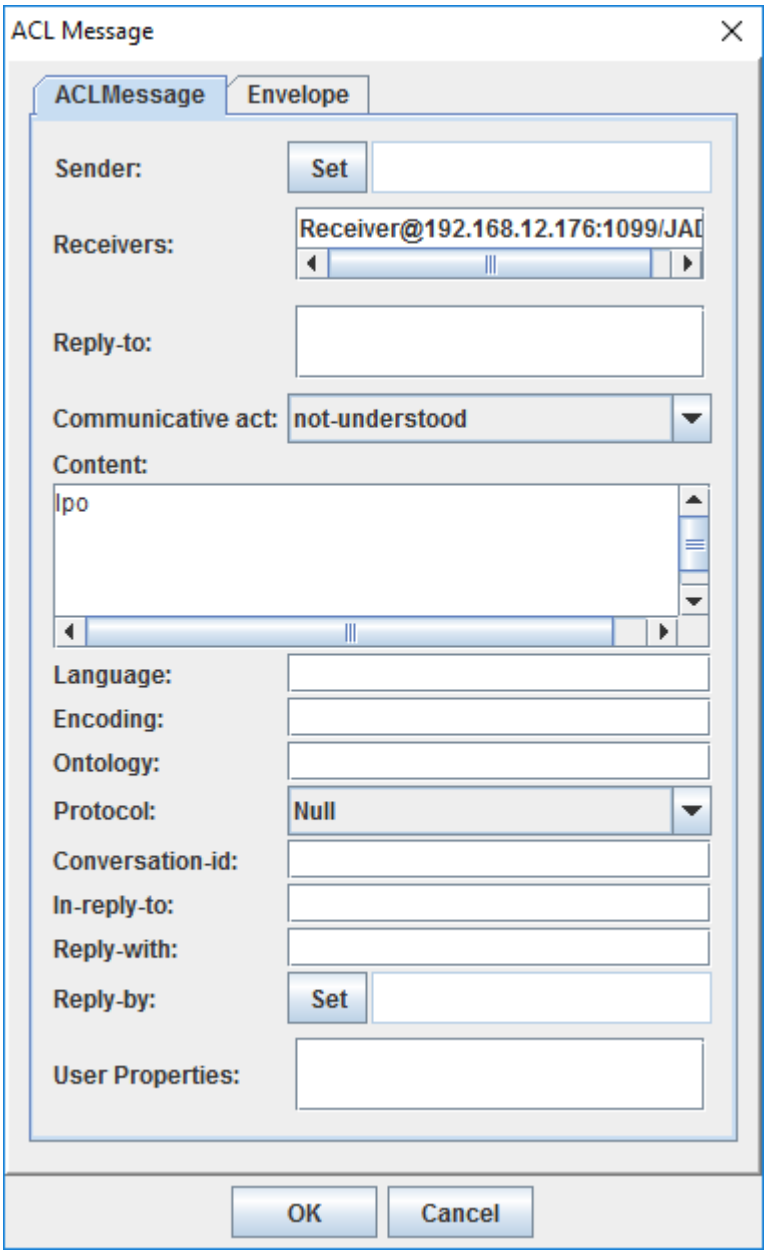


Figure 5-5: Agent message to trigger LPO Agent

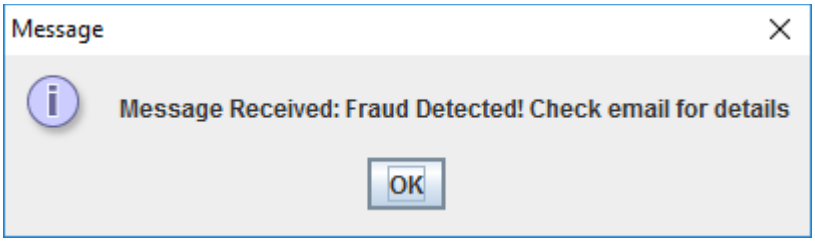


Figure 5-6: Feedback from LPO Agent

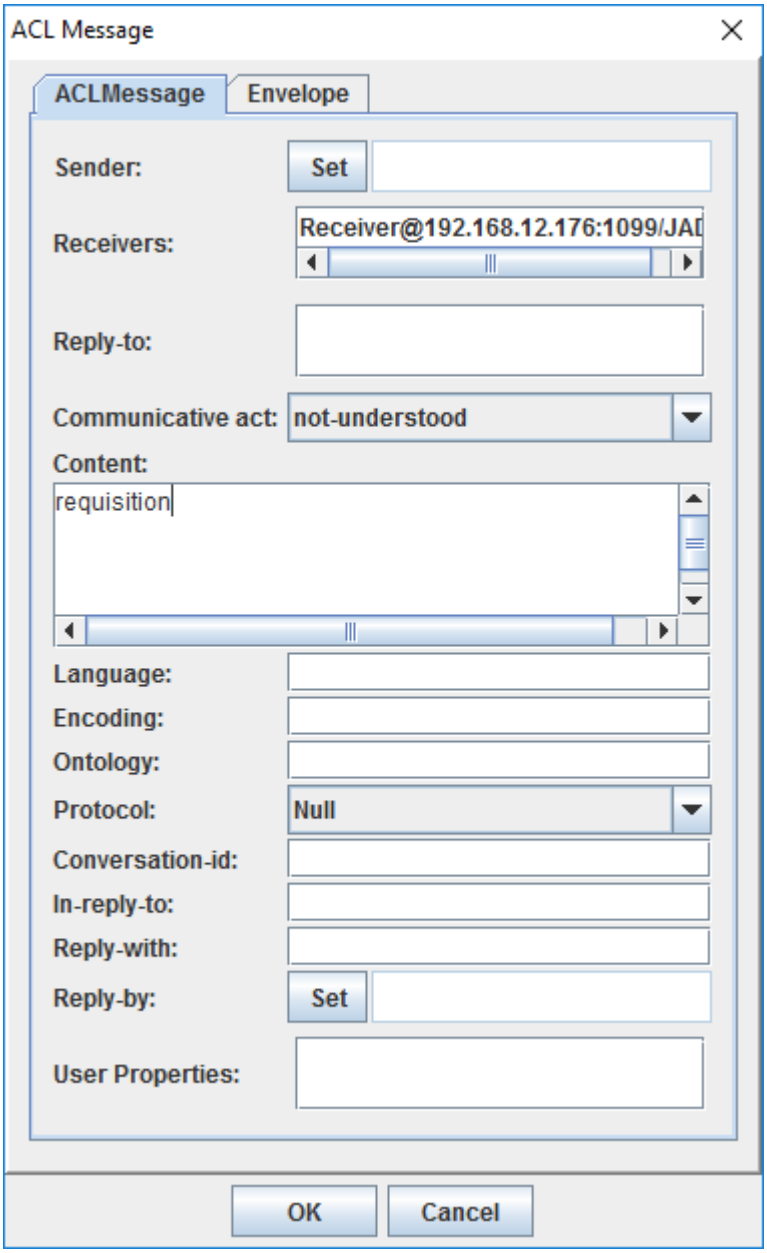


Figure 5-7: Agent message to trigger Requisition Agent

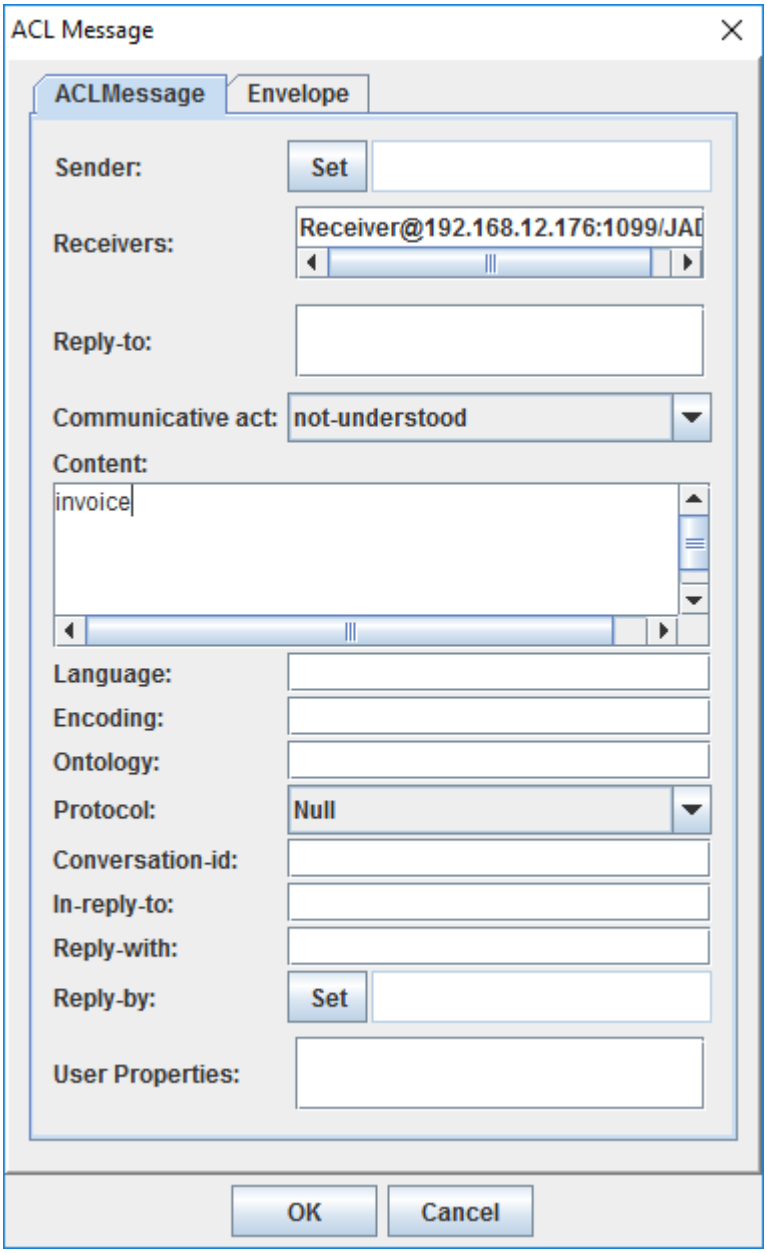


Figure 5-8: Agent message to trigger Invoicing Agent

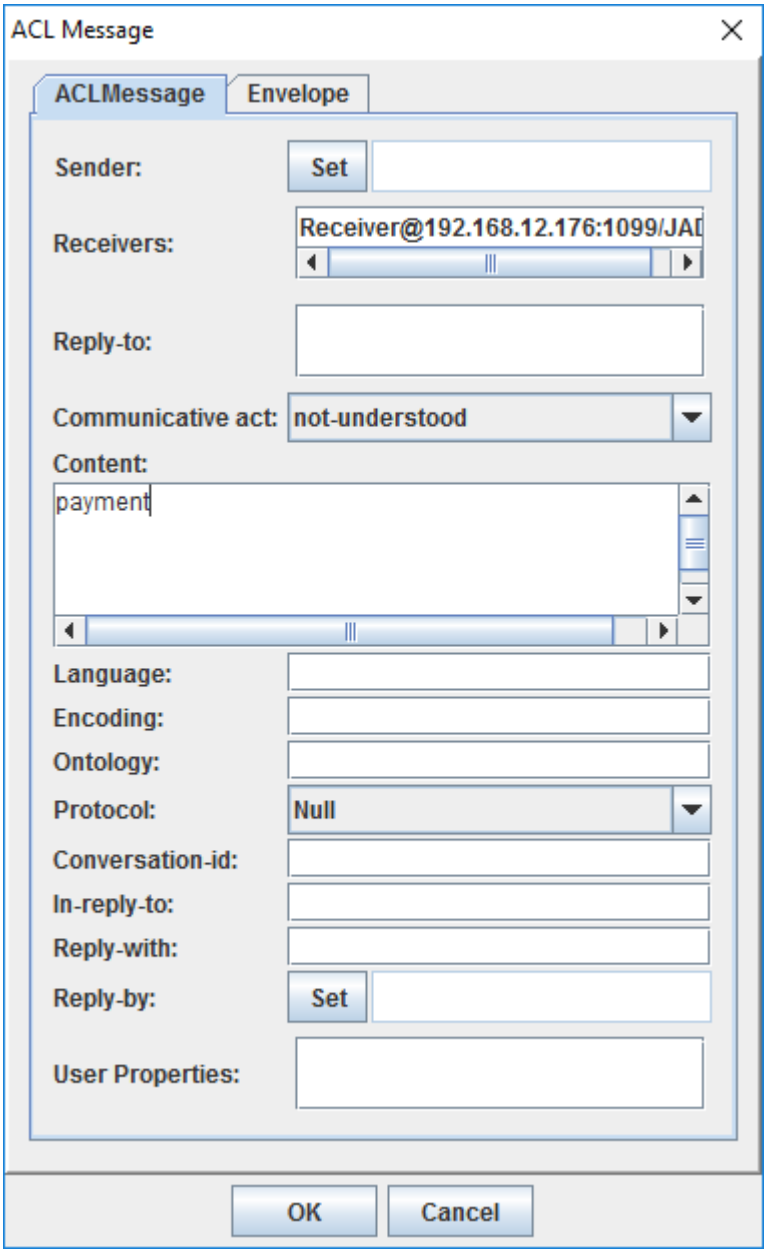


Figure 5-9: Agent message to trigger Invoicing Agent

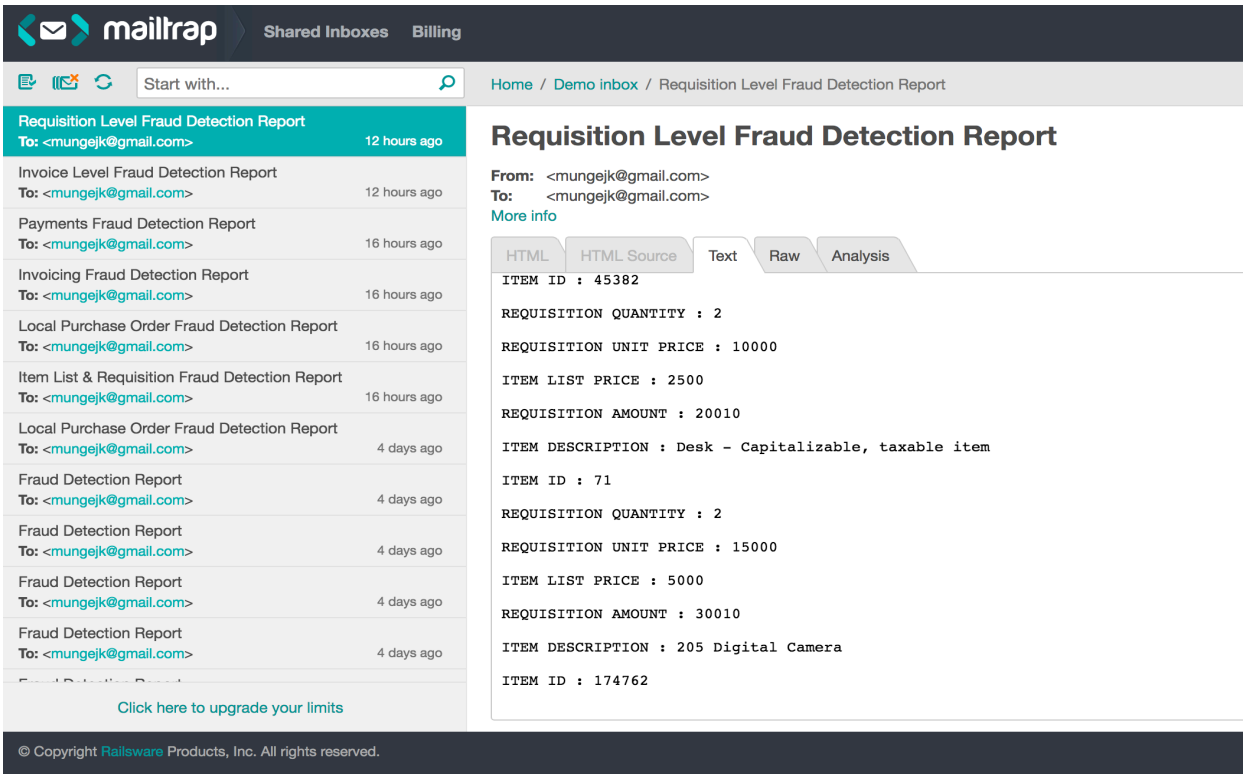


Figure 5-10: Email sent by mailer agent to notify on fraud at requisition level

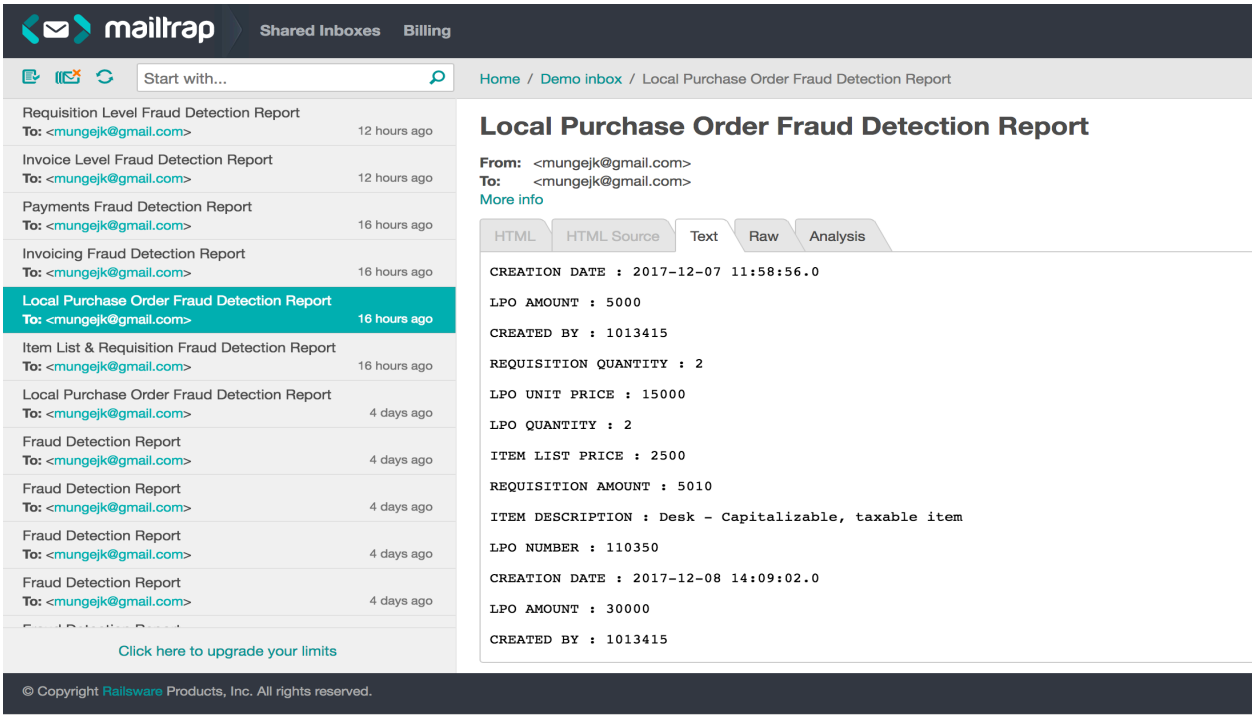


Figure 5-11: Email sent by mailer agent to notify on fraud at LPO level

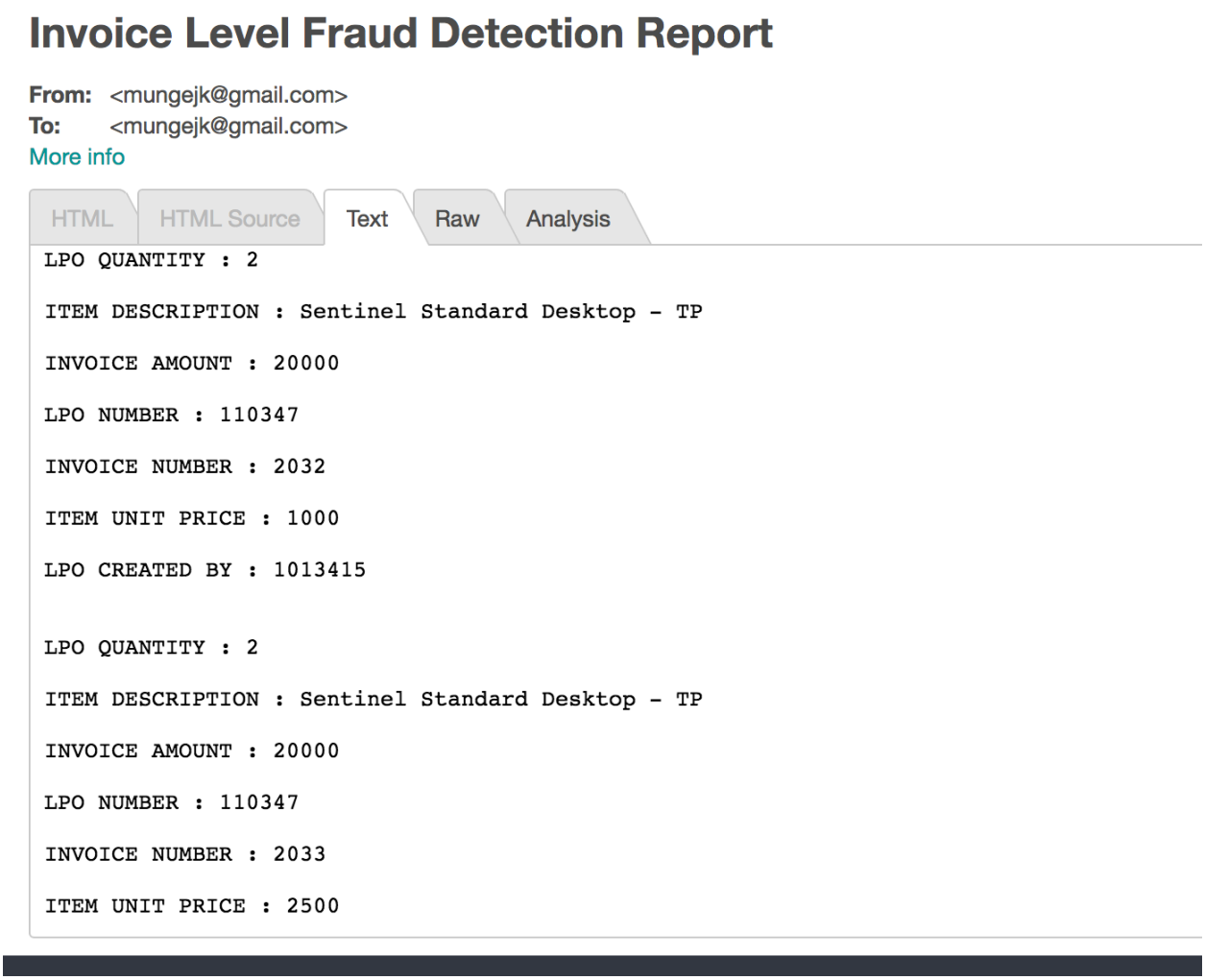


Figure 5-12: Email sent by mailer agent to notify on fraud at invoicing level

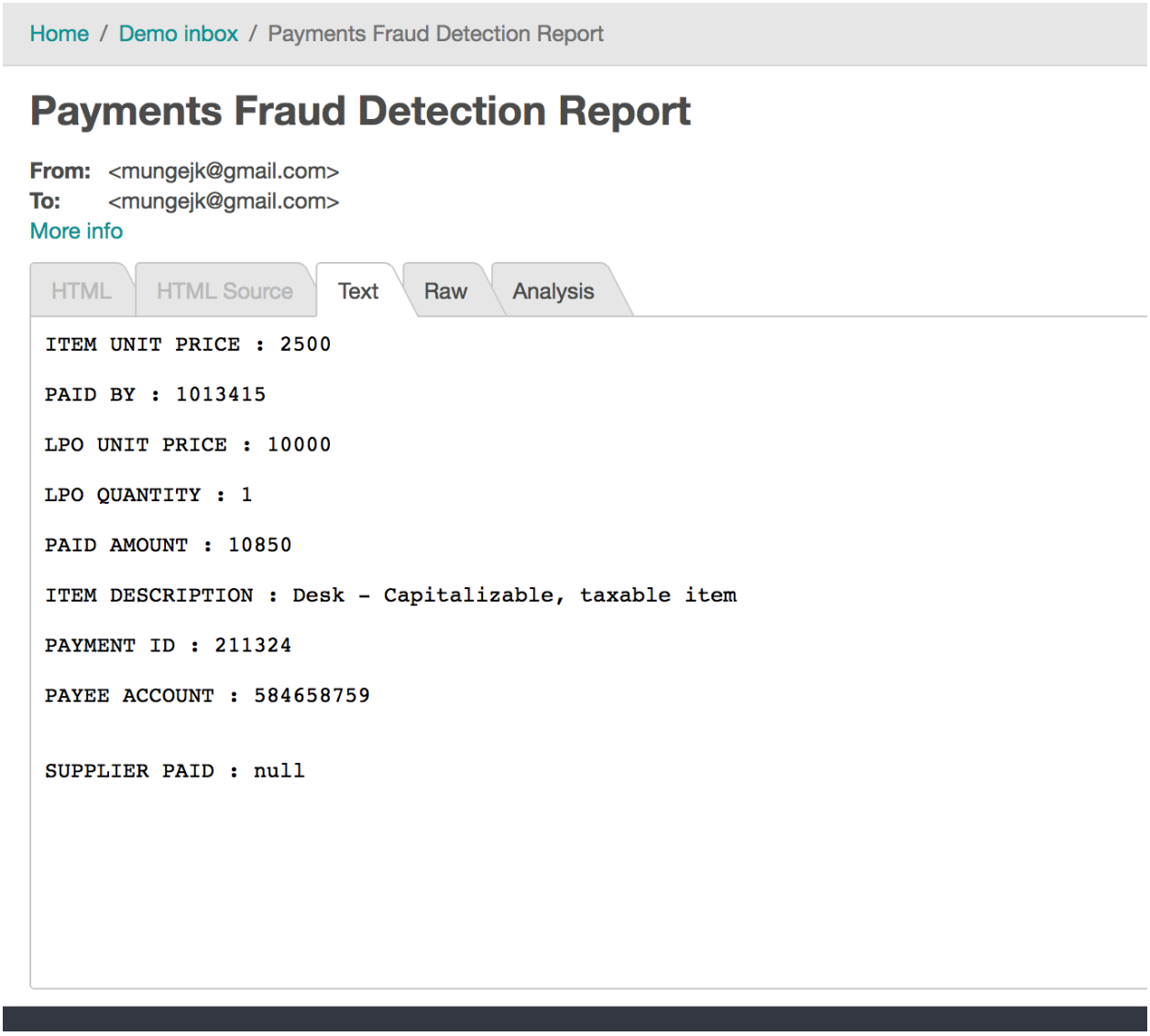


Figure 5-13: Email sent by mailer agent to notify on fraud at payment level

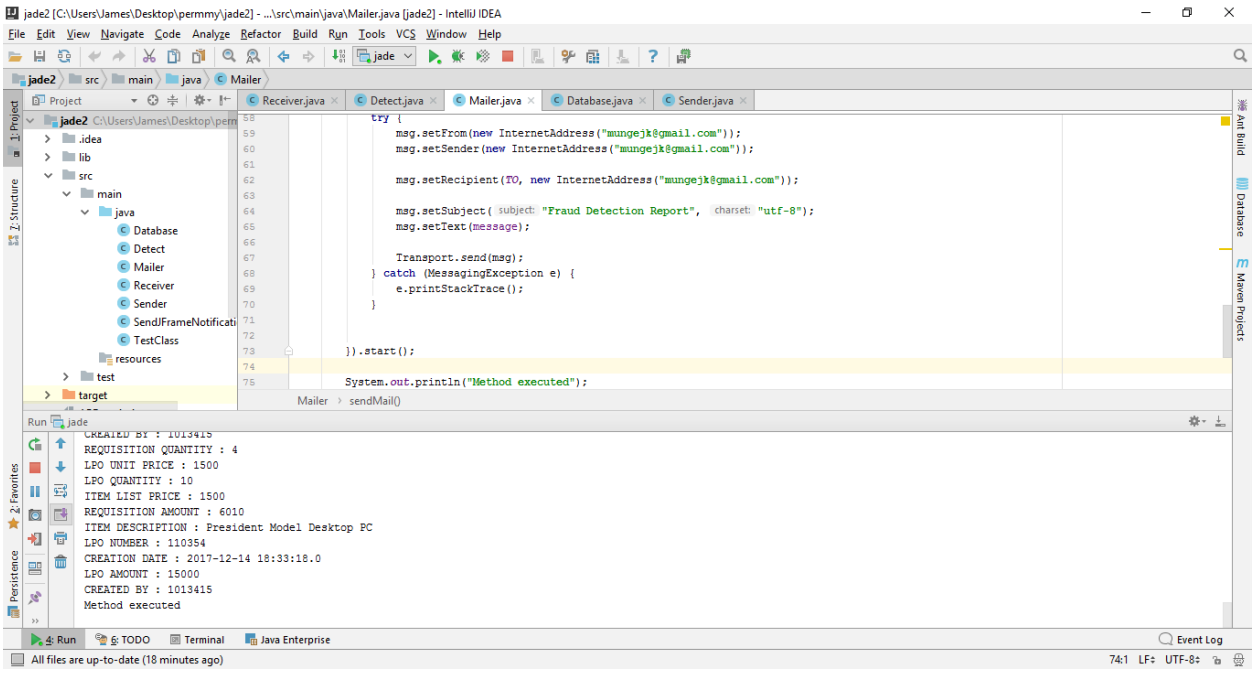


Figure 5-14: Data displayed by Agent from the e-Procurement system

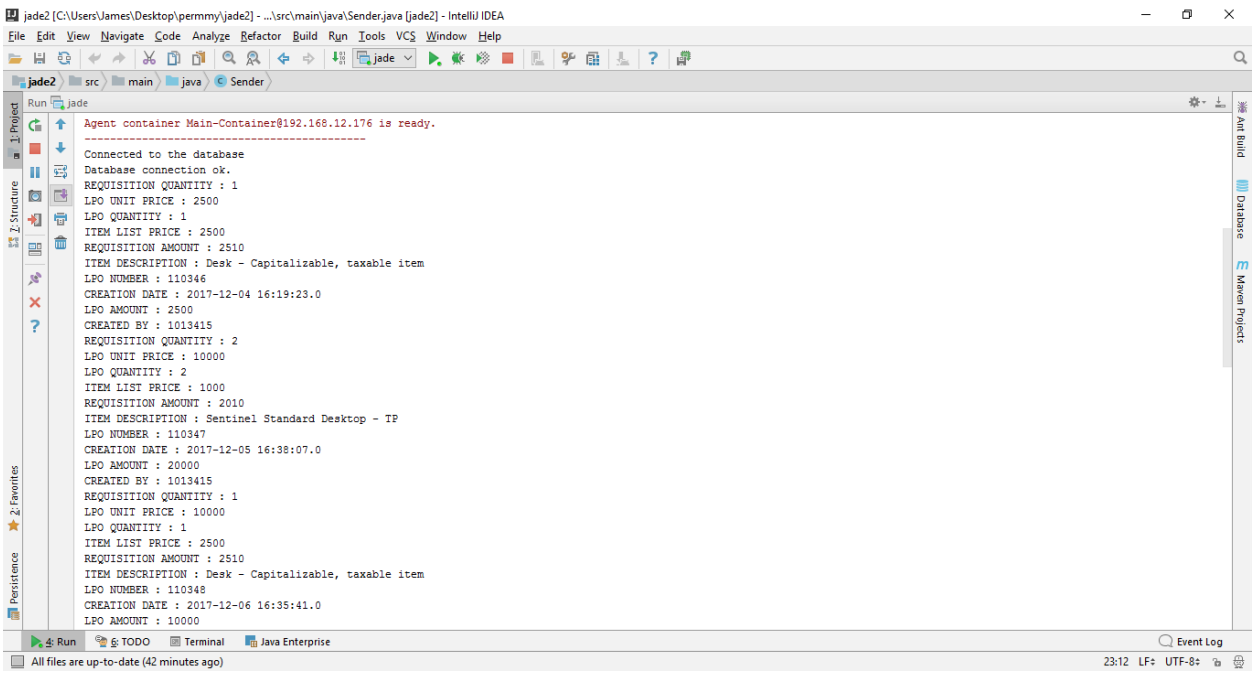


Figure 5-15: Data displayed by Agent from the e-Procurement system

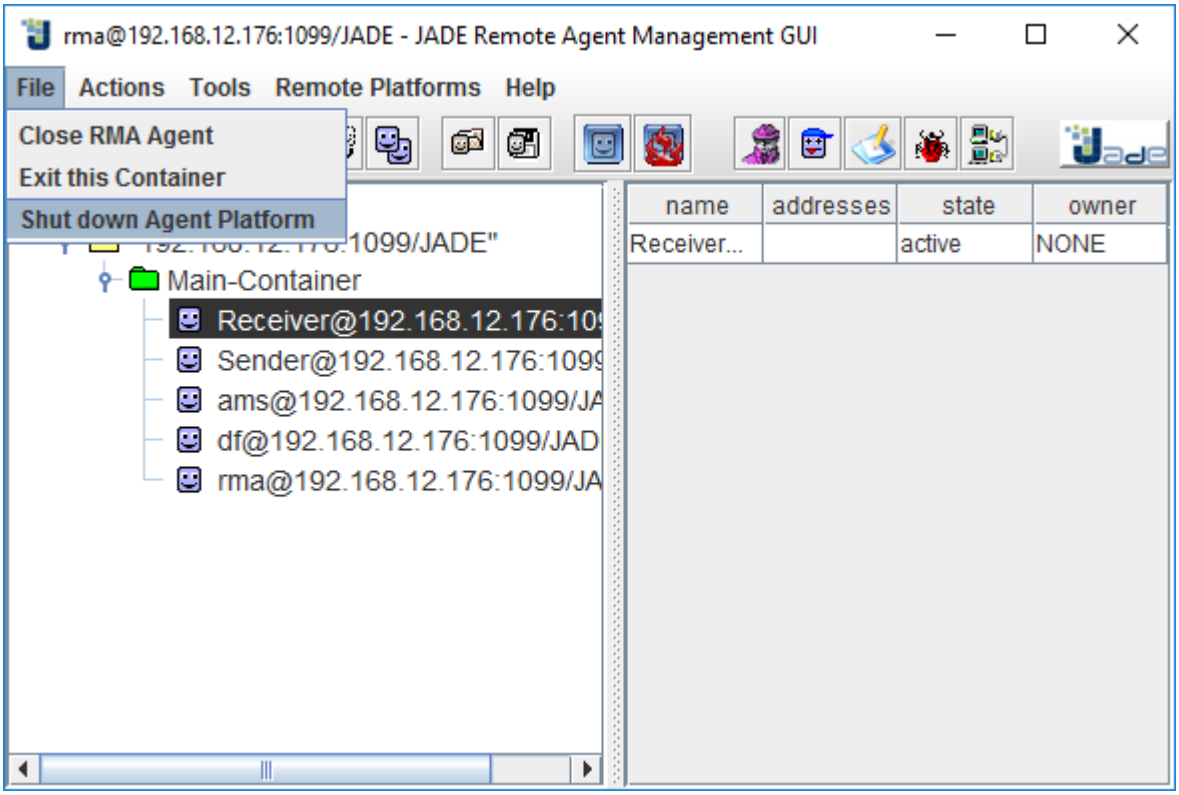


Figure 5-16: Terminating Jade Agent Communication Platform

5.4 Evaluation of results

User survey Questionnaire on the use of fraud detection tool

Question 1	I understand what e-procurement is	
	Response	**Number of Respondents**
	Strongly Agree	12
	Agree	8
	Uncertain/not applicable	0
	Disagree	0
	Strongly disagree	0
Question 2	I have used IFMIS to procure goods/services	
	Response	**Number of Respondents**
	Strongly Agree	12
	Agree	5
	Uncertain/not applicable	0
	Disagree	3
	Strongly disagree	0
Question 3	I have heard of fraud in e-procurement	
	Response	**Number of Respondents**
	Strongly Agree	18
	Agree	2
	Uncertain/not applicable	0
	Disagree	0
	Strongly disagree	0

Question 4	It is possible to eradicate fraud in e-procurement	
	Response	**Number of Respondents**
	Strongly Agree	5
	Agree	10
	Uncertain/not applicable	3
	Disagree	2
	Strongly disagree	0
Question 5	IFMIS is a secure system	
	Response	**Number of Respondents**
	Strongly Agree	2
	Agree	6
	Uncertain/not applicable	4
	Disagree	5
	Strongly disagree	3
Question 6	Procurement in government is fully automated	
	Response	**Number of Respondents**
	Strongly Agree	0
	Agree	5
	Uncertain/not applicable	1
	Disagree	14
	Strongly disagree	0
Question 7.	Is the fraud detection agent easy to use?	
	Response	**Number of Respondents**

	Yes	8
	No	12
Question 8.	Was the fraud detection agent able to detect fraud at requisition level in the e-procurement system?	
	Response	**Number of Respondents**
	Yes	20
	No	0
Question 9.	Was the fraud detection agent able to detect fraud at Purchasing Order level in the e-procurement system?	
	Response	**Number of Respondents**
	Yes	20
	No	0
Question 10.	Was the fraud detection agent able to detect fraud at Invoicing level in the e-procurement system?	
	Response	**Number of Respondents**
	Yes	20
	No	0
Question 11.	Was the fraud detection agent able to detect fraud after payment of suppliers in the e-procurement system?	
	Response	**Number of Respondents**
	Yes	20
	No	0

Question 12.	Do you think this system can help eradicate fraud in public e-procurement?	
	Response	**Number of Respondents**
	Yes	20
	No	0
Question 13.	Would you recommend such a system to your department/ministry?	
	Response	**Number of Respondents**
	Yes	20
	No	0

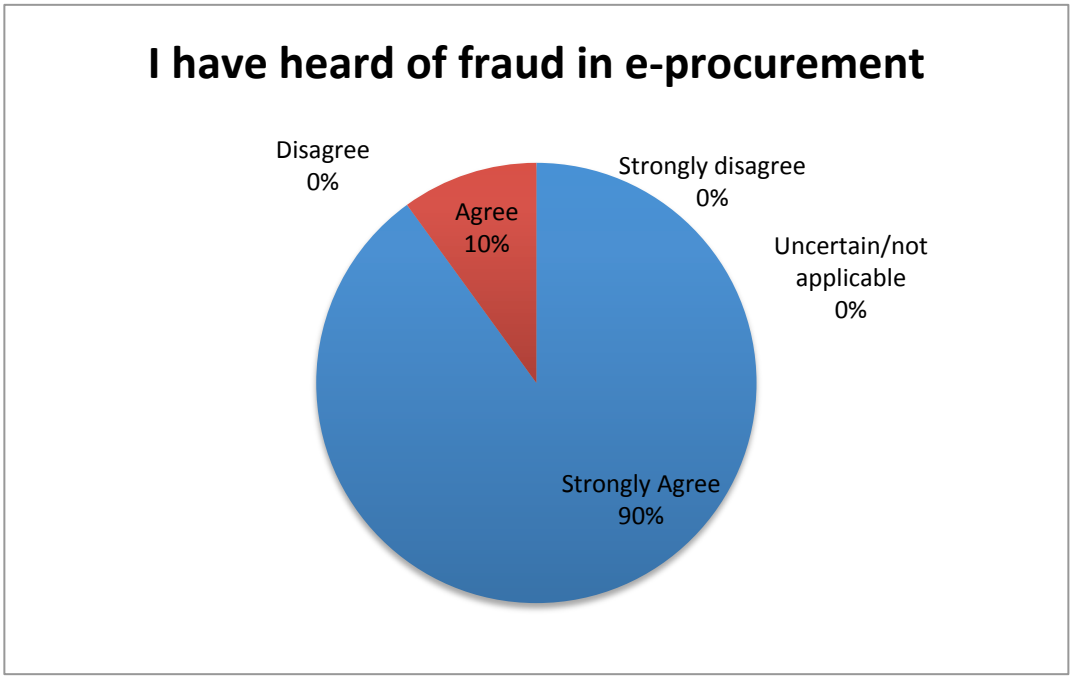


Figure 5-17: Questionnaire response on fraud awareness

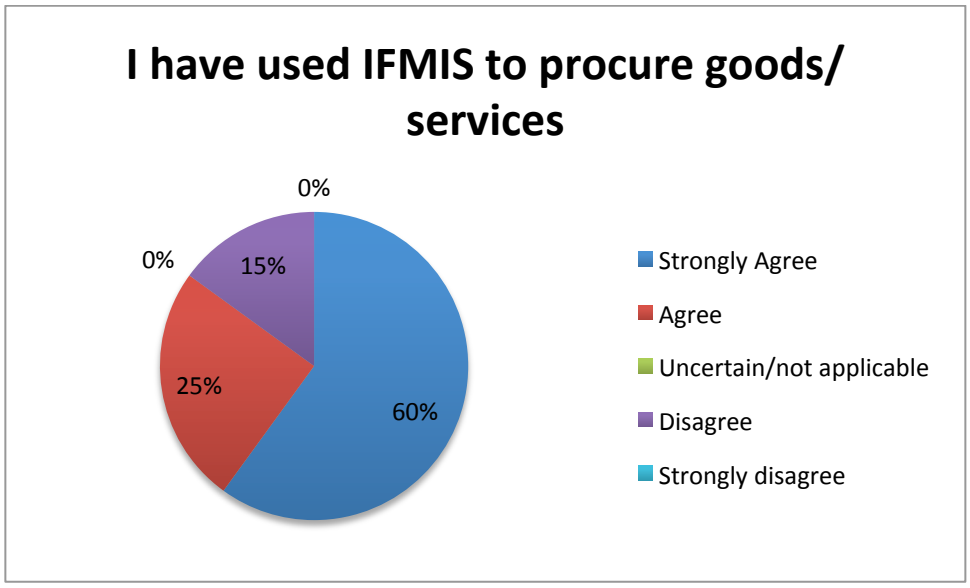


Figure 5-18: Questionnaire response on respondent having used IFMIS before

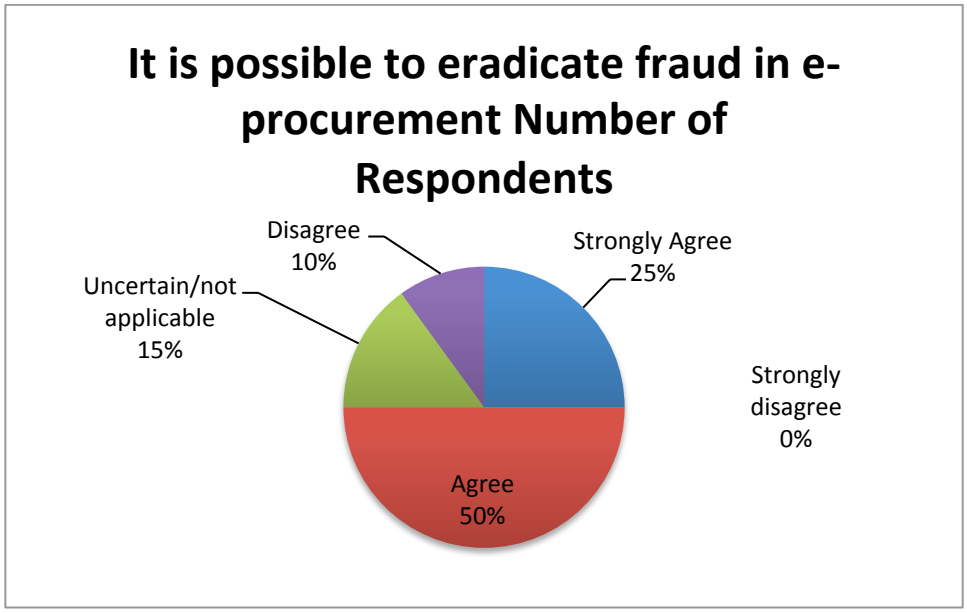


Figure 5-19: Questionnaire response on fraud eradication in e-procurement

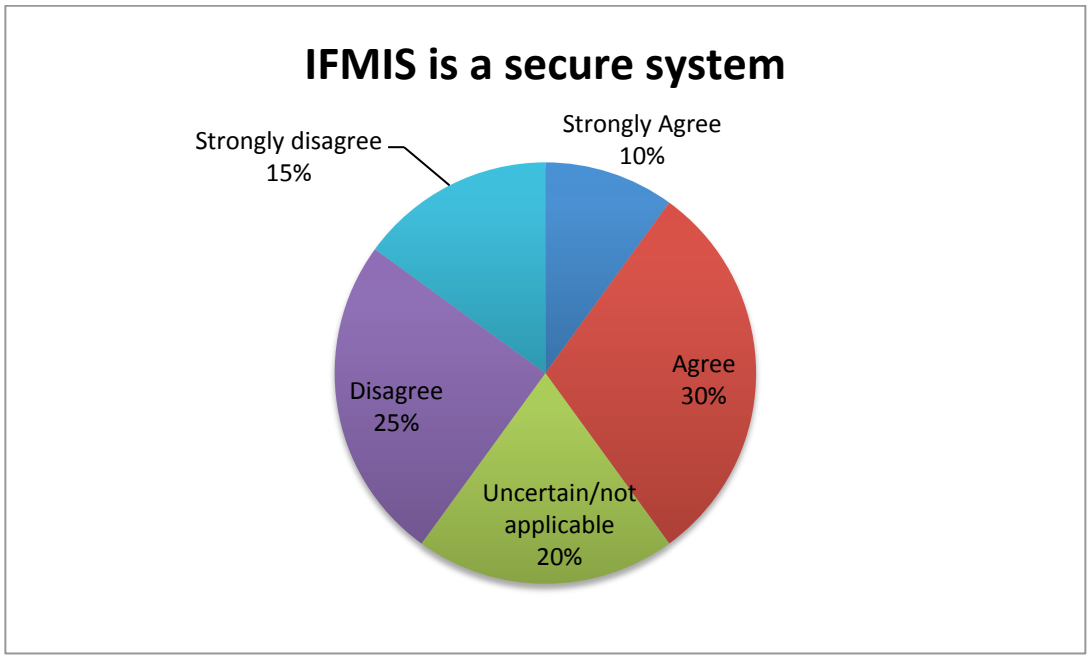


Figure 5-20: Questionnaire response on security of e-procurement system

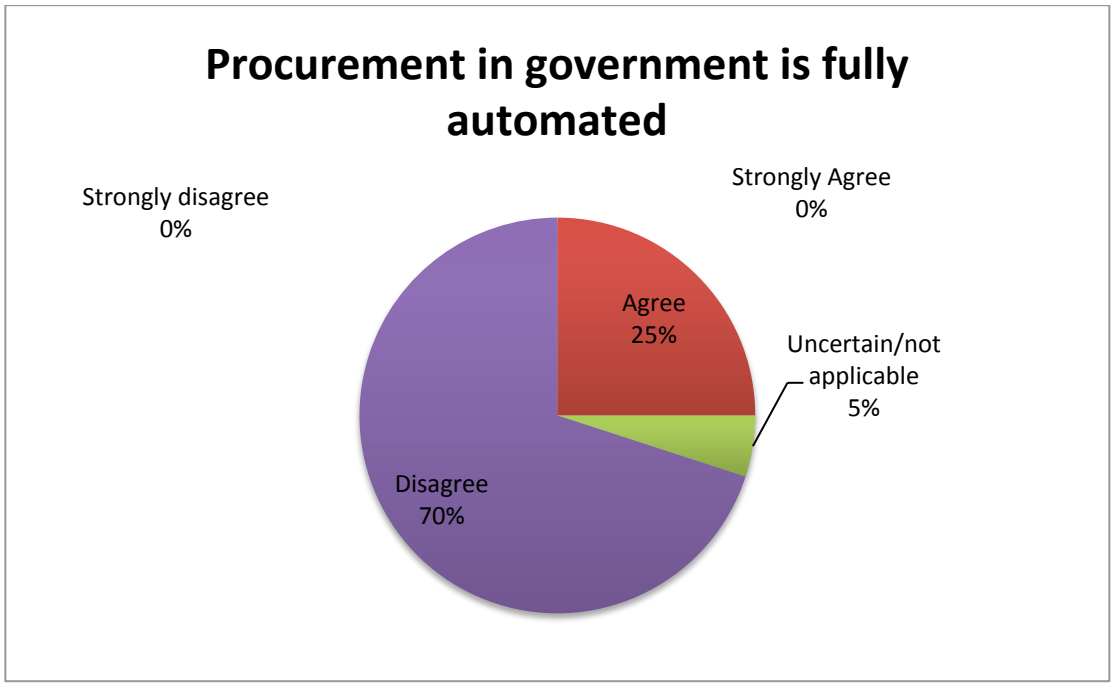


Figure 5-21: Questionnaire response on the use of e-procurement

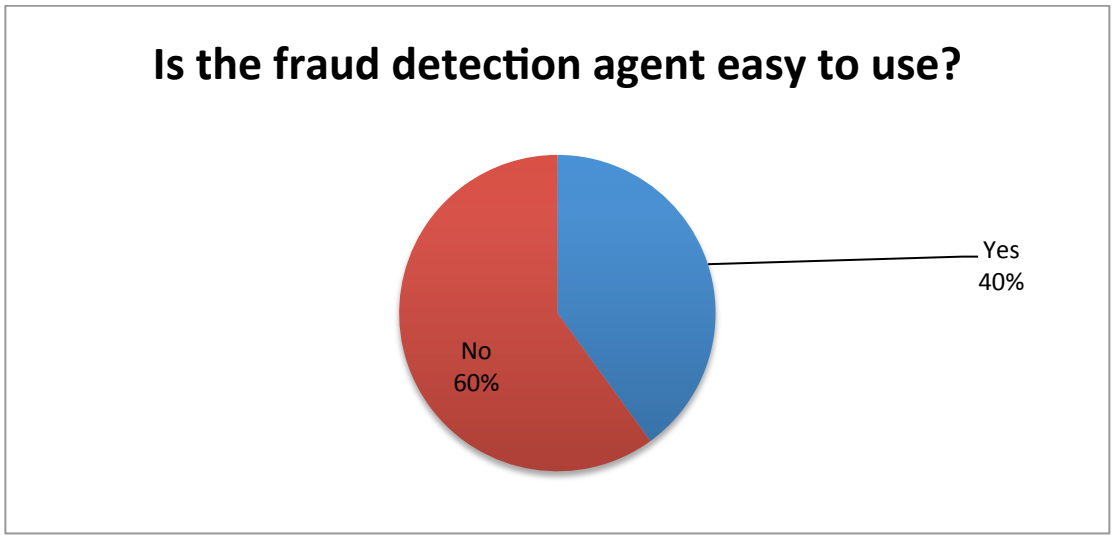


Figure 5-22: Questionnaire response on the ease of use of the agent detection tool

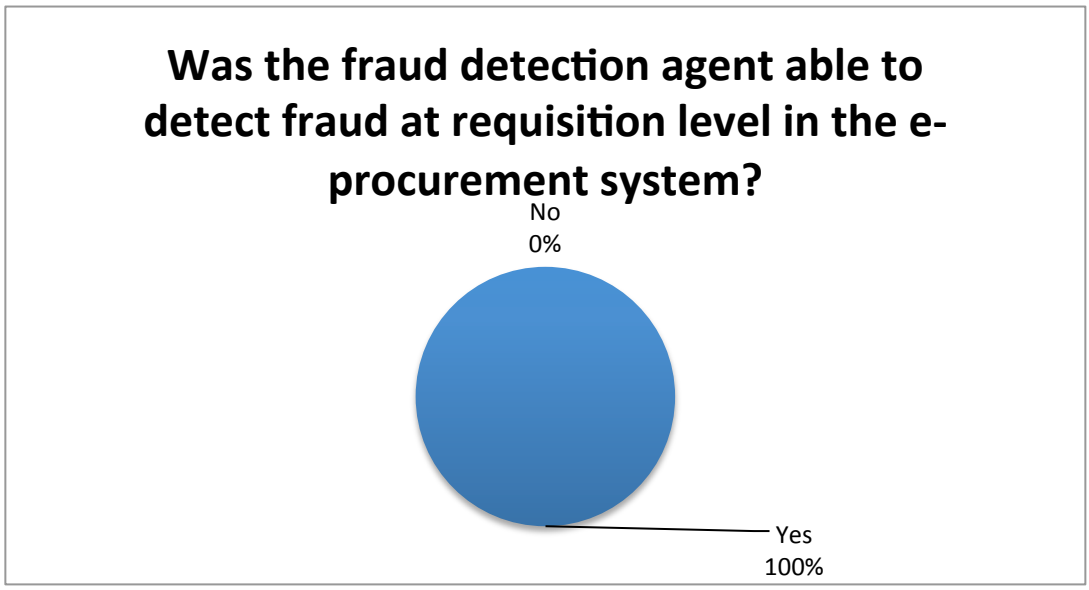


Figure 5-23: Questionnaire response on agent fraud detection at requisition level

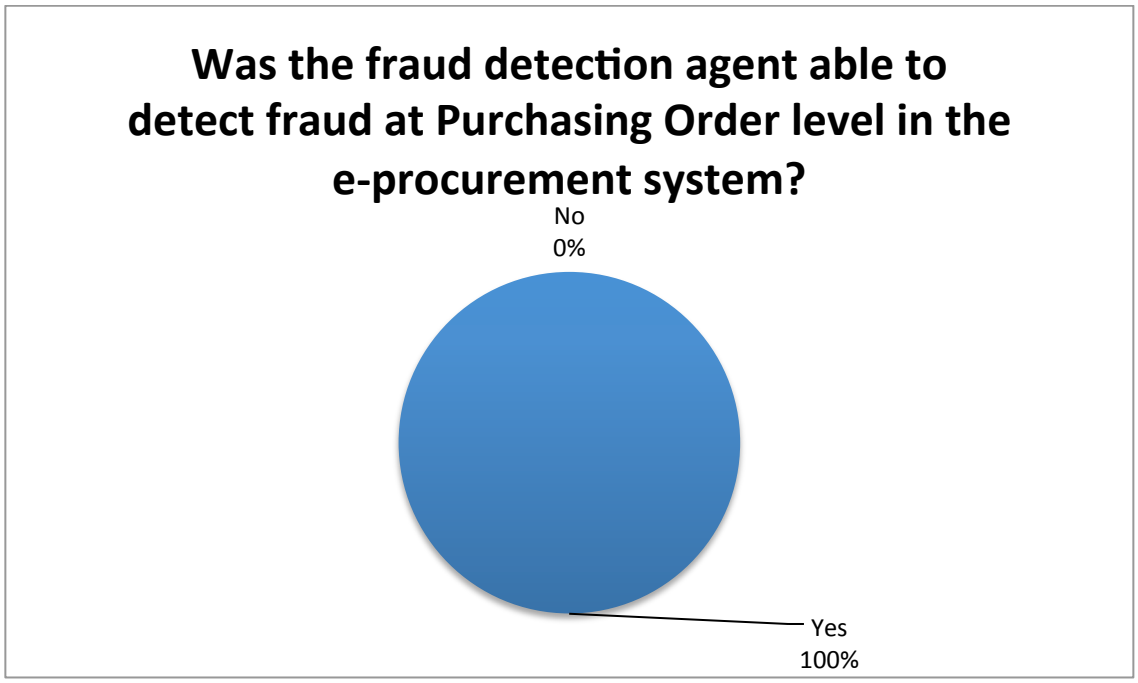


Figure 5-24: Questionnaire response on agent fraud detection at purchase order level

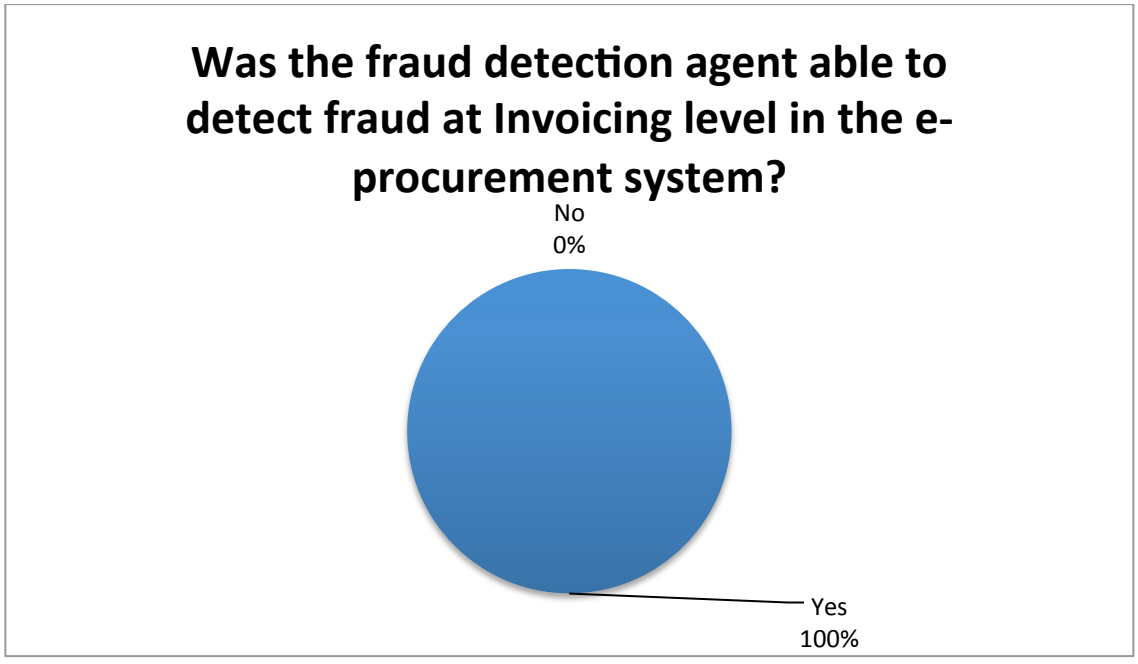


Figure 5-25: Questionnaire response on agent fraud detection at invoicing level

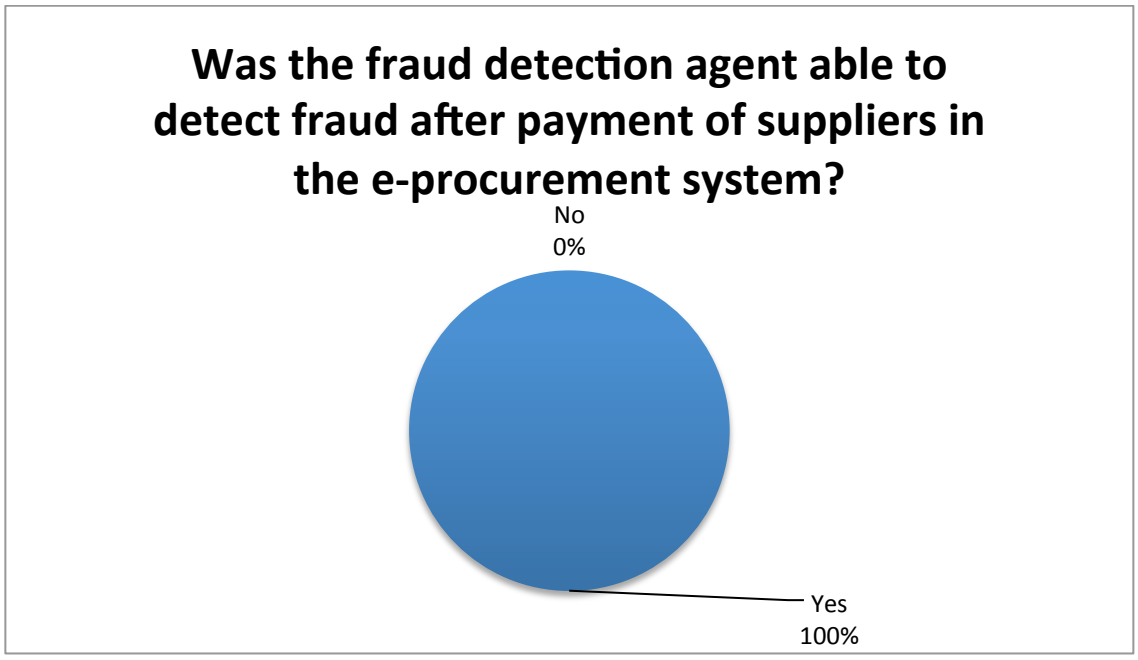


Figure 5-26: Questionnaire response on agent fraud detection at payment level

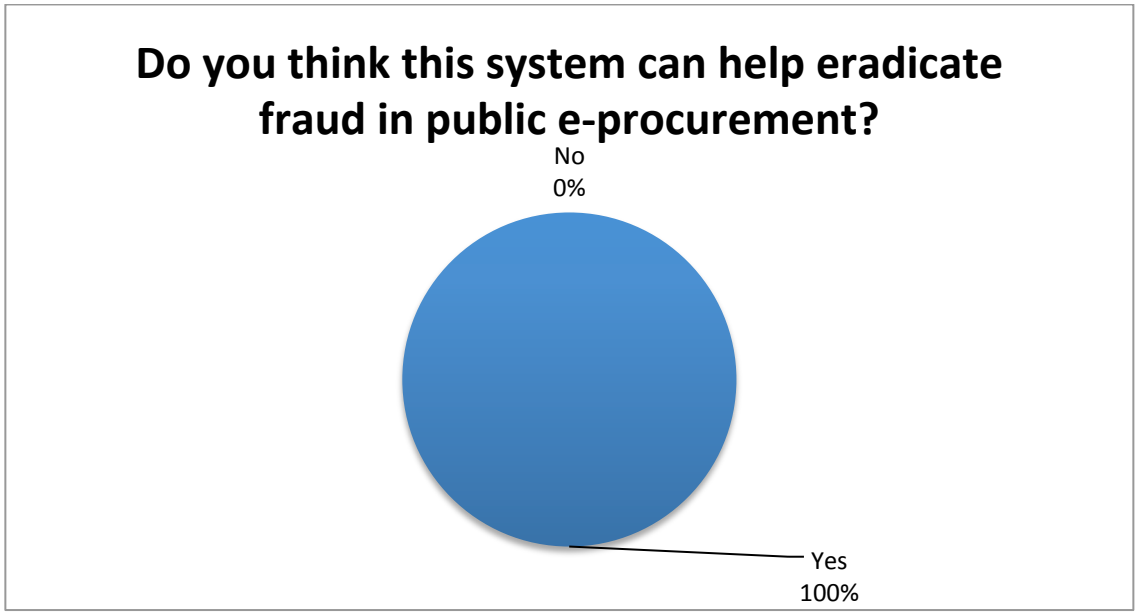


Figure 5-27: Questionnaire response on role of agents in fraud detection.

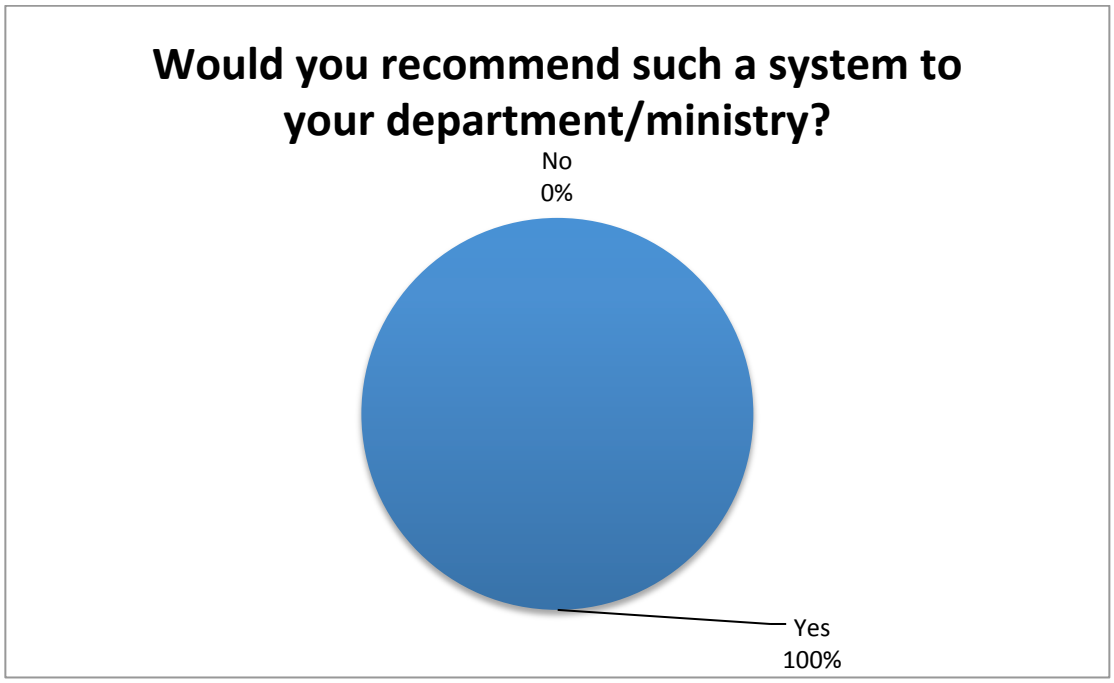


Figure 5-28: Questionnaire response on whether respondents would recommend use of agents for fraud detection and reporting in their places of work.

Chapter Six:

6 Conclusion and Recommendations

6.1 Achievements

The objective of this research project was to develop an agent prototype that can demonstrate that agents can proactively be used to detect and report fraud in public e-procurement systems. This was to a large extent achieved.

The possible fraud avenues in public e-procurement systems were identified using research tools such as questionnaires, observation, interviews and literature review. It was noted that inflation of unit cost of items at requisition level and further upward adjustments could be done while raising purchase orders. Upward adjustment of quantities can also be done after requisition approval by raising a differing higher figure on purchase orders. This however requires approvals from the various approval levels(approvers) who may be compromised or fail to take note of the discrepancies. The proceeds from such fraud may be paid to the participants in the procurement chain as kickbacks (bribes).

A simulated e-procurement prototype was developed and the entire procure to pay process conducted on the test data generated during the design phase. The critical phases that were captured are: Requisition level, Purchase order level, Receiving of goods/services level, Invoicing level and Payment of goods/services level.

The fraud agent prototype was finally designed and deployed to identify the fraudulent entries that had been captured on the e-procurement system. The agent was able to scan through the e-procurement database and pick out all entries that had significant variance from the base price or approved quantities at requisition level. Where the agent was able to detect fraud a report was sent to an email address to serve as notification to authorities who should take immediate action to stop the fraud or recover the lost money.

The success of any fraud detection agent depends to a large extent on a proper definition of rules that determine a suspicious event.

6.2 Research contributions

This research focused on a proactive fraud detection mechanism. It demonstrates that agent based technology can be used to detect and stop fraud/corruption in public entities thereby deriving maximum value for taxpayers money.

Agent based Fraud detection using multi agent technology is event driven and therefore as transactions takes place on the e-procurement system the agents perform checks against a set of set rules to determine suspicious actions that could amount to fraud.

This research project will assist the government (both national and county governments) to tackle the issue of corruption in a manner that goes beyond the deployment of ICT to automate processes. With the help of agents, it is possible to detect and report fraud cases at various levels of the procurement process even before money is lost.

A measure of integrity can also be drawn from the number of fraud cases reported on a particular individual.

6.3 Recommendations for future work

The system can be improved further in the following ways:

· Addition of intelligent agents that can validate suppliers by checking their actual existence against company databases held by the registrar of societies.

· Adaptation of the fraud detection system so as to use databases that are not SQL based but rather graph based database

Design an agent that does not require user input to activate thereby providing continuous check

for fraud.

6.4 Limitations

One limitation of this fraud detection system is that it is prompted/activated by a user and requires a valid user login and password to access a database and conduct checks.

The fraud detection agent can only notify on a case of possible fraud but cannot stop the transaction from going on. A human user has to take action in order to stop or reverse the fraudulent transaction. If the notified person ignores an alert the fraud will still occur despite being detected in good time.

The agent based fraud detection system is based on SQL command to relational databases or object relational databases. If the e-procurement system runs on a database that does not support SQL query language then fraud detection will not work.

Where public procurement processes are not fully automated or where there is a hybrid implementation of electronic processes and manual processes it would be difficult to detect all cases of fraud owing to absence of important database variables and system variables that agents can track.

6.5 Assumptions

It is assumed that public e-procurement is deployed on systems that can store audit trails of system e-procurement activities and that those variables will be available for scrutiny to fraud detection agents.

References

Abdalla, Cirne etal (1997). Security Issues in Agent Based Computing. University of California San Diego, Department of Computer Science and Engineering.

Achmad Nurmandi (2013). Status of Indonesian e-procurement: Journal of government & Politics vol4. No2.

ADB (2004), Inter American Development Bank. World Bank. Strategic Electronic Government Procurement – Strategic Overview: An Introduction for Executives, Asian Development Bank, available at: www.unpcdc.org/../strategic%20electronic%20government%20p rocurement.pdf (accessed February 2011).

Aman, A. & Kasimin, H(2011). E-procurement implementation: a case of Malaysia government. Transforming Government: People, Process and Policy, 5, 330-344

Amanda, L. M. (1998). Corruption: Causes, consequences, and policy implications. The Asia Foundation Working Paper #9.

Angeles, R. and Nath, R. (2007). "Business-to-business e-procurement: success factors and challenges to implementation", Supply Chain Management: An International Journal, Vol. 12, pp. 104-15.

Auditor General (2015). Summary of the Report of the auditor-general on the financial statements for national government for the year 2014/2015.

Bertot, J. C., Jaeger, P. T. & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. Government Information Quarterly, 27, 264-271.

Casaki, C. and Gelleri, P. (2005). "Conditions and benefits of applying decision technological solutions as a tool to curb corruption within the procurement process: the case of Hungary", Journal of Purchasing and Supply Management, Vol. 11 Nos 5/6, pp. 252-259.

Chopra, S., Dougan, D. and Gareth, T. (2001). "B2B e-commerce opportunity", Supply Chain Management Review, Vol. 5 No. 3, pp. 50-62.

Croom, S. (2000). "The impact of web-based procurement on the management of operating resources supply", Journal of Supply Chain Management, Vol. 36 No. 1, pp. 4-13

Dag Johansen, Robert van Renesse, and Fred Scheidner (1995). Operating system support for mobile agents. In Proceedings of the 5th IEEE Workshop on Hot Topics in Operating Systems. http://cstr.cs.cornell.edu/TR/CORNELLCS:TR94-1468.

Dag Johansen, Robert van Renesse, and Fred Scheidner (1995). An Introduction to the TACOMA Distributed System: Version 1.0. Technical Report 95-23, Department of Computer Science, University of Tromsø. http://www.cs.uit.no/Lokalt/Rapporter/Reports/ 9523.html.

Daily Nation (2016). Govt audits online procurement system to cut fraud: http://www.nation.co.ke/business/Govt-audits-online-procurement-system-to-cut-fraud/996-3060438-yjlss2/index.html

Davila, A., Gupta, M. and Palmer, R. (2003). "Moving procurement systems to the internet: the adoption and use of e-procurement technology models", European Management Journal, Vol. 21 No. 1, pp. 11-23.

Dike, V. E. (2005). Corruption in Nigeria: A new paradigm for effective control. Africa Economic Analysis. Accessed September 21, 2011, from http://www.africaeconomicanalysis.org/articles/gen/-corruptiondikehtm.html.

Hardy, C.A. and Williams, S.P. (2008). "E-government policy and practice: a theoretical and empirical exploration of public e-procurement", Government Information Quarterly, Vol. 25 No. 2, pp. 155-180.

Harris, R. and Rajora, R. (2006). Information and Communication Technologies for E-governance and Poverty Reduction – A Study of Rural Development Project in India, UNDP-APDIP, Regional Centre, Bangkok, available at:

www.apdip.net/publications/ict4d/empoweringthepoor.pdf.

Hellman, J. S., Geraint, J., & Kaufmann, D. (2000). Seize the state, seize the day. State capture, corruption, and influence in transition. World Bank, Policy Research Working Paper, No. 2444. Washington, DC: World Bank, 2000. Presented in the ABCDE 2000 Conference, Washington, DC, April 18–20, 2000.

Heywood, J.B. (2002). E-procurement: Managing Successful E-procurement Implementation, Financial Times, Prentice-Hall, Harlow.

Holmes, D. (2001). eGov: eBusiness Strategies for Government, Nicholas Brealey, London.

Hui, W.S., Othman, R., Omar, N.H., Rahman, R.A. and Haron, N.H. (2011). "Procurement issues in Malaysia", International Journal of Public Sector Management, Vol. 24 No. 6, pp. 567-593.

Iqbal, M.S. and Seo, J.W. (2008). "E-government as an anti-corruption tool: Korean cases", Journal of Korean Association for Regional Information Society, Vol. 11 No. 2, pp. 51-78.

Jon Hayton (2000). Procurement Fraud in E-business: Dispute analysis and investigation by Price WaterHouse Coopers

KinnyD, Georgeff M, Rao A (1996). A Methodology and modelling technique for systems of BDI agents; Australian Artificial Intelligence Institute.

Krastev, I. (2004). Shifting obsessions: Three essays on the politics of anticorruption (p. 33). Budapest: Central European University Press.

Malela Akinyi (2010). E-Procurement Model for the Public Sector of Kenya; University of Nairobi.

Kennedy, K.N. and Deeter-Schmelz, D.R. (2001). "Descriptive and predictive analyses of industrial buyer's use of online information for purchasing", Journal of Personal Selling

& Sales Management, Vol. 21 No. 4, pp. 279-290.

Kenya Gazette supplement no. 207 (2015). "The Public procurement and asset disposal act, 2015."

Mccue, C. & Roman, A. V. (2012). E-Procurement: Myth Or Reality? Journal of Public Procurement, 12, 221-248

NAO (2014). Transforming government's contract management. In: Office, N. A. (ed.). Cabinet Office: National Audit Office 2014.

Oye, N.D (January 2003). Reducing corruption in African Developing Countries: The Relevance of E-governance. Greener Journal of Social Sciences.

Padhi, S.S. and Mohapatra, P.K.J. (2011). "Detection of collusion in government procurement auctions", Journal of Purchasing and Supply Management, Vol. 17 No. 4, pp. 207-221.

PPOA (March 2009). Corruption Prevention Guidelines in Public Procurement (March 2009). Public Procurement Oversight Authority and Kenya Anti Corruption Commission.

Rabl, T., & Kuhlmann, T. M. (2009). Why or why not? Rationalizing corruption in organizations. Cross Cultural Management: An International Journal, 16(3), 268–286.

Rai, A., Tang, X., Brown, P. and Keil, M. (2006). "Assimilation patterns in the use of electronic procurement innovations: a cluster analysis", Information and Management, Vol. 43 No. 3, pp. 336-349.

Roman, A. V. (2013). Public Policy And Financial Management Through E-Procurement: A Practice Oriented Normative Model For Maximizing Transformative Impacts. Journal Of Public Procurement, 13, 337-363.

Rotchanakitumnuai, S. (2012a). "Critical governance concerns of Thailand e-government procurement", paper presented at International Conference on Information Resources Management 2012 (Conf-IRM-2012), Vienna, Austria, May 21-23.

Rotchanakitumnuai, S. (2012b). “The empirical evidences of good governance in E-government procurement”, paper presented at The 18th Americas Conference on Information Systems, Seattle, WA, USA, August 9-11.

Sı´k, E. (2002). The bad, the worse and the worst: Guesstimating the level of corruption. In S. Kotkin & A. Sajo´ (Eds.), Political corruption in transition: A sceptic’s handbook (pp. 91–113). Budapest: Central European University Press.

Siriluck Rotchanakitumnuai, (2013). "The governance evidence of e-government procurement", Transforming Government: People, Process and Policy, Vol. 7 Iss 3 pp. 309 – 321.

Smart, A. (2010). “Exploring the business case for e-procurement”, International Journal of Physical Distribution & Logistics Management, Vol. 40 No. 3, pp. 181-201.

Sofia Wickberg (March 2013). Technological innovations to identify and reduce corruption. www.u4.no/publications/technological-innovations-to-identify-and-reduce-corruption.

Stewart Robinson (2004). Simulation: The Practice of Model Development and Use.

Tatsis, V., Mena, C., Van Wassenhove, L. and Whicker, L. (2006). “E-procurement in the Greek food and drink industry: drivers and impediments”, Journal of Purchasing & Supply Management, Vol. 12, pp. 63-74.

Ware, G. T., & Noone, G. P. (2003). The culture of corruption in the post conflict and developing world. In A. Chayes & M. Minnow(Eds.), Imagine coexistence: Restoring humanity after violent ethnic conflict. San Francisco, CA: Jossey-Bass.

Warsta, M. (2004). Corruption in Thailand, International Management: Asia, Swiss Federal Institute of Technology, Zurich, April 22, available at: http://aceproject.org/ero-en/ regions/asia/TH/Corruption_in_Thailand.pdf (accessed November 2012).

Wooldridge M, Ciancarini P, (2000). Agent-Oriented Software Engineering: The State of the art. Department of Computer Science, University of Liverpool.

World Bank Institute and EBRD. (2000). Business environment and enterprise performance survey. http://info.worldbank.org/governance/beeps/.

Yusoff, W. S., Islam, M. A., Abas, Z. & Yusuf, D. H. (2010). Electronic government procurement adoption behavior amongst Malaysian SMEs. International Business Research, 4, 100-111.

Appendix A: Questionnaire

User Survey Questionnaire on the use of Fraud Detection Tool

Ministry:	
Designation:	

Please complete the following questionnaire with specific regard to the above enquiry, by placing a CROSS (X) in the appropriate box

		strongly agree	agree	not	disagree	strongly disagree
1.	I understand what e-procurement is.	☐	☐	☐	☐	☐
2.	I have used IFMIS to procure goods/services	☐	☐	☐	☐	☐
3.	I have heard of fraud in e-procurement	☐	☐	☐	☐	☐
4.	It is possible to eradicate fraud in e-procurement	☐	☐	☐	☐	☐
5.	IFMIS is a secure system	☐	☐	☐	☐	☐
6.	Procurement in government is fully automated	☐	☐	☐	☐	☐

Is the fraud detection agent easy to use

☐ Yes ☐ No

Was the fraud detection agent able to detect fraud at Requisition level in the e-procurement system?

☐ Yes ☐ No

Was the fraud detection agent able to detect fraud at Purchasing Order level in the e-procurement system?

☐ Yes ☐ No

Was the fraud detection agent able to detect fraud at Invoicing level in the e-procurement system?

☐ Yes ☐ No

Was the fraud detection agent able to detect fraud after payment of suppliers in the e-procurement system?

☐ Yes ☐ No

Do you think this system can help eradicate fraud in public e-procurement?

☐ Yes ☐ No

Would you recommend such a system to your department/ministry?

☐ Yes ☐ No

How would you improve this tool?

Suggest:

Appendix B: Fraud agent programming code

RECEIVER.JAVA CODE

```
import jade.core.Agent;
import jade.core.behaviours.CyclicBehaviour;
import jade.lang.acl.ACLMessage;

import javax.swing.*;

public class Receiver extends Agent {
   ACLMessage msg = null;
   Detect detect=new Detect();
   SendJFrameNotification jFrameNotification=new SendJFrameNotification();

   @Override
   protected void setup() {
      addBehaviour(new CyclicBehaviour() {
         @Override
         public void action() {

            //Receive a message from the sender
            msg = receive();

            if (msg != null) {
               String decrMsg = msg.getContent().toLowerCase();

               if (decrMsg.equals("lpo")) {
                  detect.retrievePoInformation();

               } else if (decrMsg.equals("requisition")) {
                  detect.checkItemListAndRequisition();

               } else if (decrMsg.equals("invoice")) {
```

```
                detect.checkInvoice();

            } else if (decrMsg.equals("payment")) {
                detect.checkPayment();

            } else if (decrMsg.equals("start")) {
                jFrameNotification.sendMsg("Welcome to fraud detection system");

            } else {
                jFrameNotification.sendMsg("Please ask for instructions to use the agent");
            }

        } else

        {

            block();

        }

    }


});

  }
}
```

SENDER.JAVA CODE

```
import jade.core.AID;
import jade.core.Agent;
import jade.core.behaviours.OneShotBehaviour;
import jade.lang.acl.ACLMessage;

public class Sender extends Agent {
   @Override
   protected void setup() {
      //super.setup();


      addBehaviour(new OneShotBehaviour() {
         @Override
         public void action() {

            ACLMessage msg=new ACLMessage(ACLMessage.INFORM);
            msg.setContent("Start");
            msg.addReceiver(new AID("Receiver",AID.ISLOCALNAME));
            send(msg);

         }

      });
   }
}
```

AGENT DETECT CODE

```
import jade.core.Agent;

import java.sql.Connection;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.sql.Statement;
import java.util.ArrayList;
import java.util.HashMap;
import java.util.Map;

public class Detect extends Agent {

    Database database = new Database();
    SendJFrameNotification jFrameNotification = new SendJFrameNotification();
    private Boolean notifyFraud=false;
    ArrayList<Integer> list=new ArrayList<Integer>();

    Boolean denouceFraud=false;

    /*Retrieve purchase order information ---2*/
    public void retrievePoInformation()
    {
        Connection connection = database.connectDatabase();
        Mailer mailer=new Mailer();
        StringBuffer data=new StringBuffer();
        StringBuffer fraudData=new StringBuffer();
        //String message="";
        HashMap<String,String> message=new HashMap<>();
        HashMap<String,String> fraud=new HashMap<>();
        if (database != null) {
            System.out.println("Database connection ok.");
```

```
        try {
            Statement statement = connection.createStatement();
            ResultSet resultSet=statement.executeQuery("SELECT PO.ITEM_DESCRIPTION
AS PO_ITEM_DESC, PO.QUANTITY AS PO_QUANTITY, PO.PO_HEADER_ID AS
PO_NUMBER,\n" +
                    "PO.UNIT_PRICE AS PO_UNIT_PRICE, PO.LIST_PRICE_PER_UNIT
AS PO_LIST_PRICE_PER_UNIT, PO.CREATION_DATE AS
PO_CREATION_DATE,\n" +
                    "PO.CREATED_BY AS PO_CREATED_BY, PRLA.QUANTITY AS
PRLA_QUANITY, PRLA.ITEM_DESCRIPTION AS
PRLA_ITEM_DESCRIPTION,PRLA.UNIT_PRICE AS PRLA_UNIT_PRICE,\n" +
                    "PRLA.CREATION_DATE AS PRLA_CREATION_DATE,
PRLA.CREATED_BY AS PRLA_CREATED_BY\n" +
                    "FROM PO_LINES_ALL PO\n" +
                    "INNER JOIN PO_DISTRIBUTIONS_ALL PDA ON
PO.PO_HEADER_ID=PDA.PO_HEADER_ID\n" +
                    "INNER JOIN PO_REQ_DISTRIBUTIONS_ALL PRDA ON
PDA.REQ_DISTRIBUTION_ID=PRDA.DISTRIBUTION_ID\n" +
                    "INNER JOIN PO_REQUISITION_LINES_ALL PRLA ON
PRDA.REQUISITION_LINE_ID=PRLA.REQUISITION_LINE_ID\n" +
                    "WHERE PRLA.REQUISITION_HEADER_ID>=181210");

            while (resultSet.next()) {
                /*LPO DETAILS*/
                int quantityLpo = resultSet.getInt("PO_QUANTITY");
                int unitPriceLpo= resultSet.getInt("PO_UNIT_PRICE");
                int amountLpo=quantityLpo*unitPriceLpo;

                /*LPO REQUISITION*/
                int quantityRequisition = resultSet.getInt("PRLA_QUANITY");
                int unitPriceRequisition= resultSet.getInt("PO_LIST_PRICE_PER_UNIT");
                int amountRequisition=(quantityRequisition*unitPriceRequisition);
```

```
            String creationDateRequisition=
resultSet.getString("PRLA_CREATION_DATE");
            String createdByRequisition= resultSet.getString("PRLA_CREATED_BY");

            String itemDescLpo= resultSet.getString("PO_ITEM_DESC");
            String creationDateLpo= resultSet.getString("PO_CREATION_DATE");
            String createdByLpo= resultSet.getString("PO_CREATED_BY");
            String lpoNumber= resultSet.getString("PO_NUMBER");

            double maxAmount=(amountRequisition*1.2);


            if(amountLpo > maxAmount || quantityRequisition != quantityLpo)
            {
               list.add(1);
               fraud=new HashMap<>();

               fraud.put("LPO NUMBER :" ,lpoNumber);
               fraud.put("ITEM DESCRIPTION :" ,itemDescLpo);
               fraud.put("LPO QUANTITY :" , String.valueOf(quantityLpo));
               fraud.put("LPO UNIT PRICE :" , String.valueOf(unitPriceLpo));
               fraud.put("LPO AMOUNT :" , String.valueOf(amountLpo));
               fraud.put("CREATED BY :" , String.valueOf(createdByLpo));
               fraud.put("CREATION DATE :" , String.valueOf(creationDateLpo));
               fraud.put("ITEM LIST PRICE :" , String.valueOf(unitPriceRequisition));
               fraud.put("REQUISITION QUANTITY :" ,
String.valueOf(quantityRequisition));
               fraud.put("REQUISITION AMOUNT :" ,
String.valueOf(amountRequisition+'\n'));

               for (Map.Entry f:fraud.entrySet())
               {
```

```
                String fraudmsg=f.getKey()+" "+f.getValue();
                fraudData.append(fraudmsg+'\n'+'\r');
                // mailer.sendMail(msg);
               // System.out.println(m.getKey()+" "+m.getValue());
            }

        }

        message=new HashMap<>();

        message.put("LPO NUMBER :" ,lpoNumber);
        message.put("ITEM DESCRIPTION :" ,itemDescLpo);
        message.put("LPO QUANTITY :" , String.valueOf(quantityLpo));
        message.put("LPO UNIT PRICE :" , String.valueOf(unitPriceLpo));
        message.put("LPO AMOUNT :" , String.valueOf(amountLpo));
        message.put("CREATED BY :" , String.valueOf(createdByLpo));
        message.put("CREATION DATE :" , String.valueOf(creationDateLpo));
        message.put("ITEM LIST PRICE :" , String.valueOf(unitPriceRequisition));
        message.put("REQUISITION QUANTITY :" ,
String.valueOf(quantityRequisition));
        message.put("REQUISITION AMOUNT :" ,
String.valueOf(amountRequisition+'\n'));

        for (Map.Entry m:message.entrySet())
        {
          String msg=m.getKey()+" "+m.getValue();
          data.append(msg).append('\n').append('\r');
          // mailer.sendMail(msg);
           System.out.println(m.getKey()+" "+m.getValue());
        }

    }
    connection.close();
```

```
            if (!list.isEmpty())
            {
              // notificationFraud();
               jFrameNotification.sendMsg("Fraud Detected! Check email for details");
               mailer.sendMail(String.valueOf(fraudData),"Local Purchase Order");
               list.clear();
               System.out.println(list.isEmpty());
            }else
            {
               denouncedFraud();
            }

        } catch (SQLException e) {
           e.printStackTrace();
        }

    } else {
       System.out.println("Could not connect to the database");
    }

}

public void checkItemListAndRequisition()
{
    Connection connection = database.connectDatabase();
    Mailer mailer=new Mailer();
    StringBuffer data=new StringBuffer();
    StringBuffer fraudData=new StringBuffer();
    //String message="";
    HashMap<String,String> message=new HashMap<>();
    HashMap<String,String> fraud=new HashMap<>();
    if (database != null) {
```

```
        System.out.println("Database connection ok.");

        try {
            Statement statement = connection.createStatement();
            ResultSet resultSet=statement.executeQuery("SELECT
MSIF.INVENTORY_ITEM_ID AS MSIF_INVENTORY_ITEM_ID,
MSIF.DESCRIPTION AS MSIF_DESCRIPTION, MSIF.LIST_PRICE_PER_UNIT AS
MSIF_LIST_PRICE_PER_UNIT,\n" +
                    "  PRLA.QUANTITY AS PRLA_QUANTITY, PRLA.UNIT_PRICE AS
PRLA_UNIT_PRICE, PRLA.CREATION_DATE AS PRLA_CREATION_DATE,
PRLA.CREATED_BY AS PRLA_CREATED_BY\n" +
                    "FROM MTL_SYSTEM_ITEMS_FVL MSIF\n" +
                    "  INNER JOIN PO_REQUISITION_LINES_ALL PRLA ON
MSIF.INVENTORY_ITEM_ID=PRLA.ITEM_ID\n" +
                    "WHERE PRLA.REQUISITION_LINE_ID>=208418 AND
MSIF.ORGANIZATION_ID=204");

            while (resultSet.next()) {

                /*REQUISITION TABLE*/
                int quantityRequisition = resultSet.getInt("PRLA_QUANTITY");
                int unitPriceRequisition= resultSet.getInt("PRLA_UNIT_PRICE");
                String requisitionCreationDate=
resultSet.getString("PRLA_CREATION_DATE");
                String requisitionCreatedBy= resultSet.getString("PRLA_CREATED_BY");
                int amountRequisition=quantityRequisition*unitPriceRequisition;

                /*ITEM LIST TABLE*/
                int itemListPricePerUnit=resultSet.getInt("MSIF_LIST_PRICE_PER_UNIT");
                String inventoryId= resultSet.getString("MSIF_INVENTORY_ITEM_ID");
                String itemDescription= resultSet.getString("MSIF_DESCRIPTION");

                double maxReqPrice=(itemListPricePerUnit*1.2);
```

```
            if(unitPriceRequisition > maxReqPrice)
            {
               list.add(1);
               fraud=new HashMap<>();

               fraud.put("ITEM ID :" ,inventoryId);
               fraud.put("ITEM DESCRIPTION :" ,itemDescription);
               fraud.put("ITEM LIST PRICE :" , String.valueOf(itemListPricePerUnit));
               fraud.put("REQUISITION QUANTITY :" ,
String.valueOf(quantityRequisition));
               fraud.put("REQUISITION UNIT PRICE :" ,
String.valueOf(unitPriceRequisition));
               fraud.put("REQUISITION AMOUNT :" ,
String.valueOf(amountRequisition+'\n'));


               for (Map.Entry f:fraud.entrySet())
               {
                  String fraudmsg=f.getKey()+" "+f.getValue();
                  fraudData.append(fraudmsg+'\n'+'\r');
                  // mailer.sendMail(msg);
                  // System.out.println(m.getKey()+" "+m.getValue());
               }
            }

            message=new HashMap<>();

            message.put("ITEM ID :" ,inventoryId);
            message.put("ITEM DESCRIPTION :" ,itemDescription);
            message.put("ITEM LIST PRICE :" , String.valueOf(itemListPricePerUnit));
            message.put("REQUISITION QUANTITY :" ,
String.valueOf(quantityRequisition));
            message.put("REQUISITION UNIT PRICE :" ,
```

```
String.valueOf(unitPriceRequisition));
                message.put("REQUISITION AMOUNT :" ,
String.valueOf(amountRequisition+'\n'));

                for (Map.Entry m:message.entrySet())
                {
                   String msg=m.getKey()+" "+m.getValue();
                   data.append(msg+'\n'+'\r');
                   // mailer.sendMail(msg);
                   System.out.println(m.getKey()+" "+m.getValue());
                }

            }
            connection.close();

            if (!list.isEmpty())
            {
               //notificationFraud();
               jFrameNotification.sendMsg("Fraud Detected! Check email for details");
               mailer.sendMail(String.valueOf(fraudData),"Requisition Level ");
               list.clear();
               System.out.println(list.isEmpty());
            }else
            {
               denouncedFraud();
            }


        } catch (SQLException e) {
           e.printStackTrace();
        }

    } else {
```

```
            System.out.println("Could not connect to the database");
        }
    }

    public void checkInvoice()
    {
        Connection connection = database.connectDatabase();
        Mailer mailer=new Mailer();
        StringBuffer data=new StringBuffer();
        StringBuffer fraudData=new StringBuffer();
        //String message="";
        HashMap<String,String> message=new HashMap<>();
        HashMap<String,String> fraud=new HashMap<>();
        if (database != null) {
            System.out.println("Database connection ok.");

            try {
                Statement statement = connection.createStatement();
                ResultSet resultSet=statement.executeQuery("SELECT
AIA.QUICK_PO_HEADER_ID AS AIA_QUICK_PO_HEADER_ID,
AIA.INVOICE_NUM AS AIA_INVOICE_NUM, AIA.INVOICE_AMOUNT AS
AIA_INVOICE_AMOUNT, PLA.PO_HEADER_ID AS PLA_PO_HEADER_ID,
PLA.ITEM_DESCRIPTION AS PLA_ITEM_DESCRIPTION, PLA.UNIT_PRICE AS
PLA_UNIT_PRICE, PLA.QUANTITY AS PLA_QUANTITY,
PLA.LIST_PRICE_PER_UNIT AS PLA_LIST_PRICE_PER_UNIT, PLA.CREATED_BY
AS PLA_CREATED_BY, PLA.CREATION_DATE AS PLA_CREATION_DATE\n" +
                        "FROM AP_INVOICES_ALL AIA\n" +
                        "INNER JOIN PO_LINES_ALL PLA ON
AIA.QUICK_PO_HEADER_ID=PLA.PO_HEADER_ID\n" +
                        "WHERE AIA.QUICK_PO_HEADER_ID>=110339");

                while (resultSet.next()) {
```

```
/*INVOICE TABLE*/
int invoiceAmount = resultSet.getInt("AIA_INVOICE_AMOUNT");
int invoiceNumber= resultSet.getInt("AIA_INVOICE_NUM");
String lpoNumber= resultSet.getString("PLA_PO_HEADER_ID");
String itemDescription= resultSet.getString("PLA_ITEM_DESCRIPTION");
int lpoQuantity= resultSet.getInt("PLA_QUANTITY");
String lpoUnitPrice= resultSet.getString("PLA_UNIT_PRICE");
String lpoCreatedBy= resultSet.getString("PLA_CREATED_BY");
int lpoListPrice= resultSet.getInt("PLA_LIST_PRICE_PER_UNIT");


double maxReqPrice=(lpoListPrice*lpoQuantity)*1.2;
//double invoiceAmountX=(lpoUnitPrice*lpoQuantity);
if(invoiceAmount > maxReqPrice)
{
   list.add(1);
   fraud=new HashMap<>();

  fraud.put("LPO NUMBER :" ,lpoNumber);
  fraud.put("INVOICE NUMBER :" ,String.valueOf(invoiceNumber));
  fraud.put("ITEM DESCRIPTION :" ,String.valueOf(itemDescription));
  fraud.put("LPO QUANTITY :" , String.valueOf(lpoQuantity));
  fraud.put("INVOICE AMOUNT :" , String.valueOf(invoiceAmount));
  fraud.put("ITEM UNIT PRICE :" , String.valueOf(lpoListPrice));
  fraud.put("LPO CREATED BY :" , String.valueOf(lpoCreatedBy+'\n'));

   for (Map.Entry f:fraud.entrySet())
   {
      String fraudmsg=f.getKey()+" "+f.getValue();
      fraudData.append(fraudmsg+'\n'+'\r');
      // mailer.sendMail(msg);
      // System.out.println(m.getKey()+" "+m.getValue());
   }
```

```
    }

    message=new HashMap<>();

    message.put("LPO NUMBER :" ,lpoNumber);
    message.put("INVOICE NUMBER :" ,String.valueOf(invoiceNumber));
    message.put("ITEM DESCRIPTION :" ,String.valueOf(itemDescription));
    message.put("LPO QUANTITY :" , String.valueOf(lpoQuantity));
    message.put("INVOICE AMOUNT :" , String.valueOf(invoiceAmount));
    message.put("ITEM UNIT PRICE :" , String.valueOf(lpoListPrice));
    message.put("LPO CREATED BY :" , String.valueOf(lpoCreatedBy+'\n'));

    for (Map.Entry m:message.entrySet())
    {
       String msg=m.getKey()+" "+m.getValue();
       data.append(msg+'\n'+'\r');
       // mailer.sendMail(msg);
       System.out.println(m.getKey()+" "+m.getValue());
    }

}
connection.close();

if (!list.isEmpty())
{
  // notificationFraud();
   jFrameNotification.sendMsg("Fraud Detected! Check email for details");
   mailer.sendMail(String.valueOf(fraudData),"Invoicing ");
   list.clear();
   System.out.println(list.isEmpty());
}else
{
   denouncedFraud();
```

```
            }


        } catch (SQLException e) {
            e.printStackTrace();
        }

    } else {
        System.out.println("Could not connect to the database");
    }
}

    public void checkPayment()
    {
        Connection connection = database.connectDatabase();
        Mailer mailer=new Mailer();
        StringBuffer data=new StringBuffer();
        StringBuffer fraudData=new StringBuffer();
        //String message="";
        HashMap<String,String> message=new HashMap<>();
        HashMap<String,String> fraud=new HashMap<>();
        if (database != null) {
            System.out.println("Database connection ok.");


            try {
                Statement statement = connection.createStatement();
                ResultSet resultSet=statement.executeQuery("SELECT AIPA.INVOICE_ID AS
AIPA_INVOICE_ID, AIPA.AMOUNT AS AIPA_INVOICE_AMOUNT,
AIPA.CREATED_BY AS AIPA_CREATED_BY, AIPA.CREATION_DATE AS
AIPA_CREATION_DATE, AIPA.BANK_ACCOUNT_NUM AS
AIPA_BANK_ACCOUNT_NUM,\n" +
                        "AIPA.REMIT_TO_SUPPLIER_NAME AS
AIPA_REMIT_TO_SUPPLIER_NAME, AIA.INVOICE_ID AS AIA_INVOICE_ID,
```

```
PLA.PO_HEADER_ID AS PLA_PO_HEADER_ID, PLA.ITEM_DESCRIPTION AS
PLA_ITEM_DESCRIPTION, PLA.UNIT_PRICE AS PLA_UNIT_PRICE,\n" +
                "PLA.QUANTITY AS PLA_QUANTITY, PLA.LIST_PRICE_PER_UNIT
AS PLA_LIST_PRICE_PER_UNIT\n" +
                "FROM AP_INVOICE_PAYMENTS_ALL AIPA\n" +
                "INNER JOIN AP_INVOICES_ALL AIA ON
AIPA.INVOICE_ID=AIA.INVOICE_ID\n" +
                "INNER JOIN PO_LINES_ALL PLA ON
AIA.QUICK_PO_HEADER_ID=PLA.PO_HEADER_ID\n" +
                "WHERE AIA.INVOICE_ID>=211301");

            while (resultSet.next()) {

                /*PAYMENT TABLE*/
                int paymentAmount = resultSet.getInt("AIPA_INVOICE_AMOUNT");
                int lpoQuantity= resultSet.getInt("PLA_QUANTITY");
                int lpoListPrice= resultSet.getInt("PLA_LIST_PRICE_PER_UNIT");
                String paymentInvoiceId= resultSet.getString("AIPA_INVOICE_ID");
                String itemDescription= resultSet.getString("PLA_ITEM_DESCRIPTION");
                String paymentCreatedBy= resultSet.getString("AIPA_CREATED_BY");
                String lpoUnitPrice= resultSet.getString("PLA_UNIT_PRICE");
                String paymentSupplierName=
resultSet.getString("AIPA_REMIT_TO_SUPPLIER_NAME");
                String paymentBankAccountNumber=
resultSet.getString("AIPA_BANK_ACCOUNT_NUM");


                double maxReqPrice=(lpoQuantity*lpoListPrice*1.2);
                if (paymentAmount > maxReqPrice)
                {
                   list.add(1);

                   fraud=new HashMap<>();
```

```
                fraud.put("PAYMENT ID :" ,paymentInvoiceId);
                fraud.put("ITEM DESCRIPTION :" ,String.valueOf(itemDescription));
                fraud.put("LPO QUANTITY :" , String.valueOf(lpoQuantity));
                fraud.put("LPO UNIT PRICE :" ,String.valueOf(lpoUnitPrice));
                fraud.put("PAID AMOUNT :" , String.valueOf(paymentAmount));
                fraud.put("ITEM UNIT PRICE :" , String.valueOf(lpoListPrice));
                fraud.put("PAID BY :" , String.valueOf(paymentCreatedBy));
                fraud.put("SUPPLIER PAID :" , String.valueOf(paymentSupplierName));
                fraud.put("PAYEE ACCOUNT :" ,
String.valueOf(paymentBankAccountNumber+'\n'));

                for (Map.Entry f:fraud.entrySet())
                {
                   String fraudmsg=f.getKey()+" "+f.getValue();
                   fraudData.append(fraudmsg+'\n'+'\r');
                   // mailer.sendMail(msg);
                   // System.out.println(m.getKey()+" "+m.getValue());
                }
            }

            message=new HashMap<>();

            message.put("PAYMENT ID :" ,paymentInvoiceId);
            message.put("ITEM DESCRIPTION :" ,String.valueOf(itemDescription));
            message.put("LPO QUANTITY :" , String.valueOf(lpoQuantity));
            message.put("LPO UNIT PRICE :" ,String.valueOf(lpoUnitPrice));
            message.put("PAID AMOUNT :" , String.valueOf(paymentAmount));
            message.put("ITEM UNIT PRICE :" , String.valueOf(lpoListPrice));
            message.put("PAID BY :" , String.valueOf(paymentCreatedBy));
            message.put("SUPPLIER PAID :" , String.valueOf(paymentSupplierName));
            message.put("PAYEE ACCOUNT :" ,
String.valueOf(paymentBankAccountNumber+'\n'));
```

```
            for (Map.Entry m:message.entrySet())
            {
               String msg=m.getKey()+" "+m.getValue();
               data.append(msg+'\n'+'\r');
               // mailer.sendMail(msg);
               System.out.println(m.getKey()+" "+m.getValue());
            }

         }
         connection.close();

         if (!list.isEmpty())
         {
           // notificationFraud();
            jFrameNotification.sendMsg("Fraud Detected! Check email for details");
            mailer.sendMail(String.valueOf(fraudData),"Payments ");
            list.clear();
            System.out.println(list.isEmpty());
         }else
         {
            denouncedFraud();
         }


      } catch (SQLException e) {
         e.printStackTrace();
      }

   } else {
      System.out.println("Could not connect to the database");
   }
}
```

```
    public void notificationFraud()
    {

       if(notifyFraud)
       {
          jFrameNotification.sendMsg("Fraud Detected! Check email for details");

          notifyFraud=false;
       }
    }

    public void denouncedFraud()
    {

          jFrameNotification.sendMsg("No Fraud Detected!");

    }


}
```

MAILER.JAVA CODE

```
import jade.core.Agent;

import java.util.Properties;
import javax.mail.*;
import javax.mail.internet.*;

import static javax.mail.Message.RecipientType.TO;


public class Mailer extends Agent{


   public void sendMail(String message, String header)
   {
      new Thread(() -> {
         Properties props = new Properties();

         props.setProperty("mail.smtp.host", "smtp.mailtrap.io");
         props.setProperty("mail.smtp.port", "2525");
         props.setProperty("mail.smtp.auth", "true");


         props.setProperty("mail.smtp.connectiontimeout", "5000");
         props.setProperty("mail.smtp.timeout", "5000");


         props.setProperty("mail.user", "bcf0d997bde781");
         props.setProperty("mail.host", "smtp.mailtrap.io");
```

```
// props.setProperty("mail.debug", "true");


class PasswordAuthenticatior extends Authenticator{
    private String username;
    private String password;

    PasswordAuthenticatior(String username, String password) {
        this.username = username;
        this.password = password;
    }

    @Override
    public PasswordAuthentication getPasswordAuthentication() {
        return new PasswordAuthentication(username, password);
    }
}

Session session = Session.getDefaultInstance(
        props,
        new PasswordAuthenticatior("bcf0d997bde781","9f38cfc6c514ce")
);

MimeMessage msg = new MimeMessage(session);

try {
    msg.setFrom(new InternetAddress("mungejk@gmail.com"));
    msg.setSender(new InternetAddress("mungejk@gmail.com"));

    msg.setRecipient(TO, new InternetAddress("mungejk@gmail.com"));

    msg.setSubject(header+" Fraud Detection Report", "utf-8");
    msg.setText(message);
```

```
            Transport.send(msg);
        } catch (MessagingException e) {
            e.printStackTrace();
        }


    }).start();

    System.out.println("Email sent!");


  }
}
```

DATABASE CONNECTION CODE

```
import sun.management.Agent;

import java.sql.Connection;
import java.sql.DriverManager;

public class Database extends Agent {

   public Connection connectDatabase() {

      Connection connection = null;
      try {
         //1.Get connection
         // connection =
DriverManager.getConnection("jdbc:oracle:thin://localhost:3306/oracle?useSSL=false",
"root", "Pbluz6480!@");
         connection =
DriverManager.getConnection("jdbc:oracle:thin:@dawson.localdomain:1521:PRD12","app
s","apps");

         if (connection != null) {
            System.out.println("Connected to the database");

         }
      } catch (Exception e) {
         System.out.println(e);
      }
      return connection;
   }
}
```