Anti-Money-Laundering System based on Mainframe and SOA

Mao Shu
College of Software
Northeastern University
Shenyang, China
Maoshu19900502@126.com

Liu Rui
College of Software
Northeastern University
Shenyang, China
liurui.transcendent@gmail.com

Li Dancheng
College of Software
Northeastern University
Shenyang, China
danchengli@126.com

Zhu Shuaizhen
College of IE
Northeastern University
Shenyang, China
frzty@126.com

***Abstract*—This paper presents an efficient anti-money-laundering warning system. With the development of science and technology, money laundering is becoming more and more intelligent. Since the existing anti-money-laundering process cannot handle this kind of crime effectively, we build a system based on mainframe with SOA architectures. For one thing, as mainframes pioneer massive data processing capacity and high security, we take this advantage to handle magnanimity financial data. For another thing, we build superscalar architecture with SOA technology. Application module is presented by service and service bus can connect independent functional entities which carry out specific tasks. Therefore, the system can adapt to the variation of money laundering means.**

Keywords: Service Oriented Architecture, Mainframe, Anti-Money-laundering

I. INTRODUCTION

With the development of science and technology, there are an increasingly growing number of financial crimes in recent years. This happens when the pillars of financial supervision, namely the rule of law and a fair and effective supervision system, are insufficient. As a result, rampant money laundering activities become a way of life both here and abroad. What's more，money laundering activities are inevitably tied up with corruption, smuggling and terrorist organization [1]. As it can provide financial assistance to other criminal activities, money laundering makes great harm to the development of national economy.

With economic globalization and financial liberalization, money laundering activities have shown the following three trends recently: 1 Money laundering activities are transferring from developed to developing countries; 2 Money launderers are becoming intelligent; 3 Money laundering activities are becoming transnational [3]. It is estimated that the annual amount of black money through money laundering is up to 200 billion at home, which accounts for 2 percent of the GDP [4]. This figure is very alarming because it indicates that money laundering is not only a serious erosion of Chinese developing economy, but a severe threat to our national security.

Statistics shows that modern financial system has become the main channel for money laundering. In addition, as finance is becoming globalization, networking and integration, money laundering by modern financial system may become more critical. Thus, the finance agency in China must establish an effective anti-money-laundering supervising system to reduce this kind of crime [4]. On a very conservative estimate, if the money laundering activities reduced 10% to 20% per year, economic losses in China can be recovered 16 to 34 billion dollars [2].

At present, more than 20 countries have established their own national anti-money-laundering organization. FinCEN, the Financial Crimes Enforcement Network, is a network of databases and financial records maintained by the U.S. federal government. Housed within the Treasury Department, FinCEN handles more than 140 million computerized financial records compiled from 21,000 depository institutions and 200,000 nonbank financial institutions [5].

AUSTRAC, Australian Transaction Reports and Analysis Centre, is Australia's Anti-Money-Laundering and counter-terrorism financing regulator and specialist financial intelligent unit [6].

In China, an effective anti-money-laundering system is still in limbo, let alone the off-site supervision function. There is neither an integrated database nor a proper data mining method to combat with money laundering activities. Furthermore, we start anti-money-laundering relatively late, so relevant law and technologies are still not mature [7]. Consequently, anti-money-laundering activities face a severe situation in China.

As the global money laundering activities have brought great harm to the world, it has aroused international attention. Overseas, some system has been applied to anti-money-laundering supervising [4]. The basic principle of these systems is regular reporting of large amount of suspicious transactions. But the supervising is merely based on database technology without a definite quantized model. Therefore, management, configuration and maintenance are hard to implement. What's more, daily financial data in the database need high security while we get little effect in security in despite of the great efforts we made [8]. Though some systems introduce anti-money-laundering models, it is difficult to share information between relevant modules, which makes the supervising process an isolated one.

II. ANTI-MONEY-LAUNDERING MODEL WITH SOA

A. *Mainframe*

Mainframe is famous for its unique reliability, stability, security, availability and massive data processing capacity. These special features make it possible to handle the above

978-0-7695-5069-5/13 $26.00 © 2013 IEEE
DOI 10.1109/CICN.2013.134

difficulties in the system. The system's hardware components have extensive self-checking and self-recovery capabilities. The system's software reliability is a result of extensive testing and the ability to make quick updates for detected problems.

Mainframe system integrates checking techniques for redundancy and error to a high degree. So it can prevent from disastrous problems. In mainframe every CPU Die has 2 execution pipelines to execute the same command. If the outcomes aren't identical, then reset the CPU's condition and re-execute the command. If the outcomes are different from each other again, the condition of CPU will be restored into another idle CPU to run again. This design mechanism reduces the chances of errors. At the same time, there is redundant design or corresponding replacement of memory chips, memory buses, I/O channels and power in mainframe to handle sudden and catastrophic attacks. Inevitably some equipment may cause some small loss, but it never causes any failure or stagnation of any task.

Even though there are some errors in the system, the mainframe's availability guarantees the proper functions. Most of the components can be replaced in hot-plugging way; even the microcode can be update in running time. To some devices that don't support hot-swapping, the replacement of them can help to avoid big problems. Apart from these techniques, IBM also introduces a new system called Parallel Sysplxe. Parallel Sysplxe combines 32 independent systems as a whole. Therefore, if the system is proper deployed, the system suffers little even if one independent system has been devastated ruined. Generally, all the work in the ruined system will start again in another system automatically. Apart from the advantage, Parallel Sysplxe can also make system maintenance more convenient. We can remove some part from the whole system in their spare time to make maintenance while other independent systems continue to work. When the maintenance finishes, we can get this inspecting system to its early position. Consequently, making full use of this feature, we can upgrade the software of the system without causing any application suspended. Accordingly it is the powerful processing mechanism that ensures the optimum application on the mainframe without any error and failure.

Actually, a mainframe channel is a PCI in some aspects. Just like bus, channel connects one or several controllers. It does share many features with bus, but they also differentiate from each other. The biggest difference is the method connecting to controller. Channels in mainframe connect the controller with some bus and tag (parallel access method) or ESCON fiber-optic cable (serial access method). In the early years, the channels are external boxes of the system. But now it is integrated into the framework. These channels are in fact I/O processors running channel programs which consists I/O instructions. Each channel can handle plenty of I/O operations and control hundreds of devices. As the channel decrease CPU'S workload, the I/O throughput of framework can reach 24 GB/s.

B. Service Oriented Architecture

SOA is a flexible and efficient set of design principles used during the phases of systems development and integration in computing. SOA is an architectural solution with key characteristics that distinguish it from previous architectural designs. Compared with traditional technology, SOA pays more attention on services and standardized technology method. A deployed SOA-based architecture will provide a loosely-integrated suite of services that can be used within multiple business domains. In fact, it is a component in a higher level.

SOA is a kind of hierarchy architecture. The bottom are functional services, the middle are atomic services and service components while the top are specific business process. SOA implementation relies on a mesh of software services. As service is the core of SOA, varies services are applied in different level. We can increase development efficiency and development quality greatly with service reusability. But these services are not isolated, they usually need to share information with each other and be interactive. SOA provides an approach to integrate various existing application module. Therefore, we can also make quick response to business-changing with service componentization.

SOA is applied to Anti-Money-Laundering system to build new framework because of its componentization, reusability, loosely-couplings and openness.

1. Componentization: Services are effective composition participants, regardless of the size and complexity of the composition rather than large number of code. And each component can provide different service. So componentization makes the application system easy to implement.

2. Reusability: Logic is divided into services with the intention of promoting reuse. Flexible services in SOA, along with the service registry and service repository, provide uniform means to deliver, locate, and interact. This promotes and maximizes reuse of services at the enterprise level.

3. Loosely-coupled: Services maintain a relationship that minimizes dependency and only requires that they maintain an awareness of each other. In SOA architecture, we can combine design and application together if we use graphical tool to assemble different components. In this way, the architecture becomes loose coupling and stable. Loosely-coupled services, even if they use incompatible system technologies, can be joined together on demand to create integrated process, or disassembled into their functional components easily.

4. Openness: First, the services according to SOA standard can communicate with each other. In addition, SOA can not only make full use of the previous resources, but also be flexible to meet the changeable architecture demand of services in the future. The key principle of SOA is providing business agility by making IT flexible to adapt to changes.

Different modules in anti-money-laundering system can communicate with each other with SOA technology. Each module is a component in the architecture, so the modules

can compose with others to adapt more complex anti-money-laundering tasks.

III. IMPLEMENTATION OF ANTI-MONEY-LAUNDERING SYSTEM

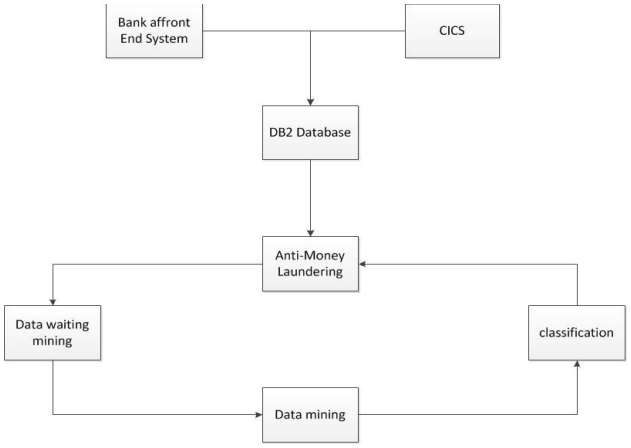

Figure 1. The process of the Anti-Money-Laundering System

The system is based on IBM mainframe. It is composed of many subsystems in SOA environment. And every subsystem consists of several functional modules. The purpose of the system is to do off-site monitoring and to accumulate information for latter anti-money-laundering. The People's Bank of China has carried out corresponding laws after analysis of money-laundering activities' features. We transfer the laws into computer language to estimate some attributes in the system. And we also set the ultimate value according to money-laundering pattern and features already known. Therefore, all financial transactions will be marked by 5 different rates. Different rates have different processing mode. Transactions in the last level will get warning directly while the other four levels will enter data mining process to do further mining.

Mainframe starts data processing unit(OPC) automatically according to the initial setting time. First invoking from bank front-end, data connect and transfer to DB2. After that, the file system in CICS closes and the data file put itself into anti-money-laundering system. This is the whole process of data file preparation. Then the system read the parameters. In this way, users can set the parameters according to different national laws and regulations. For instance, in some areas overdraft is becoming common to some credit card users. This phenomenon is considered to be suspicious based on anti-money-laundering rules in China. However, this phenomenon is normal in some developed areas. So it is necessary and beneficial to set the system parameters according to specific condition. The flexibility in setting parameters makes the system a dynamic one. What's more, this feature can also add the latest model aspects to the system in spite of the variation of money-laundering day after day.

The system executes the anti-money-laundering module according to difference of processing cycle. We divide it into 5 parts: DE (Daily Execution), WE (Weekly Execution), ME (Monthly Execution), QE (Quarter Execution), FE (Free Execution). In DE part, anti-money-laundering module is processed every day. In WE part, we compare the data in a week. ME part compare the data of the latest four weeks. In QE part, system copes with data in 3 month. FE is a real time monitoring. If the bank staff finds some questionable transactions on the counter, they can use this FE part to determine whether give warning or not. This approach makes the system more flexible and timely.

TABLE I. THE ANTI-MONEY-LAUNDERING MAIN MODULE

Module	Module Function	Remark
AMLBU01L	Back up all the remaining files in AML system.	Input data, e.g. relationship account
AMLP002D	Export CICS files to batch files	
AMLP003D	Create customer information management files	
AMLP001V	Verify the date, bank code, cash code, account number, etc.	Input information of current deposit, fixed deposit, fund, loans and credit cards.
AMLP007E	Compare the values of some transactions and identify the account owner, compare the attribute value to the initial value.	
AMLP000E	Emergency Anti-Money-Laundering solution module	
AMLPC04F	Additional files of DE, WE, ME, QE	
AMLP034W	Combine cash and financial documents weekly and compare the attribute value.	Every week
AMLP088M	Combine cash and financial documents monthly and compare the attribute value to the initial.	Every month
AMLP040Q	Combine cash and financial documents quarterly and compare the attribute value to the initial value.	Every quarter

Table 1 shows the architecture of the anti-money-laundering module.

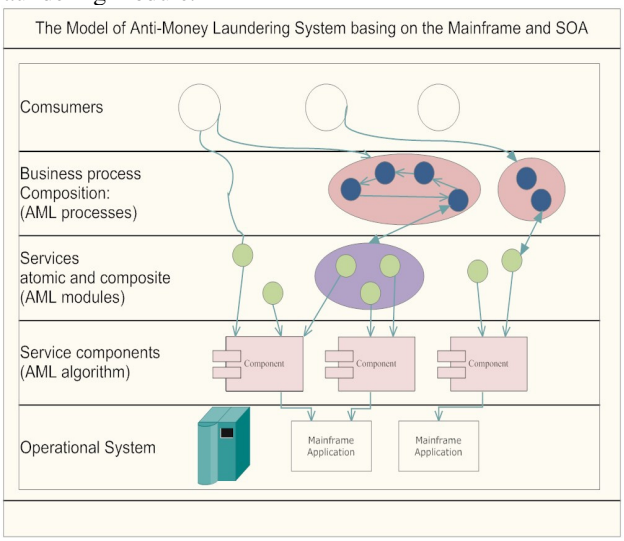

Figure 2. The model of the Anti-Money-Laundering System

The anti-money laundering model based on mainframe has a multi-tier architecture with SOA technology. The bottom tier is mainframe application. To implement web Service in CICS environment, we use several resources: URIMAP, PIPELINE and WEB SERVICE. By combining web service description, web service file and PIPELINE together, mainframe application module can be published as web service. The second tier is abstract service components rely on anti-money-laundering algorithm. The third tier is various concrete application modules. The upper tier is specific business processes. As the eclipse community has released the Swordfish framework to build enterprise service bus, different service components can form new business process to adapt to different tasks of money laundering activities. The top tier is an interface to user. User can choose an appropriate process according to the current situation through Struts framework. Therefore, each service can make interaction with others to improve efficiency. For example, processes based on weekly, monthly or quarterly may generate some useful information to support real time module while the real time module can provide the latest information of knowledge base to regular processes.

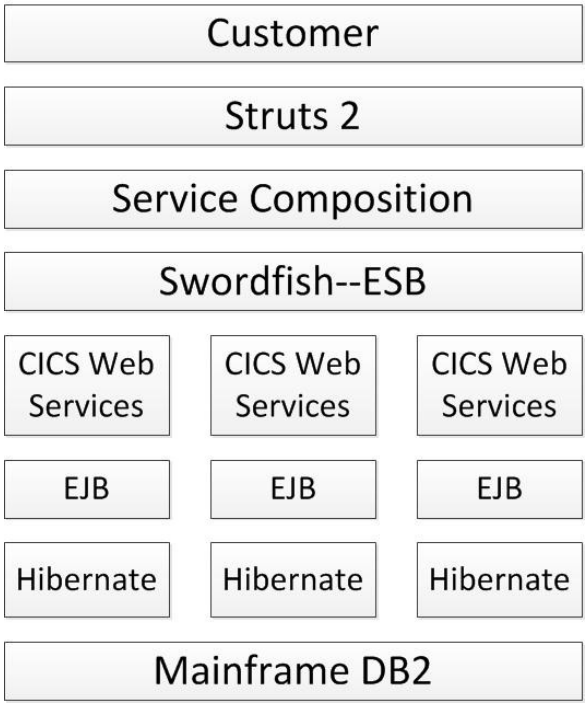

Figure 3. The architecture of the Anti-Money-Laundering System

IV. CONCLUSION AND FUTURE WORK

Based on mainframe, the system provides an efficient solution to many problems such as large amount of financial data, low quality of data and so on. Besides, the application of SOA brings many benefits to the system. It is an architecture fit to all the developments rather than a set of isolated applications that can't share information. The solution also makes it easier to work with customers and suppliers and, indeed, everyone in the business process. However, anti-money-laundering is a demanding job while the system isn't silver bullet. It is necessary to work out more efficient algorithm to make further breakthrough. In addition, the system is too dependent on the strong performance of IBM mainframe while the mainframe didn't gain popularity for the high cost. Accordingly, the system can only be used in limited scope. We will take measures to improve the algorithm performance and the system efficiency to wider the range of applications in the future research.

REFERENCES

[1] Li Chen, A Design for Anti-money Launcher System basing on the Mainframe Platform and Data mining, WuHan University, May 2005.

[2] Alvaor E. Monge, An Adaptive and Efficient Algorithm for Detecting Approximately Duplicate Database Record, pp.180–204, Jane 2000.

[3] Gao Zeng'an, National Anti-Money-Laundering Commitment: A Theoretical Perspective, Journal of social sciences, pp. 24-29, Feburary 2010.

[4] Tong Wenjun, Development,Challenge and Policy Trend of Money Laundering Monitor in International Finance, Finance and economy, vol.27, pp.13-15, November 2009.

[5] Chaim Even-Zohar, FinCEN Denies that U.S. Jewelry Industry Compliance Rules Serve as "Trade Barrier" to Protect Domestic Dealers, Diamond Intelligence Briefs, Feburary 2005.

[6] Tom Godfrey, Countermove on dirty money, The Global Standard, March 2005.

[7] Li Guo ren, The situation of anti - money - laundering and countermeasures, Journal of Guangdong Economic Management College, January 2004.

[8] Hemalatha G., Mathews R., Intelligent Agent & Multi-Agent Systems, 2009. IAMA 2009. International Conference on 22-24 July 2009, pp.1-3.