International Journal of u- and e- Service, Science and Technology
Vol.8, No. 11 (2015), pp.95-104
http://dx.doi.org/10.14257/ijunesst.2015.8.11.10

A Study on Establishing Abnormal Financial Transaction Detection System in Securities Business Circles

Gyoo-cheol Lee[1], Joonsik Jang[2], Se-jeong Park[3],
Yongtae Shin[4] and Jong-Bae Kim[5*]

[1,2]Dept. of IT Policy and Mgmt., Graduate School of Soongsil Univ., Seoul 156-743, Korea
[3,4,5]Graduate School of Software, Soongsil University, Sangdo-dong, Dongjak-gu, Seoul, Korea*
[1]sopoong297@hanmail.net, [2]justin.jang@autodesk.com, [3]sejung90@naver.com, [4]shin@ssu.ac.kr, [5]kjb123@ssu.ac.kr*

Abstract

The past has focused on domestic transactions from the point of accident prevention on the basis of security. Of course, it is a problem that its security measures had been focused on the user terminal stage. By supplementing it now, securities business circles are expected to announce "None Face-To-Face Account Opening". Therefore, they have been introducing and advancing Fraud Detection System (FDS) that integrates log data from HTS (Home Trading system) and security system; models trading patterns; and detects and analyzes abnormal financial transactions based on the scenarios. Considering such characteristics of securities business as ordering and transferring stocks or shares, the present study proposes trading patterns specialized in the business and detection plan (decision making) after examine four major functions, patterns and detection of FDS.

Keywords*: FDS, Detection, Analysis, Pattern, Security, HTS*

1. Introduction

In 2015, Pin Tech settled down in the Korean financial market as one of IT trends. Even in 2015, the use of security module turned to the discretion of a financial company, so opening a simple payment market. However, it is practically very difficult for individual consumers to do so and be bailed out. In the meantime, financial companies are busy establishing Fraud Detection System (FDS) to prevent electronic financial fraud and minimize damages from it. FDS is a framework for financial security. It should be approached as a framework and capable of providing users' convenience and safety in using financial services while financial companies have to approve safe and legitimate transactions. To do so, financial companies have to detect abnormal transactions and authorize normal transaction swiftly. However, wrong and insufficient detection can undermine the quality and reliability of financial service. It means the detection should be meticulous and perfect. To achieve the goal, it is required that sensitive personal information such as terminal information, user information, and transaction information are collected [1, 4].

With this respect, the present study intended to find the optimal patterns and rules for securities business circles by using profiling on a customer's device information, log-in

* Corresponding author. Tel. : +82-10-9027-3148.
Email address: kjb123@ssu.ac.kr(Jong-Bae Kim).

ISSN: 2005-4246 IJUNESST

data and financial transactions, which are collected when individual investors issue order, buy and sell stocks and bonds and transfer account.

2. Related Works

2.1. Key Functions of FDS and Abnormal Transaction Detection Model

According to "The Technical Guide to Abnormal Financial Transaction Detection System" of Financial Security Institute, FDS is defined as a system that does cross analysis on information of user's medium, transactions, and location, which is collected during financial transaction holistically and systematically to discriminate between abnormal and normal financial transactions [2, 7, 8].

Telecommunications Technology Association published and announced 'The Guide to Abnormal Financial Transaction Detection and Counter-Framework (December 21st, 2011)' and proposed the requirements, system functions, and detection framework against abnormal financial transactions. Particularly, the guide emphasized financial company's sharing of FDS operation and detection information [3, 5, 6].

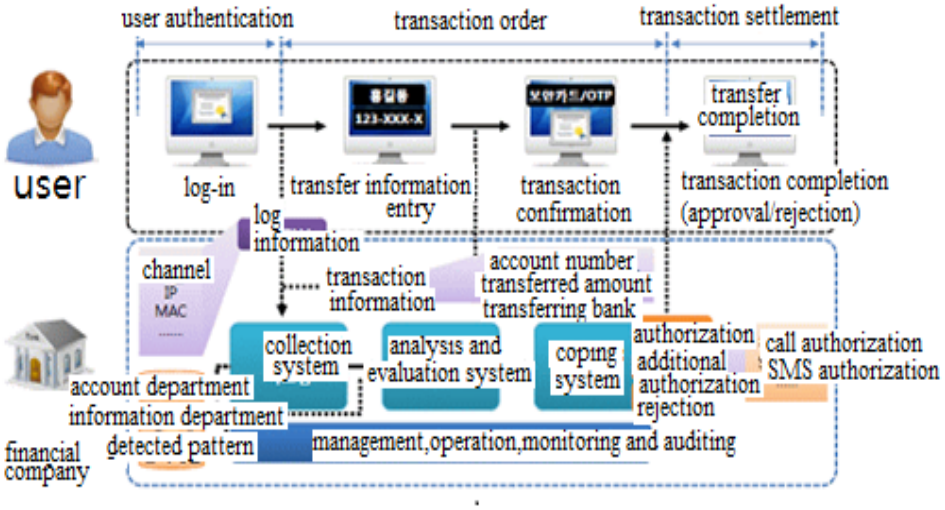

Figure 1. Example Of Cross Action of Abnormal Financial Transaction Detection System and Financial Transaction Procedure [1]

Data collection function is to collect a variety of information depending on user's access channels (Internet banking, smartphone banking and *etc*.) and information of network, hardware, and application to endure uniqueness.

Active-X and Plug-In, which are installed as separate programs and collect base information, are relatively accurate in detecting abnormal transactions because it can collect various hardware information from the user's PC. However, it requires the development of a separate collection program by the user's operation system and web browser. Web-based information collection methods (html, JavaScript) do not require the installation of a separate collection program (Clientless) and can be applied widely regardless of user's OS and type of browser, but it is hard to collect various hardware information of user's PC, so it has limitation in detecting abnormal transactions [2].

Analysis, analysis and detection function is to collect information of user's operational environment and type of transaction for a certain period, process (profile) the collected electronic financial transaction information statistically, monitor and detect suspicious transactions by filtering electronic financial transactions in real time and step by step. To

detect abnormal transactions, it uses static information (fake bank pass book, Geo IP, MAC, Blacklist and *etc*.), rule-base using accident information patterns, Score-base using various profiling attribute scores and combination of the three detection bases just mentioned.

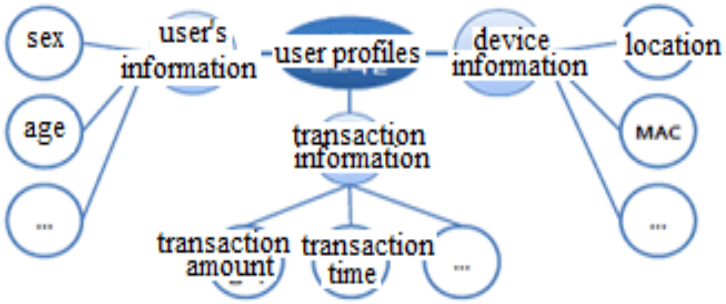

Figure 2. Analysis and Detection Functions

2.2. Detection Methods of FDS

The detection method of FDS can be shortly summarized as issuing an alert when a financial transaction breaks the bound of a pattern [8, 9]. FDS methods include Rule Method that applies several patterns, and Score Method that standardizes ordinary financial transaction patterns on a daily basis and quantifies the correction between the patterns with the patterns of illegal transactions, which results in scores.

To apply Rule Method, it is important to find abnormal financial transaction patterns out of the types of domestic financial accidents and service threat scenarios, and to create detection patterns by using information of users' medium environment transaction types together. This detection model with simply more than two rules whose scopes are set can screen fraud, but it is likely to end up in false positive error unless the two rule variables are not correlated with each other. Therefore, correlation analysis is necessary to apply to this model on the basis of the history of more than two variables. It can optimize the balance between fraud detection and false positive error.

Score Method sets the normal pattern boundaries for user's collected information (ID), integrate information of device and set patterns and sets the score range of normal pattern within (1~100), and considers the transactions not included in the normal range as abnormal transactions and detects them.

3. A Plan to Establish FDS

For this study, the paper looks into the characteristics of Power Base system and models monitoring systems connected with FDS system, which it is scheduled to build. Aside from this, this study attempts to examine collected information and detection rules.

3.1. Research System

This study is aimed to successfully co-manage the ledgers of 14 securities firms and introduce HTS service to FDS. To realize the model, this study proposes the following plan for service flow and system configuration.

3.1.1. Service Flow and System Configuration

The service flow of FDS is described as follows: the system receives transaction telegram (electric text) from securities firms and compares the transactions with abnormal transaction rules (patterns) and user's profile data to detect abnormal transactions. Depending on the level of the detected abnormality, a securities firm performs the second

authentication, blocking transaction, confirmation call through the integrated call center to check abnormal transaction. The integrated call center runs at night and on holidays in an effort to provide detection service and blocks such transaction immediately. Figure 3 shows FDS Service Flow.

The system can consist of work systems (WAS, telegram collection such as ledger), FDS system (collection of device and transaction information; processing, detection rules, black list detection, user profile comparison analysis, detection information coping), FDS Backup data (database, log data save/analysis, various profiling for entering user profile creation rules, and rules/detection information analysis), and control UI (detection activities and system monitoring UI, rule management, backup data analysis, reporting of detection results). Figure 4 shows the system configuration.

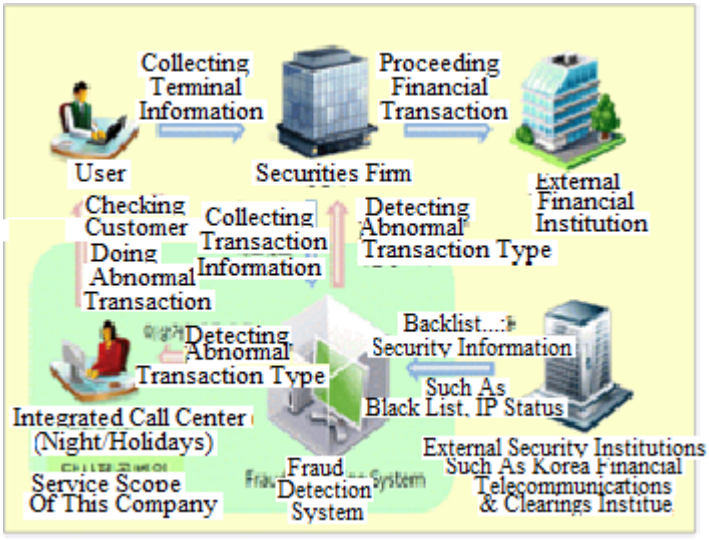

Figure 3. FDS Service Flow

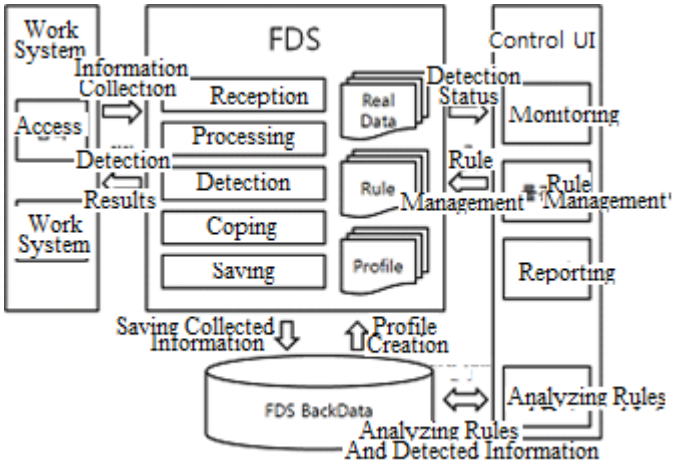

Figure 4. FDS System Configuration

3.1.2. Ledger Account Department and FD System Work Flow

FDS Work Flow is as follows:

① Customer; an HTS customer logs in with his/her terminal and makes a request for electronic financial service such as transferring and/or book entry clearing

② Ledger-Account Department; the department makes a request to FDS about transaction before handling customer's request

③ Ledger-Account Department; the department keeps preceding the concerned work without waiting for the reply of the ledger and is ready for process change according to the result from FDS

④ FDS System; FDS carries out abnormality detection for the requested case and sends the result back to the ledger account department

⑤ Ledger-Account Department; in case that the result from FDS turns out to be an abnormal transaction, it gives an abnormal transaction detection alert (including SMS) to PB branch terminal for the concerned transaction and informs a person in charge

⑥ Securities Form; a person (call center) in the securities form makes a call to the concerned customer to check the transaction

⑦ Securities Form; when the transaction is proved to be normal (true), it continues the service

⑧ Securities Form; it records the results of coping with detected abnormal transactions in FDS through PB terminal to use them later for abnormal transaction analysis

3.1.3. A Plan to Connect Ledger-Account Department System to FDS

Two scenarios can be pictured: (1) in case that FDS system is not connected with DB server of the ledger-account department and (2) in case that FDS system is connected with DB server of the ledger-account department. First, when FDS can't have access to DB server, a new interface should be developed in FEP of the ledger server. Figure 5 shows that FDS System is not connected with DB Server. So, the ledger server (AP Server) can request AP (open account, log-in and transfer) to DB server and they (APs) can be requested to FDS through the newly developed interface. Then, FDS records detection results in DB server through the new interface when requested and sends the result to AP server for the second authentication and blocking abnormal transaction. Second, when FDS can be accessed to the FDS DB server of the ledger-account department, the ledger server FEP does not need a new interface to develop since FDS is directly connected to DB server. Figure 6 shows that FDS system is connected with DB Server.

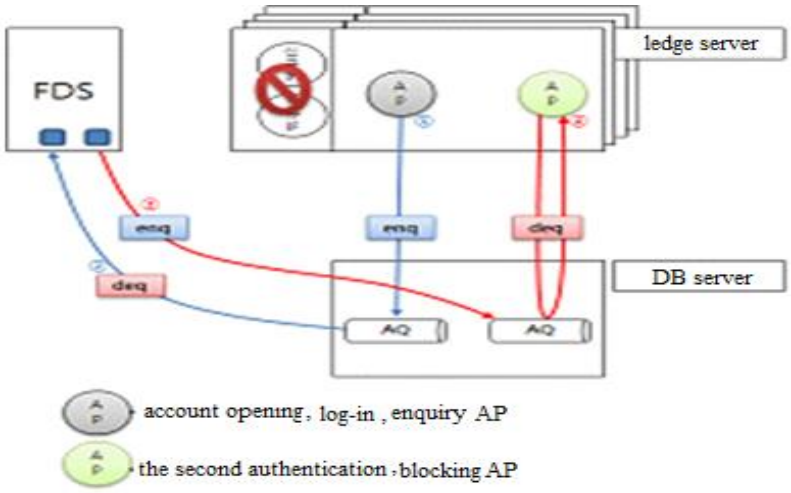

Figure 5. In Case that FDS System is not Connected with DB Server

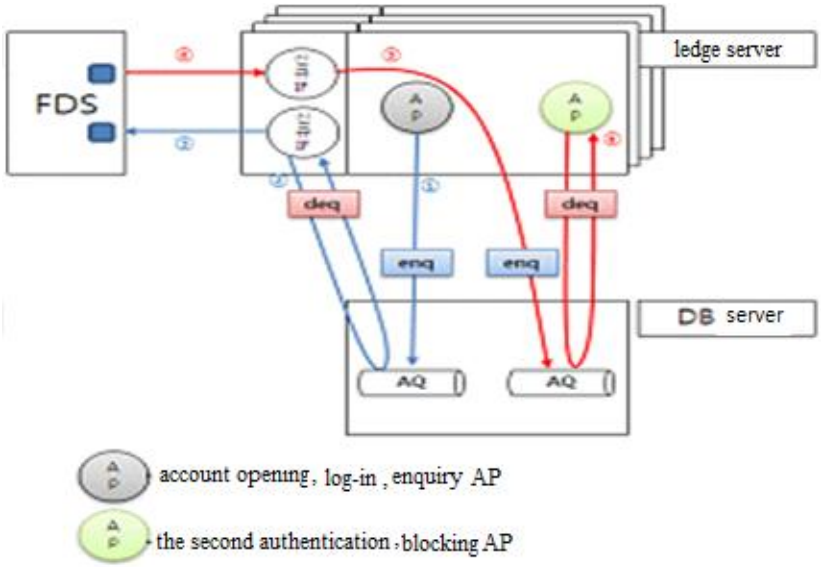

Figure 6. In Case that FDS System is connected with DB Server

3.2. Studies on Detection Rules and Patterns

The collection types of FDS information collection function can be divided into 'user's medium information' and 'accident type information'. Collecting the environment information of user's medium can vary depending on the types of access channel (Internet banking, mobile banking) and collection functions. Existing collection methods use 'plugin-based' detection method or through a collection program, or web applications such as Java Scripter. Detection patterns that use the collection information can be divided into 3 types: detection method using (i) user's access environment information such as user ID, (ii) user's information of accredited certificate issuance and changing it, and (iii) user's different transaction behaviors from ordinary financial transactions. Detection of abnormal financial transactions is to analyze their environmental elements based on the collected information at first to discriminate abnormal from abnormal transactions. And then, it usually follows the second procedure of comparing current financial transactions with past transactions. To detect abnormal financial transactions on the basis of the types of accident information, financial companies and companies in similar business lines need to survey the trend of abnormal financial transactions, PC forensic test, and analysis of accident causers by type.

3.2.1. Acquired Information Used for Financial Transaction of Security Account

It is possible to acquire information of security account, transaction medium and activities in network from the financial transaction information. Usually, such financial transactions give information of consistency, repetitiveness and non-transaction account of users by transactional attribute.

Table 1. Activities and Attributed that Can Be Collected Through Financial Transaction

Classification	Activity	Attribute
Account	Lo-In Transfer Behavior Opening Account Account Enquiry Personal Information Enquiry Issuing Accredited Certificate	Persistent Repetitive Same Amount High Amount Number Of Times Transfer-ring No Transaction Account Minors Accident Account Overseas Account New Issue Re-Issue
Medium	Simultaneous Access To PC And Smartphone Alteration Of Terminal Infor-mation (Rooting, Escaping)	
Network	Detour, Via Overseas IP	
Transaction Type	Product Type Code Account Transaction Classifica-tion Code	

3.4.2. Profiling of Collected Information

How should the collected information (entity, activity, attribute, black list and so on) be arranged and expressed in a continuous way? How should change of state (after log-in, after opening an account) be defined? The answers to these questions can reduce the false detection of FDS and time to analyze them. The table below shows the result of profiling acquired information.

Table 2. Black List Profiling

Se-quence No	IP Ad-dress	Mac Ad-dress	HDD Serial No.	Certificate Serial No.	User ID	Acci-dent Account	Fake Pass-book	E-mail	Tele-phone No.	…	delflag
1											t' or 'f'
	Medium Information				Customer Information						

Table 3. User Profiling

User ID	Sex	SSN	Login Time	Date of the Latest Change of Pass-word	…….	delflag
	m' or 'f'			YYYY:MM:SS hh:mm:ss		t' or 'f'

Table 4. Account Profiling

Account o	User ID	Open Date	Minimum Transfer Amount	Maximum Transfer Amount	Average Transfer Amount	Fixed Account	Fixed Account No	…	delflag
						t' or 'f'			t' or 'f'

3.4.3. Detection Rules and Patterns to Detect Abnormal Transaction

The performance of FDS detection and analysis include account opening, log-in, account transfer, enquiry of deposit/balance, personal information enquiry, enquiry /editing and accredited certificate. In addition, it is also necessary to consider a plan to utilize MaxMind (www.maxmind.com) information to secure overseas Geo IP information. To

cope with abnormal financial transactions, user's medium information and transaction information should be used together in establishing detection patterns. That is, more than single source information should be used to develop efficient detection patterns and reduce wrong detection. The behavior of finding and developing the patterns can be classified into access pattern, transaction pattern, and behavioral pattern out of Big Data.

Table 5. Rule Patterns Using Process State Transition

Rule No	Specifications of Rule Patterns
Rule#01	Is selling or buying of stock ordered through an account or PC (Mobile) that once was involved in financial accident or is related to it?
Rule#02	Does the order for selling or buying stocks (accessed overseas) take place from different PC (mobile) from what used to be?
Rule#03	Is it the order for selling or buying stocks that different IP used from the previous transaction and country code and IP are different from those of the previous transaction?
Rule#04	Is it the order for selling or buying stocks that has shifted from while list to black list in profiling group?
Rule#05	Has it been transferred or deposited in cash abroad to another account after contracting selling or buying stocks?
Rule#06	When it comes to the order of selling, does it keep ordering at the minimum price, rather than market price?
Rule#07	Compared with his/her past ordering (selling and buying), has he or she issued order frequently enough to be obvious?
Rule#08	…

4. Conclusions

Securities include defining works to apply, writing the basic workflow necessary to design FDS network configuration, rule management by securities firm, cooperation with a person in charge to determine the level of coping by securities firm and should be discussed from solution. In this study, we proposed trading patterns specialized in the business and detection plan (decision making) after examine four major functions, patterns and detection of FDS. The present study suggests a further study with Big Data analysis to use a bulky DB that contains tremendous information, which can reduce false detection and detect abnormal transactions in real time or very short time. This requires modeling pattern and detection with algorithm.

References

[1] Financial Supervisory Service Press, "Financial groups Fraud Detection System (FDS) Advancement 1.0", Financial Supervisory Service (FSS), **(2014)**.
[2] Financial Security Institute, "Fraud Detection System Technology Guide", **(2014)**.
[3] Telecommunications Technology Association, "Corresponding guide for Fraud detection and response framework", **(2011)**.
[4] KOSCOM internal reports, "Introduced into research and report on the financial industry FDS", KOSCOM, **(2015)**.
[5] Y. Lee, "Cloud Computer standardization direction of the mobile services spread", Korea information Processing Society, vol. 18, no. 5, **(2011)**, pp. 10-19.
[6] HWASAN Media, "The new paradigm of next generation security smart defense 2.0", HWASAN Media, **(2015)**.
[7] Y. Lee, "Cloud Computer standardization direction of the mobile services spread", Korea information Processing Society, vol. 18,no. 5, **(2011)**, pp. 10-19.
[8] H. Y. Min, "Outlier Detection Method for Mobile Banking with User Input Pattern and E-finance Transaction Pattern", Journal of Internet Computing and Services (JICS), vol. 15, no. 1, **(2014)**, pp. 161-163.

[9] H. Seo, "Novel Anomaly Detection Method for Proactive Prevention from a Mobile E-finance Accident with User's Input Pattern Analysis", KIISC, vol. 21, no. 4, **(2011)**, pp. 51-53.
[10] G.-C. Lee, "A Study on Detection and Rules for Establishing Abnormal Financial Transaction Detection System in Securities Business Circles", ASTL.

Authors

Gyoo-Cheol Lee, he is studying his Ph.D. degree of IT policy Business Administration in Graduated Soongsil University, Seoul. He worked as a developer and operator of a business sale signed by joining Koscom. And He has worked as the analysis and evaluation team leader of information protection center. His current research interests include financial IT, IT security policy, the field of analysis of infringement accident or hacking and information protection management system (ISMS).

Joonsik Jang, he received his master's degree of Business Administration in Graduated Sungkyunkwan University (1999). He is studying his Ph.D. degree of IT policy Business Administration in Graduated Soongsil University, Seoul. Currently, he has worked as the leader of the Subscription and Cloud Service business from multinational IT company Autodesk. His current research interests in related fields.

Se-Jeong Park, she received her bachelor's degree of Software Engineering in Kongju National University (2014). She is studying her master's degree of software engineering in the Graduate School of Software, Soongsil University, Seoul. Her current research interests include Database and Open Source Software.

Yongtae Shin, he is a Ph.D., professor in the School of Computer Science and Engineering, Soongsil University, Seoul, Korea. His research interests focus on Multicast, IoT, Information Security, Content Security, Mobile Internet, Next Generation Internet.

Jong-Bae Kim, he received his bachelor's degree of Business Administration in University of Seoul, Seoul(1995) and master's degree(2002), doctor's degree of Computer Science in Soongsil University, Seoul(2006). Now he is a professor in the Graduate School of Software, Soongsil University, Seoul, Korea. His research interests focus on Software Engineering, and Open Source Software.