International Journal of Engineering & Technology, 7 (3.33) (2018) 72-77

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Location based FDS Framework

Jong-Bae Kim[1]*, Myung-Jin Bae[2]

[1] *Graduate School of Software, Soongsil University,369, Sangdo-ro, Dongjak-gu, Seoul, 06978, Korea*
[2] *Department of Telecomm. Engr., Soongsil University, Sori Engineering lab, 369, Sangdo-ro, Dongjak-gu, Seoul, 06978, Korea*
**Corresponding author E-mail: kjb123@ssu.ac.kr*

Abstract

The FDS (Fraud Detection System) is a technological approach to prevent financial accidents by detecting abnormal behavior in financial transactions. In this paper, we present system components and considerations for efficient FDS construction and operation, and propose an optimized FDS operation framework based on IT governance. In addition, we propose a model that can improve the accuracy of abnormal transaction detection by using GPS information of user. This research is expected to be an operation model for Fintech based FDS that enables safe transactions without sacrificing the convenience of customers.

Keywords: *Fraud Detection System, Financial, Fintech, Location, GPS, Governance*.

1. Introduction

Fintech is a portmanteau of financial technology that describes an emerging financial services sector in the 21st century. Originally, the term applied to technology applied to the back-end of established consumer and trade financial institutions. Since the end of the first decade of the 21st century, the term has expanded to include any technological innovation in the financial sector, including innovations in financial literacy and education, retail banking, investment and even crypto-currencies like Bitcoin [1].

With Fintech technology, users can handle loans, account transfers, and product purchases more easily and conveniently. However, instead of being easy to use, there are a lot of security threats. According to US market researcher Nielson in 2014, the US smartphone penetration rate is 71%. It means that most of the population has smartphones except for infancy and old age population.

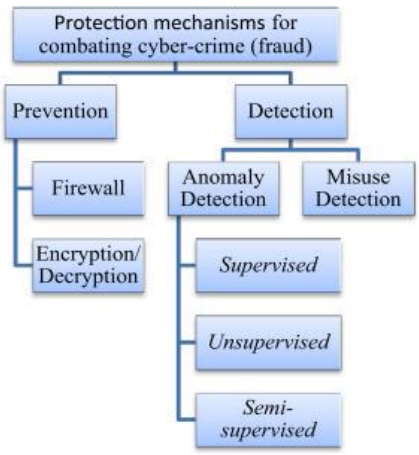

Fig. 1: Protection systems against fraud

On the other hand, with the advancement of Fintech, technologies that make payment using smart phones are pouring out. RSA reported that in the United States, the amount of credit card fraud in 2014 was 3.2 trillion won, and They predict that if Fintech continues to proliferate, it will increase to 7.5 trillion by 2018. In the United States, it is estimated that credit card fraud will erode 30% of the financial industry in 2020, as CT firms enter the banking industry. As a result, fighting fraud has become an important issue to be explored. As presented in Fig. 1, the detection and prevention mechanisms are used mostly to combat fraud [2].

The FDS (Fraud Detection System) is a technological approach to prevent financial accidents by detecting abnormal behavior in financial transactions. The FDS is a system that intercepts abnormal financial transactions by detecting suspicious transaction by analyzing the information of terminal used in electronic financial transaction, access information, transaction contents, and settlement location in a comprehensive manner. With FDS, even if the user's financial information is exposed to fraudulent use, it can be blocked before payment or additional authentication is possible.

Since the mid-90s, credit card companies have begun to build FDS. Recently, banks, insurance companies and securities firms are building FDS. Because these companies have a lot of non-face-to-face transactions. In recent years, the need for convenience in the use of simple settlement and financial services has increased due to the enthusiasm of Fin-Tech.

Therefore, the need for FDS system construction is increasing in view of enhancing security so that customers can use financial services more safely. Accordingly, Korea's Financial Security Research Institute (KRIB) published a technical guide for abnormal financial transaction detection systems in 2014. FDS is now being built in a variety of ways to meet the needs of financial institutions, combining the technical issues of Big Data Analysis and security solutions.

In this paper, we present system components and considerations for efficient FDS construction and operation, and propose an op-

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

timized FDS operation framework based on IT governance. In addition, we propose a model that can improve the accuracy of abnormal transaction detection by using GPS information of user.

2. Related Works

2.1. Fintech

Financial technology (FinTech or fintech) is the new technology and innovation that aims to compete with traditional financial methods in the delivery of financial services. Fig. 2. shows the architecture of FinTech [3].

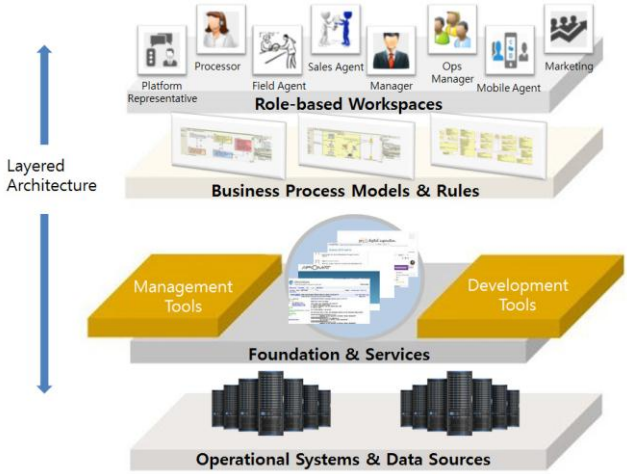

Fig. 2: Fintech Architecture

FinTech is a new industry that uses technology to improve activities in finance. The use of smartphones for mobile banking, investing services and cryptocurrency are examples of technologies aiming to make financial services more accessible to the general public. Financial technology companies consist of both startups and established financial and technology companies trying to replace or enhance the usage of financial services provided by existing financial companies [4-6].

FinTech can be characterized as the movement to bring transformative and disruptive innovation to financial services through the application of new and emerging technologies which address consumer needs through automation.

With the advent of Fintech, many changes are taking place in the existing financial environment. In recent years, the UK's Fintech industry has been attracting worldwide attention and actively supported regulatory compliance and resource support by adopting it as a next-generation growth engine at the national level.

In the United States, Fintech industries are becoming more active, especially in Silicon Valley and New York. Large ICT companies such as Facebook, Google, and eBay are also entering the financial sector. Apple's Apple Pay meets users in convenience and security.

In addition, China has been fully supported by the government and a global company called Alibaba has been established. The mobile market is also actively promoted to 500 million people.

2.2 Fraud Detection System

A typical Fraud Detection Process (examples of card fraud) is shown in Fig. 3.

Fraud Detection System is a security solution that can signal the threat of fraud before customers fall prey to the perpetrators. The system analyzes suspicious behavior and produces reports for security and risk mitigation purposes. Unlike network security solutions, the system reports suspicious activity before it escalates into fraud, identity theft or other crimes [7-9].

The existing fraud detection system analyzes the user 's media information and transaction history, and detects misuse or abnormal.

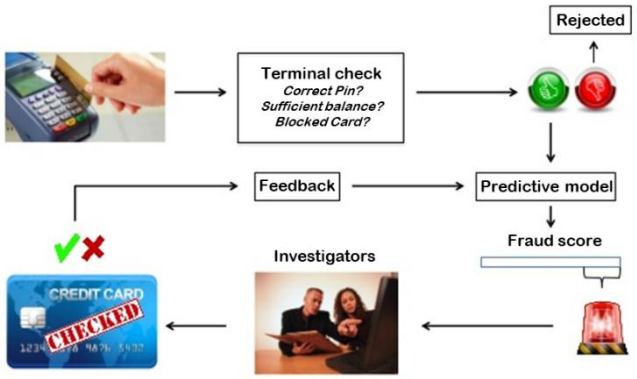

Fig. 3: Fraud Detection Process

In other words, as shown in Fig. 4, when a user generates a transaction, the FDS analyzes the media environment information, transaction information. If an error is found in the transaction, the system requests additional authentication, or not, the transaction is completed.

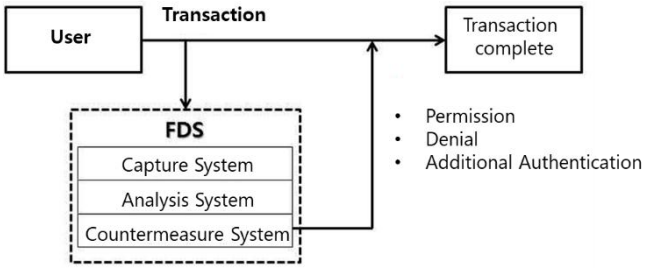

Fig. 4: Existing FDS System

Fraud detection systems are based on misuse detection and anomaly detection. It is based on the concept of (Intrusion Detection System) misuse detection system and anomaly detection system.

The misuse detection system analyzes fraud patterns in the past and detects irregularities by checking whether the fraud patterns match the currently inputted patterns. Since the misuse detection model relies on past accident information, the falser information, the lower the false rate, but cannot detect newly discovered abnormal transaction information.

The anomaly detection system analyzes user data for a few weeks or months and uses it as a reference to detect when there is a relatively rapid change or when a stochastically low activity occurs. Although it is possible to detect unknown fraudulent transactions in advance, it has a disadvantage that it is difficult to predict normal behavior, high false positives, and it takes a long time to analyze various collected information.

On the other hand, the technical guide for abnormal financial transaction detection systems that proposed by Korea's Financial Security Research Institute (KRIB) consists of information collection, analysis and detection, countermeasure, monitoring and audit. The components of the proposed FDS can be configured in a variety of ways according to the financial resources of the financial institution, FDS operation strategy and security requirements.

First, in the information gathering phase, a system and a database for collecting personal information of electronic financial users and various electronic financial transactions (information on bank transfer, use of cash card, use of credit card, loan, etc.) should be constructed.

Second, in the analysis and detection phase, statistical detection models for automated detection or business rules are developed by

analyzing patterns of behavior patterns and morale of individuals using collected data.
Third, in the response phase, the operational team's strategy for identifying abnormal transactions is implemented as a step to manage abnormal financial transactions that are filtered by analysis and detection. Finally, during the monitoring and auditing phase, unnecessary processes are removed from the information gathering, analysis and response phases to improve FDS [10].
The FDS components proposed in the Technical Guides do not reflect operational factors such as operating elements, data analysts for detection analysis, and fraud case investigators for response. In addition, the effectiveness and performance of the FDS needs to be effectively integrated with system performance and operational strategies.
For successful operation of FDS, activities such as definition of roles and responsibilities for IT departments and business's unique business domain, effective allocation of IT resources and evaluation of investment performance, and risk management and operation process should be established. With the increasing reliance on IT for business in recent years, the need for IT governance has increased in order to improve the effective management and transparency of IT investment costs.
As a framework supporting IT governance, there are COBIT, ITIL, ISO38500, BS25999 and decision model as shown in Table 1. These frameworks can be easily leveraged according to the objectives of the enterprise or organization and the purpose of the IT investment.

Table 1: IT Governance Framework

Division	Frameworks
COBIT	COBIT (Control Objectives for Information and Related Technologies) is a good-practice framework created by international professional association ISACA for information technology (IT) management and IT governance. COBIT provides an implementable "set of controls over information technology and organizes them around a logical framework of IT-related processes and enablers."
ITIL	ITIL describes processes, procedures, tasks, and checklists which are not organization-specific or technology-specific, but can be applied by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.
ISO38500	ISO/IEC 38500 is an international standard for Corporate governance of information technology published jointly by the International Organization for Standardization (ISO) and the International Electro Technical Commission (IEC). It provides a framework for effective governance of IT to assist those at the highest level of organizations to understand and fulfil their legal, regulatory, and ethical obligations in respect of their organizations' use of IT.
BS25999	BS 25999 was BSI's standard in the field of Business Continuity Management (BCM). It was withdrawn in 2012 (part 2) and 2013 (part 1) following the publication of the international standards ISO 22301 - ″Societal Security — Business continuity management systems — Requirements″ and ISO 22313 - ″Societal Security — Business continuity management systems — Guidance″

The purpose of this IT governance is to improve the value of the business and to reduce the cost of controlling and managing performance.

3. Results and Discussion

3.1 Components of FDS

The components of the FDS should be structured appropriately according to the purpose and environment of the financial institution. It is broadly divided into operations that are responsible for data collection, analysis, and investigation.
Unlike traditional IT systems, FDS should regularly analyze the changing patterns of fraud and customer behavior, and provide a method to evaluate the performance of the developed detection model. The evaluation method and the interpretation of the evaluation result can vary greatly depending on the purpose of the FDS operation of the enterprise and the response of the financial institution to the customer.
In addition to data collection, analysis, and operations, we can add data analysts or modelers as components to analyze financial fraud patterns and user usage patterns. Experienced professional researchers can also be seen as a component. And to drive the effective operation of FDS, an enterprise-wide vision, strategy, and reward system are needed to drive the organic collaboration of IT and business teams.

3.2 Location-based FDS Model

Payment methods using mobile are divided into direct payment and remote payment. There is a method of paying directly at a retail store, and a method of paying directly from mobile to mobile. In addition, there are remote payments such as online banking services and money transfer via e-mail.

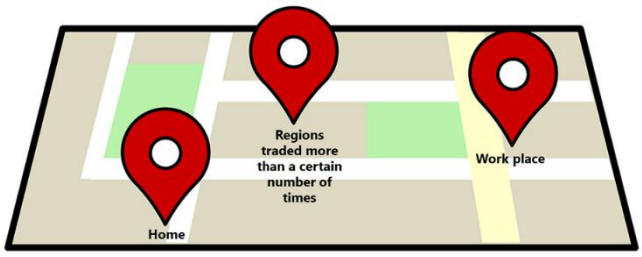

Fig. 5: Concept of Safety Zone

Direct payment is a method of using the POS or mobile terminal, and remote payment use the mobile terminal remotely. Since the direct method makes payment based on a POS or a mobile device, it can extract location information on which the POS is registered or GPS information on the mobile device. On the other hand, the remote payment method can extract the GPS information of the user's mobile device.

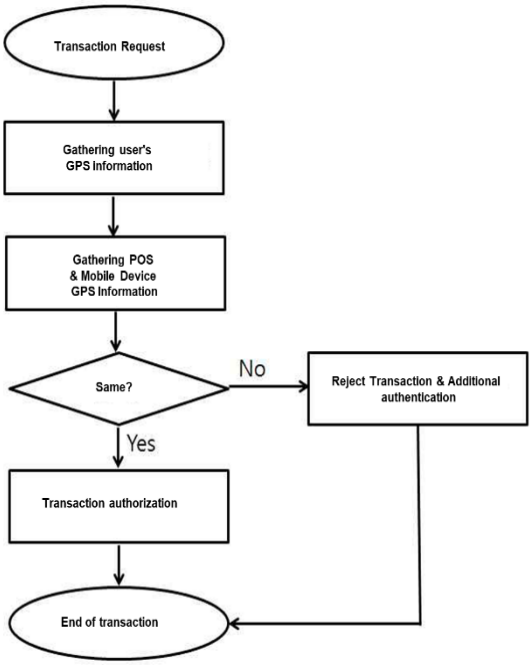

Fig. 6: Algorithm of direct payment method

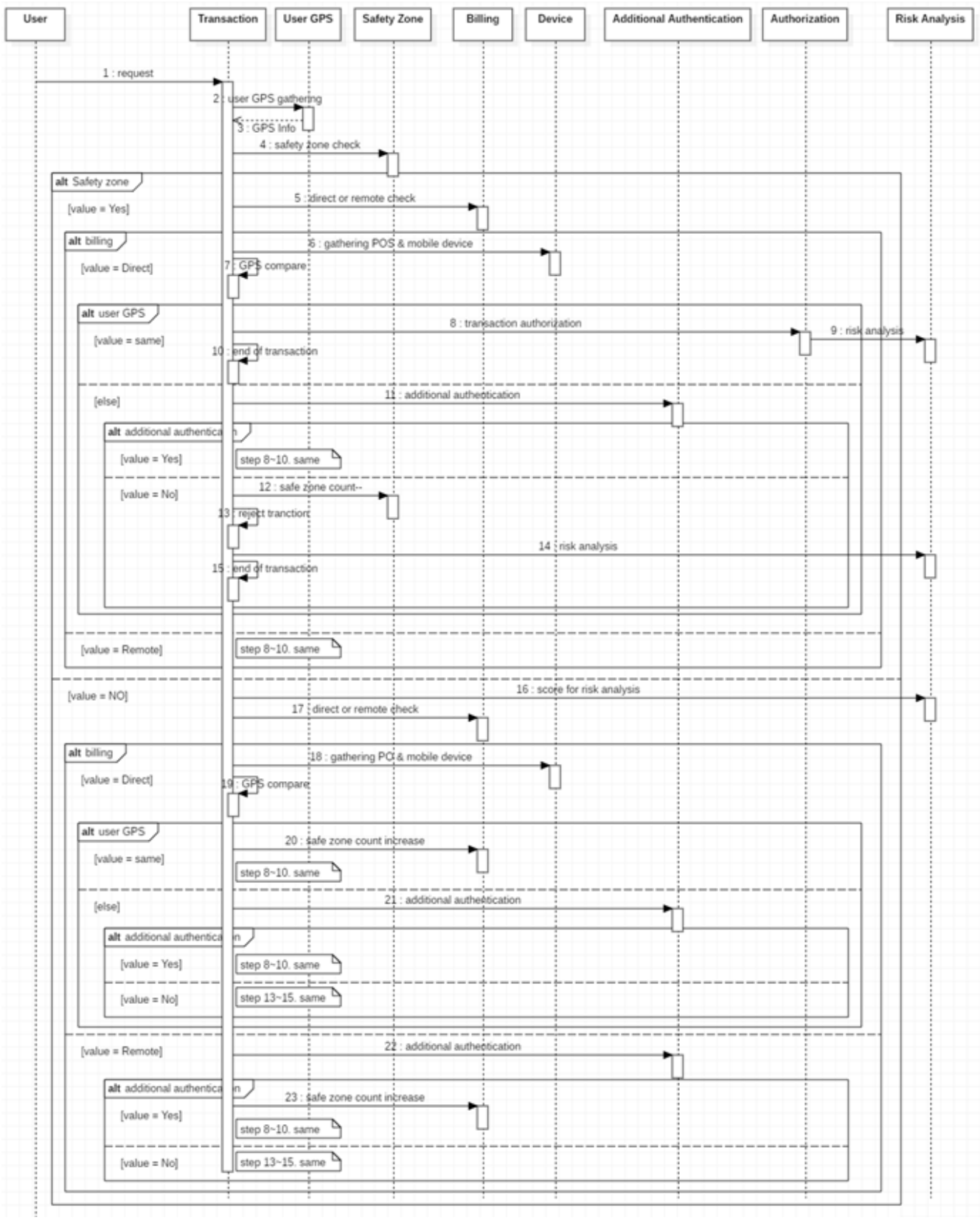

Fig. 5: Sequence Diagram

In the remote payment method, a safety zone is constructed and compared based on the location where the transaction is requested. Safety Zone means the settlement area designated by the user in advance, that is, the user's home address, work address, school address, and so on.

As shown in Fig. 7. We propose the sequence diagram that can be added to existing FDS by integrating remote payment method and direct payment method.

First, when a user requests a transaction, GPS information of the Smartphone is collected and it is compared with a safety zone. If this is within the Safety Zone, check the payment method. If it is a

remote payment transaction, it authorizes the transaction and sends the information to the FDS analysis system.
On the other hand, if the transaction is a direct transaction, the position information of the POS is compared with the GPS information of the user terminal. If they match, the transaction is allowed; otherwise, additional authentication is required.
At this time, if the user presents the additional authentication, the transaction is permitted. If the user can not present the additional authentication, the safety zone count is decreased and the transaction is rejected.
In addition, if an abnormal transaction continues to occur where additional certification is not possible at that location, the Safety Zone Count will decrease and the Safety Zone can be demoted to the Not Safety Zone.
In the second case, the risk analysis score is deducted if not in the Safety Zone. After that, the remote payment method requires additional authentication, and when the authentication is completed, the Safety Zone Count is increased and the transaction is permitted. Because the risk analysis score was deducted from the above, the FDS scores are lower than those in the Safety Zone.
If it is a direct payment method, it collects the location information of the place where the POS is registered or collect GPS information of the terminal. Then compare the collected location information and, if there is a match, the transaction authorization, and If the user has been authenticated, will be allowed to trade, and if not, will reduce the Safety Zone Count.
Transaction permits and transaction denials are scored based on the Safety Zone and used as an indicator of the FDS analysis.

3.3 Considerations for FDS

FDS should be balanced in terms of detection and operating costs. We can detect all fraudulent activities if we conduct a full inspection to detect fraudulent activity.
However, even if it is a whole number survey, if the IT process is not a real-time process but a batch process due to a lack of technical support, the financial company should endure the loss of the event after the fraud. Also, even if the real-time process is operated, it cannot be confirmed that the transaction is fraudulent if the fraud investigation is not conducted for the transaction.
If IT strategy is not balanced with business strategy, it can be concluded that IT technology investment in FDS is not effective.
Therefore, the FDS operational framework includes the data collection from the customer channel integration to the data conversion, which is a component of the FDS, the analysis that proceeds with business rules and modeling, and the operational components from approval strategy to model evaluation should be included. And FDS operations are made through demands, corporate vision and alignment with corporate stakeholders.
In addition, because FDS has various risk factors for privacy and security policy, it is necessary to check business and IT technology through security audit. Therefore, the FDS operational framework requires close cooperation between the FDS operating organization and the IT technical support organization.
The three key elements of the FDS operational framework, 1) collection, 2) analysis and operation of data, 3) security policies and security audits, are as follows.
First, the important point in data collection of the FDS operational framework is the establishment of master data for fraud detection in financial transactions such as ATM, mobile banking, and Internet banking for data collection and integrated FDS operation, and define a database model of fraud for data classification, collection and utilization. The collection of such data can be classified into transaction unit and customer unit, and various data analysis can support effective detection model building. The collection and use of data should be able to respond effectively to business needs and operational strategies, such as approval strategies, i.e. fraud detection through real-time data analysis.
The second is data analysis and operation. Analysis through data collection can be divided into analysis of fraud detection rules for short-term response and modeling for long-term response. The fraud detection rule can be used when a new type of fraud pattern that is difficult to recognize as a fraud behavior in the model is generated, or when damage is expected by credit card or account information leakage. These rule systems can be supported through the introduction of Rule Base Management (RBMS), which enables rule development and application to be managed in real time or directly by the business. In the absence of such an RBMS, the analytical team creates a fraud detection rule and applies it to the system. The modeling task should support the overlapping use of models using various technologies such as fraud patterns and personal history profiles, and enterprise-wide support for periodic model development is required.
Strategies should be established on how to investigate fraud cases detected by models and rules for fraud detection from an operational perspective. Through the investigation strategy, it is possible to check the case detected directly with all customers, and the non-critical cases can be confirmed through texts or messages. It is also possible to reject the approval at the time of the financial transaction through the approval strategy, or to temporarily stop the transaction through the five-minute hold time, thereby establishing various strategies to prevent further attempts to the criminals. Establishment of approval and operational strategies should be established through objective performance evaluation of rules and models.
Third, security policy and security audit considerations. FDS develops models through various financial transaction information and personal information, and conducts fraud detection through the developed model. At this time, FDS should be operated by aligning with the company's security policy in order to protect personal information and leakage of financial transaction information during data analysis. This is because large amounts of financial transactions and customer information can be handled through data analysis experts and third parties to develop detection models.
To prevent leakage of personal information and financial transactions, modeling and rule creation should be supported so that data cannot be deduced from an individual using data analysis and modeling using anonymization techniques. And if modeling is going on through a third party, we should be careful to use and approve non-authorized users of our data.
It is also necessary to apply technical and managerial security measures to protect personal information so that investigators do not directly identify or process customer information.

4. Conclusions

When building and operating FDS in financial institutions such as insurance and banks, the most important thing is maximizing profit through customer satisfaction. Until now, we have limited our customers' use of financial services or installed various security software in order to increase fraud detection rate and minimize accident loss. However, this approach has made it difficult for customers to make financial transactions and to reduce the convenience of financial transactions. However, with the advent of Fintech recently, customers' demand for the simple payment market is growing.
This study suggests a method to judge the abnormal transaction based on the user 's location. This research is expected to be an operation model for Fintech based FDS that enables safe transactions without sacrificing the convenience of customers.

References

[1] Gomber, P., Kauffman, J., Parker, C., Weber, W., On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. Journal of Management Information Systems, Vol. 35 Issue 1 (2004), 220-265.

[2] Aisha, A., Mohd, M., Anazida, Z., Fraud detection system: A survey. Journal of Network and Computer Applications., 68 (2016), 90-113.
[3] Jungoh, P., Byungwook, J., A Study on Authentication Method for Secure Payment in Fintech Environment. The Journal of the Institute of Internet, Broadcasting and Communication (IIBC), Vol. 15, No. 4 (2015), 25-31.
[4] Gozman, D., Liebenau, J., Mangan, J., The Innovation Mechanisms of Fintech Start-Ups: Insights from SWIFT's Innotribe Competition. Journal of Management Information Systems, Vol. 35 Issue 1 (2018), 145-179.
[5] Dhar, V., Stein, M., FinTech Platforms and Strategy: Integrating trust and automation in finance. Communications of the ACM, Vol. 60 Issue 10 (2017), 32-35.
[6] Mooney, W. Jr., Fintech and Secured Transactions Systems of the Future. Law and Contemporary Problems, Vol. 81, Issue 1 (2018), 1-20.
[7] Jayabrabu, R., Saravanan, V., Tamilselvi, J.J., A framework for fraud detection system in automated data mining using intelligent agent for better decision making process. 2014 International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), Mar (2014), 1-8.
[8] GeumYeon J., InSeok K., A Study on the Institutional Limitations and Improvements for Electronic Financial Fraud Detection. The Journal of the Institute of Internet, Broadcasting and Communication (IIBC), Vol. 16, No. 6 (2016), 255-264.
[9] Budi, S., Julita, H., Bambang, R., Laksono, T., System for detection of national healthcare insurance fraud based on computer application. Public Health of Indonesia, Vol 4, Issue 2 (2018), 46-56.
[10] TaeEun, K., JungMi, L., SeonHo, H., GwangYong G., A Study of Finance Fraud Detection System Operation Framework. Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, Vol.5, No.4 (2015), 9-17.