International Journal of u- and e- Service, Science and Technology
Vol.9, No. 9 (2016), pp.213-220
http://dx.doi.org/10.14257/ijunesst.2016.9.9.21

GPS-Based Fraud Detection Model

Min-gyu Lee[1], Hyo-jung Sohn[2], Baek-min Seong[3] and Jong-bae Kim[4*]

[1,2,3,4]*Graduate School of Software, Soongsil University, Seoul 156-743, Korea*
[1]*marse101@naver.com,*[2]*hyojung.sohn@gmail.com,*
[3]*feeling127@naver.com,*[4]*kjb123@ssu.ac.kr*

Abstract

As smartphones rapidly spread in the society, the number of security accidents is also dramatically increasing. Particularly, the rapid growth of FinTech provides users with a convenient payment method. FinTech, which is a combination of 'Financial' and 'Technique', means a technology that handles financial transactions based on IT technology. Users can make a payment anytime and anywhere by using FinTech and smartphone. Accordingly, since it has become easier to make a payment, security accidents related to financial transaction are increasing. Financial security accidents related to the use of smartphones can take place in various ways such as stealing, hacking and fraud, and the amount of damage and loss is astronomical. Therefore, this study aims to propose FDS (Fraud Detection System) using GPS information provided as default by terminals such as smartphone.

Keywords*: Smartphone, Fraud Detection, Global Positioning System*

1. Introduction

FDS is more necessary under the environment in which a smartphone is used as a means of payment. Moreover, as the financial payment system is becoming more convenient, in order to use the newly developed FinTech in a more stable manner, new types of FDS algorithms or factors are more needed than ever. FinTech, which is a combination of 'Financial' and 'Technique', means a technology that handles financial transactions based on IT technology [1]. FinTech has such merits as enabling its users to get loan, transfer money and purchase products in an easier way. However, the convenience is accompanied with security threats.

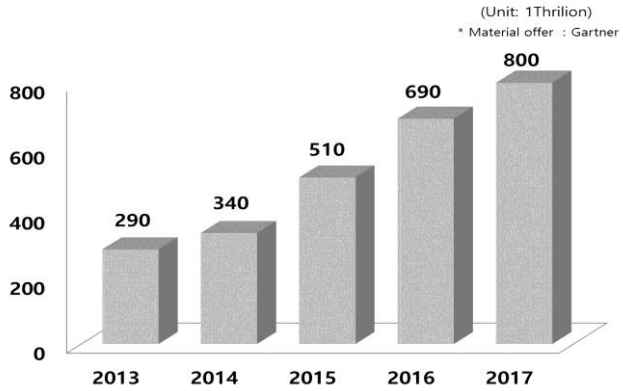


Figure 1. World Market Size of Mobile Payment

* Corresponding Author

ISSN: 2005-4246 IJUNESST

Figure 1, shows the estimated world market size of mobile payment. As mobile terminals are used more widely, mobile payment market rapidly grows at a proportionate rate.

According to Nielsen, a US market research company, the penetration rate of smartphones in the US in 2014 was 71% [2]. It means almost all of Americans possess smartphones when the population of early childhood and old ages are excluded. As FinTech develops every day, new technologies that help its users make a payment through a smartphone are pouring out into the market. In the meantime, RSA reported that the amount of illegitimate use of credit card was USD 3.2 trillion in 2014 only, and it forecasted that the amount would increase up to USD 7.5 trillion in 2018, if FinTech penetrated even further into the market [3].

Therefore, there exists FDS (Fraud Detection System) to prevent such illegal use at the level of FSP (Fintech Service Provider).

FDS is a system to blow the abnormal financial transactions through detecting the suspicious transactions based on the comprehensive analysis on the information of the terminal use for electronic financial transactions, its aces information, details of the transaction, payment location, etc. FDS enables to block or request additional authentication before payment completes even when user's financial information is exposed to illegal use.

In existing FDS, there is no model using GPS information of user's terminal to detect frauds. For the reason, this study suggests a model that can utilize user's terminal GPS information and increase the accuracy of detection of frauds.

2. Related Works

2.1. The Elements to Detect Illegal Smartphone-Based Transactions

Table 1. Elements to Detect Illegal Smartphone-Based Transactions

Type of Mobile OS	The Elements to Detect Illegal Smartphone-based Transactions
IOS	UUID, System Version, Device Name
Android	Electronic Serial Number, Mobile Identification Number, USIM Serial Number, Wi-Fi Information

If the elements to detect illegal smartphone-based transactions are classified based on OS, the elements like UUID (Unique User Identifier), iOS system version and device name may be found on iOS and ESN (Electronic Serial Number), MIN (Mobile Identification Number), USIM Serial Number and Wi-Fi information on Android.

2.2. FDS (Fraud Detection System)

Fraud Detection System analyzes user's media and transaction information and uses misuse and anomaly detection techniques to detect illegal use.

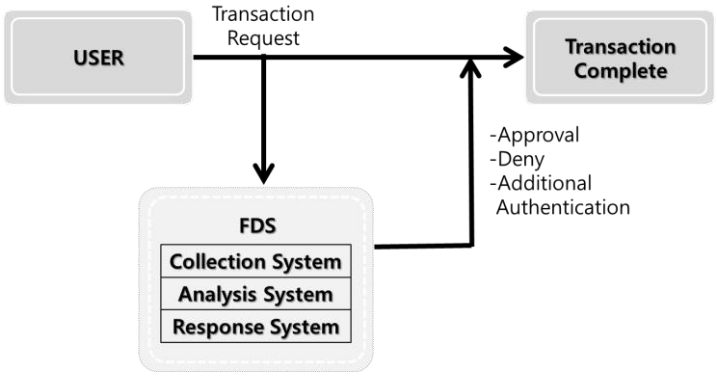


Figure 2. FDS System

According to Figure 2, when a user starts a transaction, FDS system analyzes media environment information, transaction information and accident pattern information. When a transaction is proven to be an anomaly, it requests additional authentication or reject the transaction. Approval is granted only when there is no anomaly in the transaction. Even though there is an existing FDS model that collects the location information of the retail stores where the payments are made and uses such information for analytical purposes, but no FDS model uses the GPS information of user's terminal to detect suspicious transactions.

2.3. Classification of FDS

FDS (Fraud Detection System) includes the misuse and anomaly detection model. They are designed based on the concept of Intrusion Detection System (IDS) that analyzes packets on the network to detect intrusion [5-6].

2.3.1. Misuse Detection Model*:* This model analyzes the patterns of past illegal behaviors and matches the current pattern with the past ones to detect fraudulent acts. As misuse detection model depends on the past accident information, the accuracy improves as it has more information of the past transactions. However, it cannot detect a newly discovered type of fraud [4].

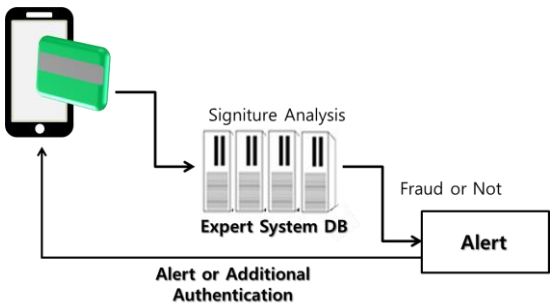


Figure 3. Misuse Detection Model

2.3.2. Anomaly Detection Model: This model analyzes weeks' or months' worth of user's data as a reference and detects the cases of dramatic change or with statistically low possibility. It is possible to detect unknown fraudulent acts in advance. However, it is difficult for the model to expect normal behaviors, and the model shows low accuracy. Furthermore, it takes a long time to analyze a variety of information that is collected.

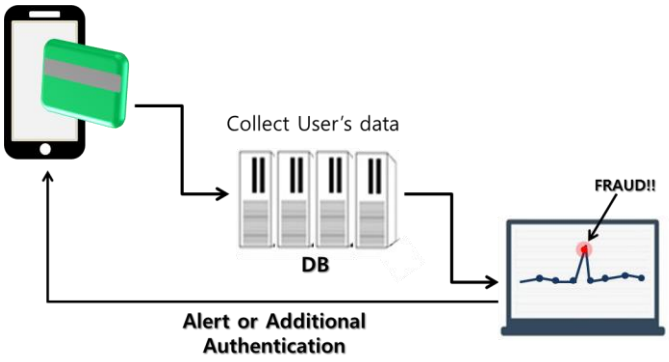


Figure 4. Anomaly Detection Model

2.4. FinTech

The appearance of FinTech brought many changes to the existing financial environment. FinTech started to function as an intermediary in the environment where there was unilateral communication between the financial institutions and customers. Figure 5, shows the environment where FSP is located in the middle to enable the user to make the payment in a more easy and simple manner, which is different from the conventional way of transaction between users and financial institutions.

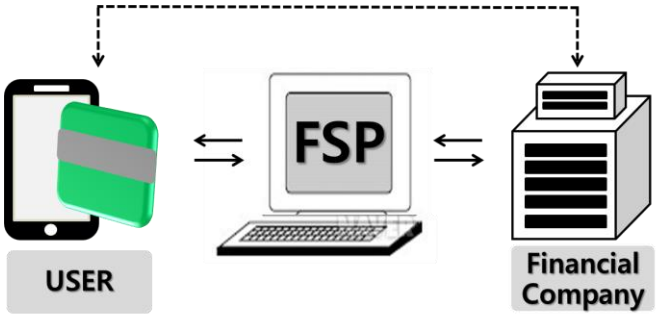


Figure 5. Payment Environment Applied with FinTech

3. Proposed FDS Model

3.1. Classification of Payment Methods

The mobile FinTech payment methods are divided into direct and remote payment. Direct payment may be made in retail stores or between mobile devices. Remote payment may be made in online banking, fund transfer through e-mail, *etc.*, First, direct payment is a payment directly made at POS or mobile terminal through a mobile terminal. Remote payment is to perform financial transaction in distance through a mobile terminal.

Because direct payment takes place at POS or through a mobile device, location information of POS or GPS information of a mobile device by which payment is made can be collected. In addition, remote payment can collect GPS information of user's mobile device.

3.2. Use of User's GPS Information in Remote Payment Method

The remote payment method compares the data after establishing the "Safety Zone" based on the location where the transaction is requested. Safety zone means a safe place that a user defines in advance for a safe payment. For example, safety zone is established

based on the address of a user's home, workplace, and/or school. And when payment occurs in a place outside the safety zone, the location is weighted in score and marked on the map. When a certain number of transactions occur in a place outside the safety zone, it is designated as another safety zone. This method is helpful for safe payment because the locations where payments are frequently made are displayed on the map.

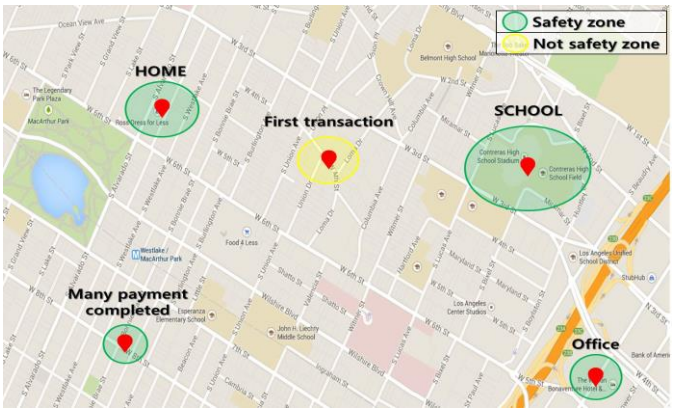


Figure 6. Example of Safety Zone

3.3. Comparison of GPS Information in Direct Payment Method

The direct payment method compares the user's GPS information, location of the store where the payment is made, and GPS information of the mobile device used for payment.

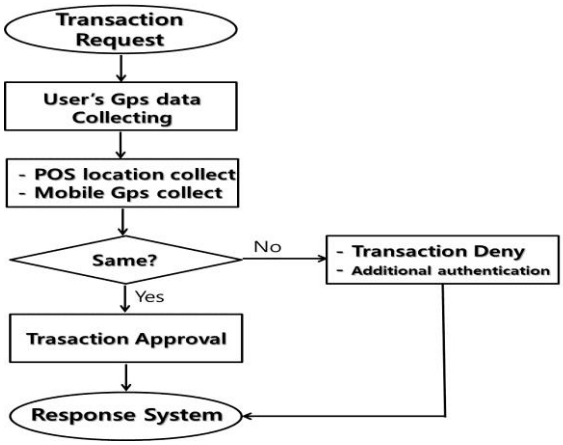


Figure 7. Direct Payment Algorithm to Compare GPS Information

Figure 7, shows the direct payment algorithm to make the comparison on the user's GPS information with the other locations. When a user requests a transaction, the GPS information of the user's mobile terminal, location information of POS at which payment is made or GPS information of the other mobile devices are collected. When the user's GPS information matches with that (location information) of POS or the other mobile through which the payment is made, the transaction is approved. If not, the transaction is rejected, or additional authentication is required.

3.4. Integrated Algorithm

This Section proposes an algorithm that can be added to the existing FDS through combining the aforementioned remote and direct payment method. First, the proposed

algorithm collects GPS information of the user's smartphone when he (she) requests a transaction and determines whether he (she) is within the pre-defined safety zone.

First, in case the request is made within the safety zone, the proposed algorithm confirms the method of payment. If it is a remote payment, it jumps to the transaction approval phase, which is based on the premise that there is no abnormality found in the transaction, and the data is transmitted to FDS analysis system. Meanwhile, if it is direct payment transaction, the location information of POS and GPS information of the user's terminal are collected and compared. In case the two matches, the transaction is approved. If not, extra authentication is requested. In this case, if the user successfully goes through the process, the transaction is approved, while the transaction is rejected, and the scope of Safety Zone is decreased in case the process fails. "Safety Zone Count" indicates the fact that in case multiple payment transactions are made through extra authentication in a place not registered as a Safety Zone, the status of the place should be elevated to that of the Safety Zone. Likewise, in case abnormal transactions where the user fails to complete the extra authentication process repeatedly occur in a certain place, the "Safety Zone Count" decreases to demote the previous Safety Zone to the status of "Not Safety Zone".

Second, in case the request is made outside the safety zone, the risk level analysis point first decreases. Next, in case it is a remote payment, extra authentication is requested. When the authentication is completed, the Safety Zone Count increases, and the transaction is approved. When approval is granted to the transaction, a score lower than the one that could be given for the approved transaction that occur inside the Safety Zone is registered to FDS because the risk level analysis point has decreased. In the case of direct payment, the location information of POS or GPS information of the user's terminal are collected and compared. In case the two matches, the transaction is approved. If not, extra authentication is requested. In this case, if the user successfully goes through the process, the transaction is approved, while the transaction is rejected, and the scope of Safety Zone is decreased in case the process fails. Based on the scope of Safety Zone, score will be given based on transaction approval and rejection and be used as an indicator for the analysis on FDS.

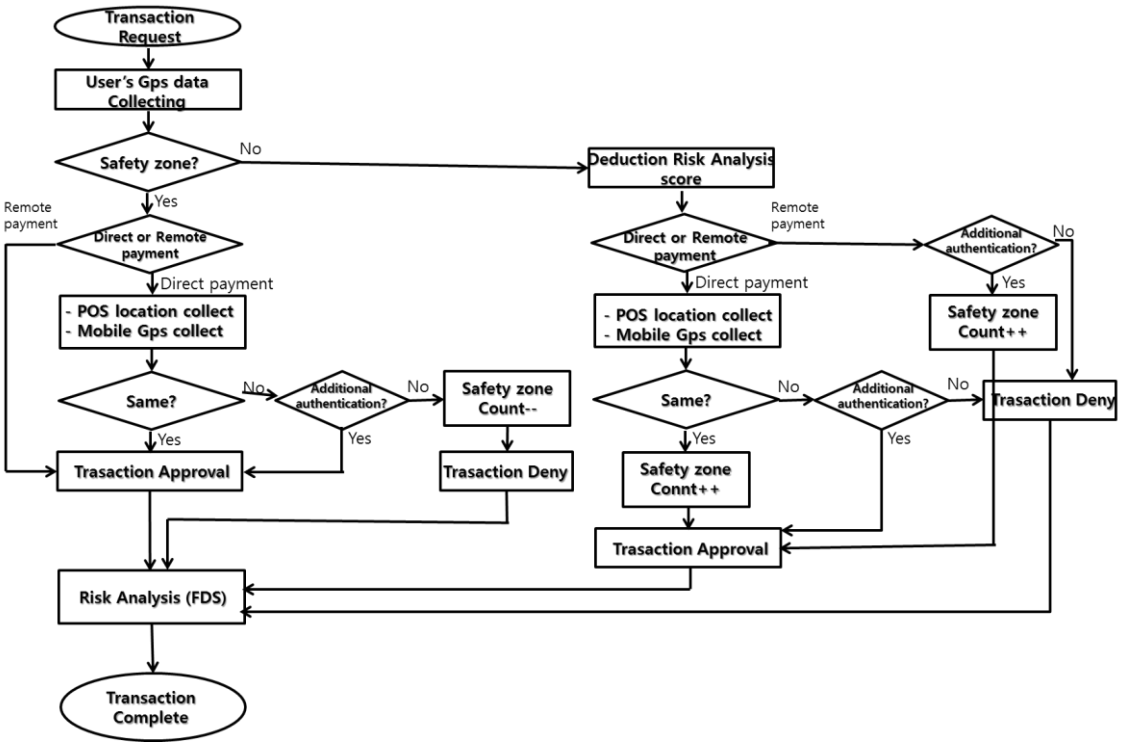


Figure 8. Integrated Algorithm

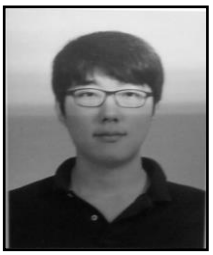
4. Conclusion

This study proposed a model that can more accurately detect abnormalities through applying the GPS information to FDS under the FinTech environment where the mobile terminals are used. The study divided user's terminal-based payment methods into direct and remote payment and suggested methods to use GPS information and to detect fraud for each of them. The future research is planned to propose a scoring methodology that applies the above model to FDS.

References

[1] http://ko.wikipedia.org/wiki/%ED%95%80%ED%85%8C%ED%81%AC, May 23.
[2] http://www.nielsen.com/us/en/insights/news/2014/mobile-millennials-over-85-percent-of-generation-y-owns-smartphones.html, Sept., 5.
[3] RSA, CYBERCRIME ROUNDUP,**(2014)**.
[4] http://news.mt.co.kr/mtview.php?no=2014092511337113560,Sept,.8.
[5] J. Akhilomen, "Data Mining Application for Cyber Credit-card Fraud Detection System", Proceedings of the World Congress on Engineering, (2013) Vol III, WCE, London, U.K. **(2013)** July 3-5.
[6] P. Richhariya, P. K. Singh and E. Duneja, "A Survey on Financial Fraud Detection Methodologies", International Journal of Commerce, Business and Management, vol. 1, no. 1, **(2012)**.

Authors



Min-Gyu Lee, received his bachelor's degree of Information and Telecommunication in Dongguk University (2014). And he is studying his master's degree in Software Engineering in the Graduate School of Soongsil University, Seoul. His current research interests include Open source software and Security.

Hyo-Jung Sohn, received her bachelor's degree of Business Administration in Soongsil University in Seoul (2006). And she is studying her master's degree in software engineering in the Graduate School of Soongsil University in Seoul. Her current research interests include pen source development and management information system.

Baek-Min Seong received his bachelor's degree of Business Administration in Soongsil University, Seoul (2014). And he is studying his master's degree in Software Engineering in the Graduate School of Soongsil University, Seoul. His current research interests include database.

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