GPS를 적용한 이상금융거래탐지시스템 모델

이민규* · 손효정** · 성백민*** · 김종배○

*,**,***,○숭실대학교 SW특성화대학원

E-mail : marse101@naver.com*,hyojung.sohn@gmail.com**,

feeling127@naver.com***,kjb123@ssu.ac.kr○

요 약

스마트폰의 확산으로 금융관련 결제는 어디서나 가능하게 되었기에 편리함이 증가하였다. 하지만, 위와 같은 편리함과 동시에 사용자의 단말이 해커의 공격에 취약하거나 분실할 경우 심각한 문제가 된다. 따라서, 위와 같은 부정행위가 있을 경우 이를 자동으로 탐지하는 시스템이 필요하다. 그러므로, 본 논문은 이러한 문제점을 고려하여 스마트폰을 이용한 금융업무를 처리할때 GPS정보를 적용한 이상금융거래탐지시스템(Fraud Detection System) 모델을 제안한다.

Ⅰ. 서 론

2014년 미국 시장조사기관 Nielson에 따르면 스마트폰의 보급률은 미국인의 71% 라고 보고하였다[1]. 유아기,노년기 인구를 제외 한다면 인구 대부분이 스마트폰을 보유하고 있다. 핀테크 기술이 날로 발전하여 스마트폰을 이용하여 결제할 수 있는 기술들이 쏟아져 나오고 있다. 한편, RSA는 2014년 한해 미국에서 신용카드 부정사용 금액이 3조 2000억이라 보고했고 핀테크가 지속적으로 확산되면 2018년도에는 7조 5천억 까지 증가할 것으로 전망했다[2]. 따라서 이러한 부정사용을 막기 위해서 핀테크 서비스 제공자(Fintech Service Provider)(FSP)단 에서 부정사용을 막기위한 이상거래탐지시스템이 필요하다.

이상금융거래탐지시스템이란 전자금융거래에 사용되는 단말기의 정보, 접속정보, 거래내용, 결제 위치 등을 종합적으로 분석하여 의심되는 거래를 탐지하여 이상금융거래를 차단하는 시스템이다. FDS를 활용하면 이용자의 금융정보가 부정사용에 노출되어도 결제전에 차단이나 추가인증을 가능케 한다.

기존의 FDS에서 결제된 장소의 위치를 수집하여 분석에 활용한 모델도 있지만 사용자 단말의 GPS정보를 활용하여 이상거래탐지를 하는 모델은 존재하지가 않는다. 따라서 본 연구에서는 사용자 단말의 GPS정보를 활용하여 더욱 이상거래탐지 정확도를 높일 수 있는 모델을 제안한다.

Ⅱ. 기존의 이상금융거래탐지시스템

기존의 이상거래 탐지시스템은 이용자의 매체정보, 거래내역 등을 분석해서 오용탐지, 이상탐지 기법으로 부정사용을 탐지 하였다[3][4]. 그림 1을 보면 이용자가 거래트랜잭션을 발생 시키면 FDS가 매체환경 정보, 거래정보, 사고유형정보등을 분석하여 트랜잭션에 이상이 발견되면 추가인증을 하거나 해당거래를 거부하고 이상이 없다면 허가하여 거래가 완료된다. 기존의 FDS에서 결제된 소매점의 위치를 수집하여 분석에 활용한 모델도 있지만 사용자 단말의 GPS정보를 활용하여 이상거래탐지를 하는 모델은 존재하지가 않는다.

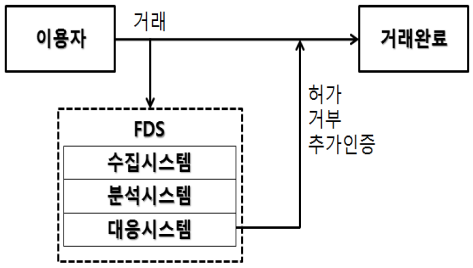

그림 1. 이상금융거래탐지시스템 개념도

Ⅲ. 제안하는 이상금융거래탐지시스템 모델

3.1 결제방식 분류

모바일을 활용한 결제 방법으로는 직접결제와 원격 결제로 나뉘어 진다. 소매점에서 직접결제하는 방법이 있고, 모바일에서 모바일 간에 직접결제하는 방법이 있다. 그리고, 온라인 금융업무, 이메일을 통한 금전전송등 원격결제를 하는 방법이

있다. 먼저, 직접결제란 모바일단말을 이용해서 POS나 모바일 단말에 직접결제 하는 방법이고. 원격 결제란 모바일 단말을 이용해서 원격으로 금융업무를 수행하는 방법을 말한다.

직접결제 방식은 POS나 모바일기기등을 대상으로 결제 하기 때문에 POS가 등록된 위치정보나 결제된 모바일기기의 GPS정보를 추출할 수가 있다. 그리고, 원격결제방식은 사용자 모바일기기의 GPS정보를 추출 할 수가 있다.

3.2 원격결제방식에서 사용자 GPS 정보 활용

원격결제방식에서는 거래가 요청된 위치를 기반으로 Safety Zone을 구축 하고 이를 비교한다. Safety Zone이란 사용자가 미리 지정한 결제하는데 안전한 지역, 예를 들어서 사용자의 집주소, 근무지주소, 학교주소등을 기반으로 결제하는데 안전한 지역을 먼저 구축한다. 그리고, 이 지역

외에서 결제시도가 이루어진다면 점수화에 차등을 두어 반영하고 지도에

표시하여 일정횟수이상 그 지역에서 거래가 발생하였다면 Safety Zone으로 승격시킨다. 이러한 방법은 사용자가 주로 결제를 이용하는 위치를 지도상에 표시할 수 있기 때문에 안전한 결제에 도움이 된다.

그림 2. Safety Zone 예시

3.3 직접결제방식에서 GPS정보 비교

직접결제방식에서는 사용자의 GPS정보와 결제된 소매점의 위치, 결제된 모바일 기기의 GPS정보를 비교한다.

그림 3은 직접결제방식에서 사용자 GPS정보와 비교하는 알고리즘 이다. 사용자가 거래요청을 하면 트랜잭션과 함께 사용자 단말의 GPS정보를 수집하고 결제되는 POS가 등록되어 있는 위치 혹은 결제되는 상대 모바일 GPS정보를 수집한다. 그리고 사용자 GPS정보와 POS위치 혹은 결제 되는 모바일 단말의 위치가 일치한다면 거래가 허가되

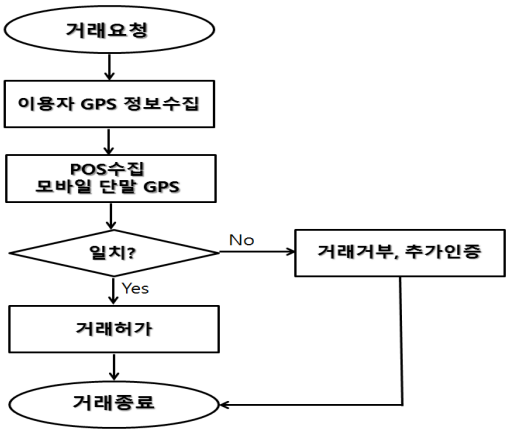

그림 3. 직접결제방식에서 GPS정보를 비교하는 알고리즘

고 일치하지 않는다면 거래가 거부되거나 추가인증을 한다.

3.4 통합 알고리즘

본 절에서는 앞에서 설명한 원격결제방식과 직접결제방식을 통합하여 기존의 FDS에 추가할 수 있는 그림 4와 같이 통합알고리즘을 제시한다. 먼저 사용자가 거래요청을 한다면 사용자 스마트폰의 GPS정보를 수집하고 Safety zone 내에 있는지 비교한다. Safety

zone내에 있다면 결제방식을 확인하고 원격결제라면 거래에 이상이 없다는 거래허가 시그널을 FDS분석시스템에 전송한다. 직접결제방식이라면 POS가 등록된 곳의 위치정보를 수집하거나 모바일에서 모바일간의 결제라면 상대모바일 단말의 GPS정보를 수집한다. 그 다음 수집된 위치정보를 비교하고 일치한다면 거래허가를 일치하지 않는다면 추가인증을 받도록 하고 인증을 하였다면 거래허가를, 추가인증을 하지 않는다면 Safety zone Count를 감소시킨다. Safety Zone Count란 Safety zone이 아닌 곳에서 일정 횟수 이상 성공적으로 거래를 마쳤다면 Safety zone으로 승격시킬수 있도록 하기 위해 고안하였다. 하지만 Safety zone으로 승격된 장소도 이상행위가 많이 감지 된다면 Safety Zone자격을 박탈 당할 수 있다. Safety Zone을 기준으로 거래허가와 거래거부는 각각 점수화 되어 FDS에서 분석의 지표로 활용된다.

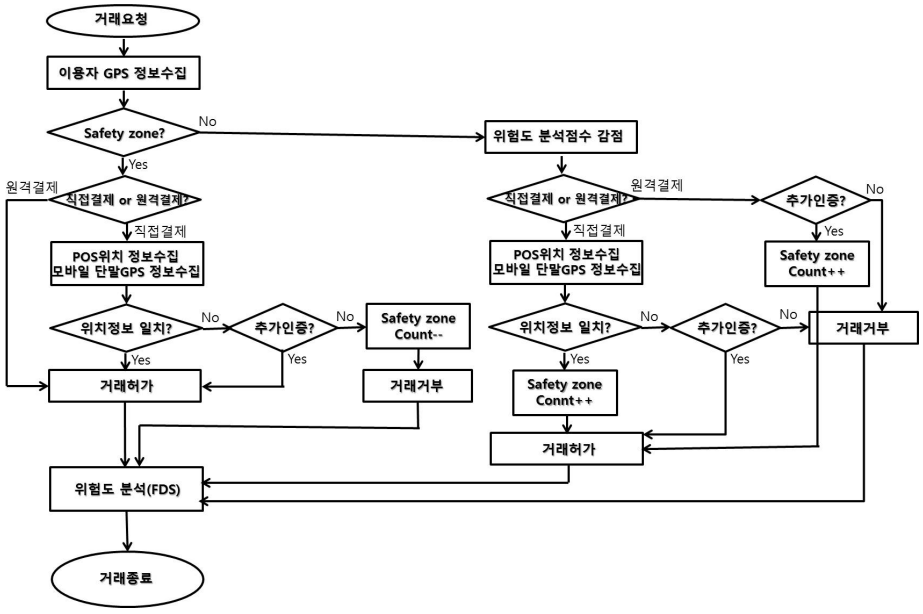

그림 4. 통합 알고리즘

Ⅳ. 결 론

본 논문에서는 모바일 단말을 사용하는 핀테크 환경에서 GPS정보를 FDS에 적용하여 이상탐지를 더욱 정확하게 판별할 수 있는 모델을 제시하였다. 사용자 단말의 결제 방식을 직접결제와 원격결제 두가지 방식으로 나눠서 각각 GPS정보를 활용할 수 있는 방법과 이상탐지를 위한 방법을 제시하였다. 향후 논문계획은 제안된 모델을 FDS에 적용 시키기 위한 스코어링 방법을 제시하기 위한 연구를 진행할 계획이다.

참고문헌

[1] http://www.nielsen.com/us/en/insights/news/2014/mobile-millennials-over-85-percent-of-generation-y-owns-smartphones.html
[2] RSA, 2014 CYBERCRIME ROUNDUP
[3] John Akhilomen, Data Mining Application for Cyber Credit-card Fraud Detection System, Proceedings of the World Congress on Engineering, 2013 Vol III, WCE 2013, July 3 - 5, 2013, London, U.K.
[4] Pankaj Richhariya, Dr. Prashant K Singh ,Endu Duneja A Survey on Financial Fraud Detection Methodologies, International Journal of Commerce, Business and Management ,Vol. 1, No.1, 2012