The Journal of the Convergence on Culture Technology (JCCT)
Vol. 6, No. 1, pp.455-461, February 29, 2020. pISSN 2384-0358, eISSN 2384-0366

http://dx.doi.org/10.17703/JCCT.2020.6.1.455
JCCT 2020-2-56

전자지불거래에서 상대위치와 연동한 도용 위험성 산출방법

Relative Location based Risk Calculation to Prevent Identity Theft in Electronic Payment Systems

서효중*, 황호영**

Hyo-Joong Suh*, Hoyoung Hwang**

요 약 인터넷뱅킹과 전자지불거래는 인터넷을 이용한 개인의 경제적 행동 중 매우 중요하고 민감한 내용이다. 핀테크와 관련한 해킹 및 도용이 발생할 경우 사용자의 직접적 금전피해로 이어지므로 이러한 사고를 막기 위해 적극적 방법들이 사용되고 있으며, 특히 이상금융거래탐지시스템(FDS)은 전자지불거래시의 위험률을 도출하고 도용을 탐지한다. 전자지불과 같은 상거래의 경우 스마트폰의 상태, 물품과 매장의 종류, 구매자의 위치 등 프로파일링에 따라 위험률을 도출하고 있다. 본 논문에서는 이러한 전자지불거래에 있어서 기존의 물리적 위치에 의한 것이 아닌 사용자의 상대적 위치에 의한 위험률 도출 방법을 제안하고자 한다. GPS 주소나 IP 경로주소와 같은 정보를 활용하는 절대위치와 달리, 상대위치는 무선랜 환경을 감지하여 무선 AP의 ID 및 MAC 주소를 이용한 각 개인의 상대위치 정보를 활용하며, 각 개인의 특성을 감안한 상대적 디지털 환경을 누적 감지하는 방법을 통해 전자지불거래를 검증하여 위험률을 도출하는 방법이다. 절대위치의 경우 국적이나 주소 등의 정적 데이터 수집을 통하여 아이디를 도용할 수 있는 약점이 있는 반면, 상대위치의 경우 연관된 디지털 정보의 모사가 쉽지 않아 이로 인한 보안상의 이득을 얻게 된다.

주요어 : 인터넷뱅킹, 전자지불, 핀테크, 상대위치, 이상금융거래탐지시스템

Abstract Electronic payment system using Internet banking is a very important application for users of e-commerce environment. With rapidly growing use of fintech applications, the risk and damage caused by malicious hacking or identity theft are getting significant. To prevent the damage, fraud detection system (FDS) calculates the risk of the electronic payment transactions using user profiles including types of goods, device status, user location, and so on. In this paper, we propose a new risk calculation method using relative location of users such as SSID of wireless LAN AP and MAC address. Those relative location information are more difficult to imitate or copy compared with conventional physical location information like nation, GPS coordinates, or IP address. The new method using relative location and cumulative user characteristics will enable stronger risk calculation function to FDS and thus give enhanced security to electronic payment systems.

Key words : Internet banking, electronic payment, fintech, relative location, FDS

*정회원, 가톨릭대학교 컴퓨터정보학부 교수 (제1저자)
**정회원, 한성대학교 컴퓨터공학부 교수 (교신저자)
접수일: 2019년 12월 29일, 수정완료일: 2020년 01월 16일
게재확정일: 2020년 01월 24일

Received: December 29, 2019 / Revised: January 16, 2020
Accepted: January 24, 2020
*Corresponding Author: hyhwang@hansung.ac.kr
Dept. of Computer Engineering , Hansung Univ, Korea

Ⅰ. 서 론

데이터통신이 원활해지던 1995년 인터넷뱅킹이 시작된 이후로, 인터넷을 이용한 금융 및 지불거래는 그 효율성과 신속함으로 인해 널리 보편화되었다. 하지만 공중망을 이용하는 인터넷의 특성상 데이터 경로에서의 해킹이나 스니핑의 위험은 피할 수 없었고, 이는 곧 인터넷뱅킹 금융 사고로 현실화되었다. 이러한 위험을 줄이기 위해 인터넷뱅킹에는 암호화, 보안카드인증, 본인인증 등의 보안검증을 포함하게 되었다[1]. 인터넷뱅킹은 상거래 금액과 건수에 있어서 기존의 금융거래와 다른 특성을 나타나게 되는데, 실제로 금융기관을 이루어지는 방문 거래에 대비하여 상대적으로 적은 금액, 그리고 많은 건수를 나타내고 있다. 이러한 특성은 PC에 기반한 지불거래 건수 및 평균금액과 스마트폰에 기반한 지불거래 건수 및 건당 금액에서 공통적으로 나타나는데, 그중에서도 발생 건수는 점차 PC 기반 뱅킹으로부터 스마트폰 기반 뱅킹으로 이동하고 있다. 각 입출금 거래의 총 건수와 거래 당 평균 금액에 대한 경로별 비율은 다음 <표 1>과 같으며, 건당 금액간의 상관관계는 <표 2>와 같이 나타나고 있다[2].

표 1. 입출금 경로별 지불거래 건수 비율의 변화 (%)
Table 1. Proportion trend according to payment methods (%)

	창구	CD/ATM	텔레뱅킹	인터넷뱅킹	전체
2017년 6월	10.6	37.8	10.5	41.1	100
2017년 12월	10.0	34.7	9.9	45.5	100
2018년 6월	8.8	34.3	7.5	49.4	100
2018년 12월	8.8	30.2	7.9	53.2	100
2019년 6월	**7.7**	**28.9**	**6.8**	**56.6**	**100**

표 2. 장치에 따른 거래의 건수와 금액의 상관관계
Table 2. The relation between the number and the amount among payment methods

	창구대면거래	PC기반	스마트폰
거래건수	적다	중간	많다
건당 금액	높다	중간	낮다

결과적으로 창구대면거래의 경로인 은행 영업소는 급격히 줄어들고 있으며, 이와 상반되게 금융 기업의 인터넷 기반 거래의 인프라는 급격히 확충되고 있다. 이에 더불어 스마트폰의 포화된 보급 과 더불어 인터넷뱅킹 중 스마트폰을 이용한 비대면거래 건수는 더욱 급격히 증가하고 있으며, 스마트폰은 개인의 다양한 앱 사용과 더불어 뱅킹 겸용으로도 이용되기에 취약한 보안성에 대한 보완이 더욱 요구되고 있다. 다음 <표 3>은 2018년 보고된 인터넷뱅킹 및 이 중에서 스마트폰 뱅킹이 차지하는 건수와 금액 정도를 나타낸 현황이다[2]. 나타난 바와 같이 개인거래의 특성상 스마트폰을 이용한 모바일뱅킹은 건수에서는 다수를 차지하고 있으나, 건당 금액은 훨씬 낮은 비율로 나타남을 알 수 있다. 2019년 상반기의 경우, 건수에서는 인터넷 및 모바일뱅킹이 차지하는 비중이 전체의 61.8%에 이르나 금액에서는 12.7%의 비중을 보이고 있다.

표 3. 일평균 인터넷뱅킹 서비스 이용 실적 (천건, 십억, %)
Table 3. The numbers of daily Internet banking service (thousand, billion, %)

		2017		2018		2019
		上	下	上	下	上
이용건수	인터넷뱅킹	93,993	95,840	112,603	125,232	147,164 (+17.5%)
	모바일뱅킹	58,031	59,287	70,448	78,730	90,910 (+15.5%)
	조회	85,891	87,249	102,776	114,293	135,264 (+18.3%)
	이체	8,096	8,577	9,814	10,926	11,884 (+8.8%)
	대출	5.8	14.5	12.5	12.4	15.9 (+28.5%)
이용금액	인터넷뱅킹	42,147	44,061	47,454	47,644	47,755 (+0.2%)
	모바일뱅킹	3,711	4,388	5,232	5,453	6042 (+10.8%)
	이체	42,101	43,902	47,311	47,496	47,564 (+0.1%)
	대출	45.6	159.3	143.1	148.8	191.3 (+28.6%)

결국 인터넷에 기반한 지불거래의 위험성을 탐지하고 사기거래를 줄이기 위한 이상금융거래탐지시스템(FDS: Fraud Detection System)이 의무화되기에 이르렀으며, 최근 사회문제 해결에 다양하게 도입되고 있는 머신러닝에 기반한 FDS 시스템의 도입도 보편화되어 가고 있다.

관련 기관 및 규정으로써 개인금융 비대면 거래에서 필요로 하는 본인인증 도구인 공인인증서는 1999년 전자서명법, 2001년 전자정부법에 의해 시행된 것이다. 공인인증서는 각 개인 및 법인의 실제 정보를 검증하여 한국정보인증과 금융결제원을 통해 확인되고 발급하게 되며, 현재는 금융거래, 신용지불로부터 각종 공인인증 인터넷 사이트의 가입, 전자정부 가입 등 개인 및 법인의 전자적 본인 증빙과 공적 행동에서 필수 인증수단으로 보편화 되었다[3]. 이와 병행하여 또 다른 방법으로는 인터넷진흥원이 주도하는 i-PIN과 우리나라 법에 의해 반드시 실명가입해야 하는 이통통신 전화번호 및 통신사를 경유하여 진행하는 본인인증 방법이 사용되고 있다. 또한 고도화된 전자금융사기를 탐지하기 위한 FDS 시스템의 도입 및 금융관련 기업간의 금융사고 관련 정보통합의 중심 보안 전문기관으로써는 2015년에 설립된 금융보안원이 그 핵심 역할을 하고 있다.

국내 뿐 아니라 세계적으로 급격히 증가하고 있는 전자지불 및 전자상거래는 핀테크 기술의 발전과 발맞추어 진화하고 있으며, 발전과 더불어 편의성도 확대되고 있지만 이에 비례하는 사기사고도 확대되고 있다. 인터넷에 기반한 전자상거래 시대 이전에도 지불관련 금융사기는 드물지 않았으며, 가장 많은 사기가 발생하는 것은 신용카드 지불관련 사건이었다. 실물 카드에 기반한 지불에 있어서도 마그네틱 라인이 복제된 카드에 의한 금융사기가 발생하고, 이로 인한 카드사의 보험료 상승 및 손실이 누적되었다. 이에 신용카드사는 지불이 이루어지는 상황을 종합적으로 분석하여 지불승인 거절 및 금융사고 통보를 하는 형태로 시스템을 발전시켰다. 이때의 기반기술은 비교적 단순한데, 이전에 지불이 이루어졌던 시간, 위치와 비교하여 상이하게 다른 시간이나 물리적으로 가능하지 않은 거리에서 지불요청이 발생한 경우 등 시간적, 지리적 위치와 지불업종, 제품 등에 따라 금융사기를 탐지하여왔다. 인터넷에 기반한 전자지불이 도래하게 되면서, 신용카드사는 발빠르게 FDS 시스템을 도입하게 되었으며, 은행과 함께 대표적인 전자지불 사기거래 탐지 시스템을 운용하는 주체가 되었다[4]. 이에 관련한 보다 상세한 내용 및 본 논문에서 제안하는 상대위치에 기반한 도용 탐지방법, 그리고 위험률 도출 사례는 각각 2장, 3장, 4장에서 기술한다.

II. 핀테크 기반 금융과 기반기술

전자지불과 직접 연관된 사항으로 필수적인 것은 본인인증이다. 전자지불의 완결은 2단계의 체계적인 검증을 포함하고 있는데, 첫 번째 단계는 계정에 접속한 것이 실제 본인임을 증명하는 것이고, 두 번째 단계로는 지불 관련한 행위가 실제 본인이 진행한 것임을 증명하는 것을 의미한다. 첫 번째 단계인 본인임을 증명하는 것은 주민등록증, 여권, 운전면허증 등 국가기관이 인증한 본인임을 확인하는 실체적 증명서를 이용하고, 이로부터 파생하여 만들어지는 전자적 증명서인 공인인증서 및 본인인증 가입된 통신사 전화번호에서 시작되며, 실체적 증명서와 공인인증서, 전화번호를 병행하여 첫 번째 단계인 본인을 증명한 계좌 생성이 완결된다. 이에 연관하여 계좌 자체의 본인인증은 되었지만, 차후 이 계좌에 접속하는 것이 본인임을 증명할 수 있어야만 하며, 이 절차에서 각종 암호 및 생체인증 등 여러 과정을 포함한다[5]. 또한 이것이 앞서 이야기한 두 번째 단계, 즉 지불관련한 행위가 실제 본인임을 증명하는 것이 된다. 인터넷에 의존하는 이 두 단계에 있어서 포함되는 통신매체, 컴퓨터 등 디지털기기, 생체인식 센서, 카메라 등 종합적인 보안체계가 수립되어야 하며, 각 기기와 통신, 센서, 소프트웨어 등 한 곳이라도 보안 취약점이 발생할 경우 해킹 및 금융사고로 이어질 수 있다. 이에 관한 보안 표준은 FIDO로 규정되고 있다[6].

본인행위의 증명은 전자상거래 외에도 구글, 네이버와 같은 인터넷 계정에서도 필요한 것으로써 필요에 따라 실체적 본인임을 증빙하는 첫 번째 단계를 필요로 하지 않는 인터넷 계정 같은 종류가 있고, 국내법상, 또는 금융거래와 같은 중요한 행위임에 따라 첫 번째 단계와 두 번째 단계를 모두 필요로 하는 경우가 있다. 국내의 경우 두 번째 단계 중 서비스 제공 기업의 의무와 관련하여 전자지불과 관련한 경우와 그렇지 않은 경우에 따라 여러 법적 규정을 두고 있으며, 이에 따라 다양한 보호 체계를 도입하고 있다.

<그림 1>은 금융기관에서 포괄하고 있는 여러 보호 및 다중 인증 보안 도구를 나타낸 것이다[7]. 그림에서 나타나는 명시적 보안절차는 주로 금융사고를 막고 본인거래임을 확인하기 위한 단계적 절차임에 반해, 명시적으로 나타나지 않는 보안절차가 병행되고 있다.

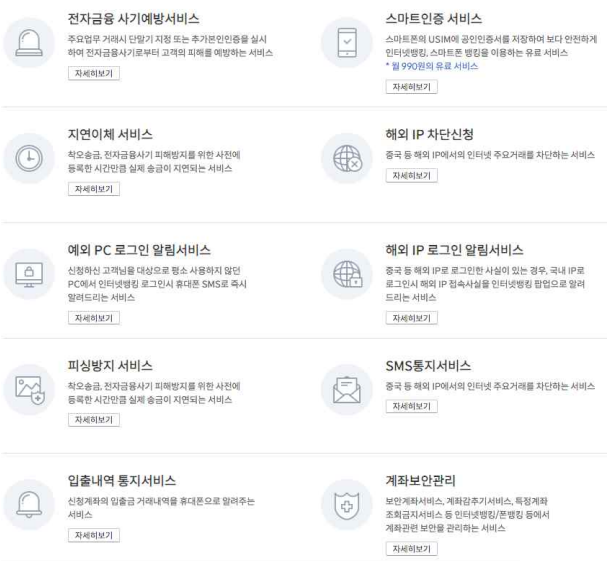

그림 1. 복잡한 다단계의 본인인증 절차를 거치고 있는 은행 본인인증 형태 (신한은행)[7]

Figure 1. Multi-level complex tools for processing of personal identification (Shinhan bank)[7]

이상금융거래탐지시스템(FDS)은 위와 같은 보안절차와 병행하여 사용되며, 앞서 설명하였던 신용카드 지불거래에서의 시공간적, 매장과 물품의 종류 등과 관련한 이상거래 탐지방법이 보다 고도화 된 것으로 설명할 수 있을 것이다. 다음 <그림 2>는 머신러닝을 포함한 위험탐지용 FDS 시스템의 내부 흐름이다[8].

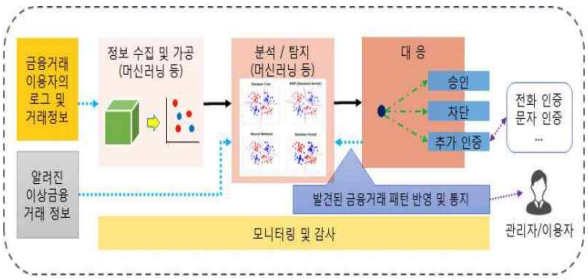

그림 2. FDS 시스템 동작 방식[8]

Figure 2. Operation process of FDS systems[8]

인터넷에 기반한 전자지불에 있어서 FDS 시스템이 사용할 수 있는 파라미터는 접속 단말기의 IP주소로부터 시작하여 스마트폰의 해킹 여부, 스마트폰에 추가적으로 설치되어 있는 프로그램 여부 등 보다 넓은 디지털 환경으로 확대되었으며, 이러한 추가요소의 종합적인 조합에 따라 전자지불의 위험률을 산출하고, 산출된 위험률에 따라 실제 지불이 이루어지기 전에 점진적 단계를 추가하는 등 가변적 처리를 하고 있다. 다음 <그림 3>은 앞서 서술한 첫 단계 로그인 및 두 번째 거래인증 단계와 FDS 시스템의 위치정보 및 IP와 관련된 연동, 도출 위험률에 따르는 단계적 인증절차를 통합하여 나타낸 것이다[9].

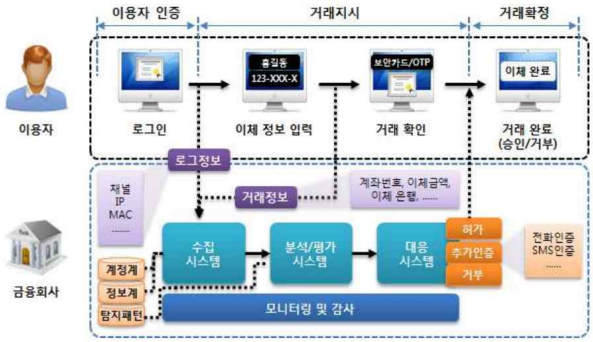

그림 3. 위험률 도출에 따른 본인거래 확인 검증의 단계처리[9]

Figure 3. User authentication according to risk calculation ratio[9]

인터넷에 기반한 전자지불에 있어서 주요 요소 중 하나는 절대위치, 즉 지역과 IP주소가 된다. 인터넷에 연결되어 있는 스마트폰의 경우 기기 자체에 내장된 GPS 센서 및 이동통신 기지국을 통해 이루어지는 A-GPS를 이용하여 위치정보서비스를 받을 수 있으며, 안드로이드 및 아이폰과 같은 경우 전자지불이 이루어지는 어플에 의해 이와 같은 위치정보가 서버쪽으로 전송되어 FDS 에 의해 이용된다. 이 정보와 더불어 IP주소 및 패킷경로는 단말의 지역적 위치를 알 수 있는 방법으로 활용되며[10], 시간정보와 함께 일차적으로 전자지불의 도용 위험률을 산출하는 데 핵심 정보로 사용된다. 본 논문에서 초점을 맞추고 있는 것은 바로 이 FDS 서버쪽에서의 도용 위험률 산정방법을 개인 디지털 환경을 이용하여 보다 정밀하게 개선하는 방법에 대한 것이다.

III. 상대위치에 기반한 위험률 도출방법

앞 장에서 서술한 스마트 단말의 위치정보는 지역적, 물리적 절대위치를 알게 해 주는 방법이다. 이 방법을 이용해 물리적으로 이동할 수 없는 시간거리 내에서 연쇄된 전자지불이 이루어지거나 하는 경우 대단히 높은 위험률로 산출하게 된다. 하지만 이 방법은 본인인증 과정에서 필요한 암호를 취득한 해커에 의해 쉽게 도용할 수 있다는 단점이 있다. 해커가 단말의 정보와 함께

필요 암호를 취득할 경우 사용자의 국적 등은 물론 위치정보도 동시에 쉽게 취득할 수 있다. 따라서 전자지불 도용을 할 경우 위치정보 또한 거짓으로 모사할 수 있으며, IP 접근 경로의 경우 모사하려는 지역에 있는 VPN서버를 이용하도록 경로를 설정할 경우 쉽게 속일 수 있다. 특히 수많은 유무선 라우터의 경우 이러한 용도로 활용될 수 있으며 보안에 있어서도 취약한 상황이다[11]. 따라서 쉽게 노출될 수 있는 위치 정보와 IP 접근경로만으로는 도용거래를 막는 것을 보장할 수 없다.

본 논문에서 주목하는 것은 이와 같이 절대위치 정보가 쉽게 모사할 수 있다는 것에서 시작되었다. 절대적으로 단정할 수는 없으나, 많은 사람의 경우 전자지불과 같은 중요한 거래를 함에 있어서 일정 장소에서 반복적으로 일어날 것을 예상할 수 있고, 실제 전자지불에 있어서 어느 위치에서 반복적으로 일어나는가를 수집하고 있으며, FDS 시스템에서 이를 위험률 산정에 이용하고 있다. 본 논문에서 실험한 방법에서는 전자지불이 일어나는 절대위치와 본 연구에서 주목하는 상대위치 정보를 수집하였으며, 수집 대상이 되는 앱은 크게 세 개 등급으로 분류하였다. 절대위치로는 집과 사무실(학교), 그리고 기타 세 유형으로 구분하고 등급으로 분류하였다. 다음 <표 4>는 수집 대상이 되었던 앱의 유형이며, <표 5>는 등급별 특정 장소와 일치한 액세스의 비율이다.

FDS에서 수집하는 이와 같은 정보에 더불어 보다 고도화된 위험률 산출을 위해 상대위치 정보를 같이 수집하였는데. 상대위치 정보의 설정은 접속 단말에서 검색되는 액세스 포인트(AP)의 SSID 및 MAC 주소를 이용하였다. 이를 위해 연구진의 시스템에 총 4개월간 앱을 설치하여 데이터 수집을 지속하였다.

표 4. 앱의 유형: 전자지불, 로그인기반, 웹 액세스
Table 4. Application types: electronic payment, login based, web access

앱의 유형	등급	대상 프로그램	사례
전자지불, 증권 등	1	은행, 전자지불	원터치뱅킹, NH뱅킹, Paynow, 앱카드, 크레온
로그인기반 포털, 교통	2	네이버 등	네이버 앱, 카카오지하철, 카카오버스
웹 액세스	3	웹 브라우저	크롬, 기본 브라우저

표 5. 등급과 특정 위치 연관 액세스 비율 (총 565건 수집건수)
Table 5. The relation between application types and location (total 565 collected cases)

등급	집/사무실	기타 장소	집/사무실의 비율(%)
1	61	1	96.8
2	87	281	23.6
3	36	98	26.9

수집 결과를 정리하면, 총론적으로는 대다수의 접속에 있어서 집과 사무실에서 전자지불이 이루어짐이 확인되었고, 이 비율은 타 유형의 앱 실행과 분명히 구별되는 특성으로 나타났다. 물론 이러한 결과는 모든 사람에게 공통적 나타나는 특성이라고 할 수는 없을 것이다. 하지만 유사한 특성을 나타내는 다수의 사람에게는 개인별 환경을 수집, 위험률 산정에 적용할 수 있으며, 개인은 일정 행동을 반복하는 습성이 있는 바, 전자지불과 같은 중요한 행위에 있어서 이 개인의 특성은 유지될 것임은 자명하다. 결과적으로 이와 같이 반복된 행위는 특정인이 진행하는 전자지불에 있어서 FDS 시스템의 위험률 산정에 유용하게 사용될 수 있으며, 본 논문은 이와 같은 위험률 산정 방법을 다음과 같은 순서절차로 제안한다.

- 전자지불에 관련한 앱의 시작과 함께 무선랜 환경을 스캔한다.
- 수집된 AP의 SSID, MAC 주소, 공공 AP 일치의 경우 해당 SSID와 MAC을 FDS 서버로 전송한다.
- FDS 서버는 해당 사용자의 상대환경으로 전자지불 상황에서의 주변 무선장치의 MAC을 축적한다.
- 상대환경의 위험률은 반복된 누적의 발생 비율을 파라미터로 하여 산출한다.

이와 같은 흐름은 다음의 <그림 4>와 같이 단순화시켜 도시할 수 있다.

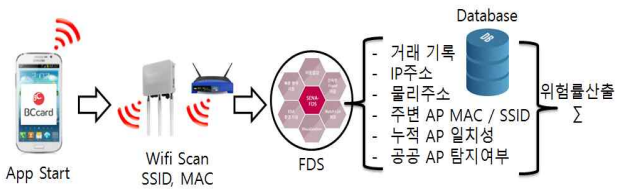

그림 4. 상대위치 수집 및 위험률 도출 방법
Figure 4. Collecting relative location information and risk ratio calculation

위 그림에서 나타낸 위험률 산출 식에서 비율특성함수는 DFS의 기타 축적 데이터베이스 및 머신러닝 등을 활용한 함수 형태로 축약시킬 수 있다[12].

$$\sum = \frac{\text{특정상대위치}}{\text{누적금융 위치}} \text{X (비율특성함수) X (공공 SSID, MAC 탐지토글 함수)}$$

이러한 흐름에 따라 특정 인물이 전자지불을 시도할 때, 그 위치에서 감지된 AP의 SSID와 MAC 주소가 누적된 과거의 탐지된 AP와 일치하지 않는다면, 위와 같이 상대위치에 상관된 위험률을 산출할 수 있다. 이에 더불어 공공 목적으로 사용하는 AP의 고정적 운용특성을 부가할 수 있으며, 이 조건은 공공용 AP의 검색 일치성에 따른 위험성을 추가함으로 가능해진다. 공공 AP의 SSID 데이터베이스를 예외조건으로 사용할 수 있는 이유는 이 AP의 설치위치가 변하지 않는 특성을 나타냄과 더불어, 예를 들면 “Public Wifi@Mapo”와 같이 고정된 SSID 검색이 특정 물리적 위치를 내포하는 의미를 동시에 갖게 되기 때문이다. 즉 명칭 데이터베이스에서 이전에 나타나지 않았던 공공 AP의 SSID가 감지되거나, 반대로 사라지게 된다면 이를 반영하여 높은 위험률로 산정하도록 한다. 간략화하여 표현한 위 위험률 산출 수식에서 공공 SSID, MAC 탐지토글 함수는 공공 SSID의 고유한 특성에 따라 함수로 축약하여 표현한 것이다.

Ⅳ. 실험 및 고찰

앞서의 절차와 방법에 따라 절대위치와 함께 상대위치 정보를 실제 단말에서 수집하였고, 본 제안의 활용성 검증을 실시하였다. 개인정보의 민감성이 있는 스마트폰 환경의 특성상, 더욱 민감한 금융거래 정보와 연동한 수집이며, 스마트폰에 추가적인 부하와 에너지 사용을 발생시키기에 연구진 및 주변 직접관계인으로 수집 대상을 제한하였으며, 수집기간에 걸쳐서 자연스러운 전자지불 활동을 하게 한 바 어느 정도 의미있는 결과를 수집하였다고 판단한다.

이미 서술한 바와 같이 본 방법은 여러 사람의 집합에 대한 집단적 보편성을 이용하고 있지 않으며, 각 개인의 행동 특성에 따른 고유 특성을 활용하고 있으므로 소수 각 개인의 수집 데이터만으로도 의미있는 적용 가능성과 유의성을 확보할 수 있다.

앞서 제시한 <표 4> 및 <표 5>와 같은 특정 금융앱 및 대표적인 포털과 웹 브라우저를 대상으로 제한적 수집을 한 결과를 적용하고, <그림 4>의 흐름과 같은 AP 검색을 통한 상대위치 반영 방법으로 위험률을 도출할 경우 DFS 시스템의 동작 구성에 따라 구체적인 값은 달라질 수 있으나 다음 <표 6>과 같은 개략적인 결과가 됨을 확인할 수 있다.

표 6. 앱의 유형: 전자지불, 로그인기반, 웹 액세스
Table 6. Application types: electronic payment, login based, web access

전자지불 앱의 실행위치	위험률	위험률 도출 원인
집, 사무실	저	누적 동일 상대위치 실행 경우
특정 공공 SSID 토글 탐지	고	상대위치의 부정합 발생
기타 장소	고	과거 기록 없는 상대위치에서의 실행 경우

이 의미를 정리하면 다음과 같다.

- 일반 어플과 달리 전자지불 관련 어플의 경우 특정 주변 AP와의 결합 특성을 나타내며, 이는 AP에 대한 접속 여부와 상관없이 특정 상대위치를 확인하는 방법으로 사용할 수 있다.
- 특정 지역에 결합되어 있는 공공 SSID 감지상태의 변화는 상대위치의 변화와 위험성 산출에 사용할 수 있다.
- 무선랜 환경으로 도출할 수 있는 상대위치는, 물리적 위치를 의미하는 GPS, IP 주소와 결합하여 사용할 수 있으며, 이 경우 더욱 높은 절대-상대위치 조합의 위험률을 도출할 수 있다.

Ⅴ. 결 론

본 논문은 인터넷에 기반한 비대면 전자지불거래에 있어서 거래의 위험률을 도출함에 있어서 FDS 시스템이 축적하는 위치정보에 주목하였다. 현재 시스템에 의해 각 개인의 거래에 대하여 지역적 위치정보 및 IP 주소 경로가 이용되고 있으며, 이러한 정보는 공개되고 고정된 값을 가지고 있음으로 인하여 해킹 및 모사될

수 있음을 제시하였다. 본 논문에서는 결과적으로 보다 정교한 위험률을 도출하기 위해 각 개인의 전자지불 거래에 있어서 개인 환경적인 반복성을 내재하고 있음을 주목하였으며, 개인 환경의 주요 요소로써 스캔되는 AP의 SSID와 MAC 주소를 상대위치 환경으로 축적, 활용하는 방법을 제시하였다. 또한 이 정보를 기존의 지역위치 및 IP 접속 경로와 결합하여 보다 높은 위험성을 나타내는 전자지불거래를 탐지할 수 있는 방법을 제안하였다.

이 방법은 전자적 지불거래가 일어나는 스마트 단말의 무선랜 환경을 탐지함으로써 상대위치로활용한 것으로, 각 개인 환경의 반복성을 활용한 것이다. 이 정보는 이전에 사용하는 절대위치와 달리 예측하기 쉽지 않으며, 공개되지 않는 정보이기에 보다 정교한 위험률 산출에 이용할 수 있음을 확인하였다.

References

[1] You, Han-Na; Lee, Jae-Sik; Kim, Jung-Jae; Park, Jae-Pio; Jun, Moon-Seog, “A Study on the Two-channel Authentication Method which Provides Two-way Authentication using Mobile Certificate in the Internet Banking Environment”, The Journal of Korean Institute of Comm. and Info. Sci., Vol.36, No.8B, pp.939-946. 2011. DOI: 10.7840/KICS.2011.36B.8.939

[2] Domestic Internet Banking Service Report, First Half of 2019, Public Report no. 2019-10-08, Bank of Korea, 2019.

[3] Hong, Ki-seok; Lee, Kyung-ho, “Advanced Mandatory Authentication Architecture Designed for Internet Bank”, Journal of The Korea Institute of Info. Secu. and Crpto., Vol.25, No.6, pp.1503-1514, 2015.
DOI: 10.13089/JKIISC.2015.25.6.1503

[4] Raj, S. Benson Edwin; Portia, A. Annie, “Analysis on Credit Card Fraud Detection Methods”, International Conf. on Computer, Communication and Electrical Technology. IEEE, 2011. DOI: 10.1109/ICCCET.2011.5762457

[5] Yun, Min-Seop “A Study on Fintech and Consumer Protection Measures”, Korea Consumer Agency, Dec. Chungchongbuk-do, 2015.

[6] Lindemann, Rolf; Baghdasaryan, Davit; Hill, Brad, FIDO Security Reference, FIDO Alliance Proposed Standard, 2015.

[7] Banking Security Managing, Shinhan Bank, Retrieved at Dec., 28, 2019, from https://www.shinhan.com/hpe/index.jsp#050401020000.

[8] Security Research Dept.-2017-032 Trends of Machine Learning-based Fraud Detection System, Financial Security Institute, 2017.

[9] Financial Security Institute 2014-08 Technical Guide of Fraud Detection System, Financial Security Institute, 2014.

[10] Suh, Hyo-Joong, “Sensual Confidence of Personal Certification by Network Paths”, Convergence Research Letter, Jul. Vol.3, No.3, pp.713-716, 2017,
DOII: 10.14257/ajmahs.2017.12.66

[11] Kavak, Hamdi; J Padilla, Jose; Vernon-Bido, Daniele; Y. Diallo, Saikou; Gore, Ross, “The Spread of Wi-Fi Router Malware Revisited”. In 20th Communications and Networking Simulation Symposium, 2017.

[12] Abdallah, Aisha; Aizaini Maarof, Mohd; Zainal, Anazida, “Fraud Detection System: A Survey”, Journal of Network and Computer Applications, Vol.68, pp.90-113, 2016.
DOI: 10.1016/j.jnca.2016.04.007

[13] Xia, Xuehao; Bae, Soo Hyun, “Social Responsibility Activities and Financial Performance of the Financial Industry”, The Journal of Convergence and Culture Technology (JCCT), Vol. 5, No. 3, pp.71-78, 2019.
DOI: 10.17703/JCCT.2019.5.3.71

[14] Lee, Dongwoo; Kim, Daehyun; Lee, Junghoon; Lee, Seungyoun; Hwang, Hyunsuk; Mariappan, Vinayagam; Lee, Minwoo; Cha, Jaesang, “Design of Low Cost Real-Time Audience Adaptive Digital Signage using Haar Cascade Facial Measures”, The International Journal of Advanced Culture Technology (IJACT), Vol. 5, No. 1, pp.51-57, 2017.
DOI: 10.17703/IJACT.2017.5.1.51

※ 이 논문은 2016년 정부의 재원으로 한국연구재단의 지원을 받아 수행된 연구사업 (2016R1D1A1B01006716)으로 이루어졌음. 이 연구는 한성대학교 교내연구비지원으로 수행되었음.