Journal of the Korea Academia-Industrial cooperation Society
Vol. 22, No. 5 pp. 325-333, 2021

https://doi.org/10.5762/KAIS.2021.22.5.325
ISSN 1975-4701 / eISSN 2288-4688

셀 브로드캐스팅 보안 인증시스템 및 비즈니스 모델에 관한 연구

최정문[1], 이정우[2*]
[1]연세대학교 정보대학원 석사과정, [2]연세대학교 정보대학원 교수

A Study on Cell-Broadcasting Based Security Authentication System and Business Models

Jeong-Moon Choi[1], Jungwoo Lee[2*]
[1]Graduate School Of Information, Yonsei University
[2]Graduate School Of Information, Yonsei University

요 약 공유 서비스나 사물인터넷기술이 확산됨에 따라 보안인증이 적용되어야 하는 분야와 그 범위가 넓어지고 있다. 이동을 전제로 하는 서비스들에 있어서는 기존의 개인 소유물이나 특성에 관한 보안인증만으로는 충분치가 않아서 위치에 기반한 인증기술들도 개발이 되고 있다. 하지만 기존 위치기반 보안인증기술의 대부분은 주로 서버 근접도나 위성위치추적을 활용하는 기술로 개발이 되고 있어서 그 활용의 범위가 좁고 이동 시 핸드오버 문제가 발생한다. 본 연구에서는 이러한 기존의 위치기반 보안인증기술보다 그 활용의 범위가 넓고 따라서 편의성과 사업성이 높은 셀 브로드캐스팅(Cell Broadcasting)기술 활용 위치기반 보안인증기술에 대해서 소개하고 이와 관련된 응용 사례 및 비즈니스 모델들을 소개하였다. 기술 개발의 현황과 아울러 이를 활용하여 사업을 개발하고 있는 기업 사례를 심층 분석하여 비즈니스 모델의 변화가 어떻게 이루어지고 있는지를 자세히 분석하였다. 여기서 제안된 셀브로드캐스팅 보안인증시스템은 다각화되고 있는 미래형 비즈니스모델의 근간이 되는 기술이며 기존의 위치인증방법 및 시스템을 보완한 모델로 그 의미가 있다.

Abstract With the rapidly changing era of the fourth industrial revolution, the utilization of IT technology is increasing. In addition, the demand for security authentication is increasing as shared services or IoT technologies are being developed as new business models. Security authentication is becoming increasingly important for all intelligent devices such as self-driving cars. However, most location-based security authentication technologies are being developed mainly with technologies that utilize server proximity or satellite location tracking, which limits the scope of their physical use. Location-based security authentication technology has recently been developed as a complementary replacement technology. In this study, we introduce location-based security authentication technology using cell broadcasting technology, which has a wider range of applications and is more convenient and business-friendly than existing location-based security authentication technologies. We also introduced application cases and business models related to this. In addition to the current status of technology development, we analyzed current changes in business models being employed. Based on our analysis results, this study draws the implication that technology diversification is necessary to improve the performance of innovative technologies. It is meaningful that it has found and studied advanced technologies other than existing location authentication methods and systems.

Keywords : Cell Broadcasting, Location Based Service, Security Authentication, Business Model, Information Technology

*Corresponding Author : Jung-Woo Lee(Yonsei Univ.)
email: jlee@yonsei.ac.kr
Received February 1, 2021 Revised April 30, 2021
Accepted May 7, 2021 Published May 31, 2021

1. 서론

1.1 연구의 배경 및 목적

정보통신기술의 급속한 발달은 제품의 생산과 유통을 중심으로 형성되어 있는 산업사회 패러다임을 넘어서 새로운 지식정보사회를 열고 있다. 대형 자본 투여를 전제로 하는 대량 생산 패러다임에서 움직이는 산업사회와는 달리 지식정보사회는 정보를 생산하고 유통하며 활용하는 서비스들이 중요해지고 고도화된 정보응용기술을 활용해서 생산되는 정보와 지식의 가치가 인정되는 사회를 의미한다. 정보응용기술을 기반으로 인공지능, 사물인터넷 등 모바일 기기들을 활용하는 IT서비스 시장이 커지고 있으며, 이에 따라 사용자들의 정보 보안과 개인들의 인증이 중요하게 부각되고 있다.

본 연구에서는 셀 브로드캐스팅 기술을 활용한 새로운 형태의 위치기반 보안인증 기술의 상세를 소개하고 이를 활용한 다양한 비즈니스 모델의 시나리오들을 분석하였다. 셀 브로드캐스팅 기술을 기반으로 한 보안인증의 활용은 전자금융거래 등 중요한 순간에 기존의 인증에 부가하여 인증하는 추가 인증의 새로운 대역외(OOB, Out of Band, 이하 OOB)인증으로 시작되었다. 또한, 위치와 시간을 결합하여 기존에 사용되고 있는 OTP(One Time Password)보안토큰 방식의 취약점을 해결할 수 있는 기술로 활용될 수 있다. 이에 금융업계와 관공서 등 다양한 분야에서 본 기술에 주목하고 있으며, 기존의 서비스와 결합하여 새로운 서비스 모델로 활용 가능성이 높을 것으로 보인다.

본 연구는 셀 브로드캐스팅을 활용하여 위치기반 보안인증을 보완하는 기술의 상세를 소개한다. 아울러 본 기술을 활용하는 비즈니스 모델들을 시나리오 형태로 개발 제시하여 앞으로 이를 활용하는 융합연구의 기반을 제시하고 있다.

1.2 연구의 구성

본 논문의 구성은 총 5장으로 이루어져 있으며, 각 장의 내용은 다음과 같다. 제 2장에서는 보안 인증 기술, 위치기반 기술에 대한 이론적 개념과 위치기반 보안 인증 선행 기술들을 검토하고 이어서 제 3장에서는 셀 브로드캐스팅 기술을 활용한 위치기반 보안 인증이 기존의 연구들에 비해서 어떠한 위상을 차지하고 있는지를 기술개발 현황을 중심으로 개념화하고 이와 관련된 서비스 모델이 어떻게 진화하여 왔는지 소개한다. 제 4장에서는 본 기술을 적용한 사례를 비즈니스 모델의 종류를 중심으로 연구한 결과를 제시한다. 마지막으로 제 5장에서는 본 논문의 결론을 제시하고 본 기술에 대한 기대효과 및 향후 추가 연구 방향에 대해 기술한다.

2. 선행연구와 이론적 배경

2.1 보안 인증 기술

기술 분야에서의 인증(認證, Authentication)이란, 다중 사용자 컴퓨터 시스템 또는 망 운용 시스템에서, 시스템이 단말 작동 개시(log-on) 정보를 확인하는 보안 절차이다[1]. 일반적으로 온라인상에서 아이디(ID)와 패스워드(Password) 입력으로 본인을 확인시키는 인증 방법이 사용되고 있다. 패스워드 기반의 인증 방법은 구현하기 쉬워 많이 사용되고 있으나, 보안성이 가장 약한 인증 방법이다. 일반적으로 보안 인증 방법을 분류할 때는 인증하려는 대상에 따라 나누는데, 인증의 대상이 사람인 경우 “사용자 인증”, 인증의 대상이 디바이스와 같은 기기인 경우에는 “기기 인증”이라고 한다[2]. 즉, 인증은 주체의 신분을 확인하고 증명하는 과정이다. 네트워크 서비스에 접근하려는 주체가 정당한 사용자인지 아닌지를 분명히 식별해 낼 수 있어야 하고, 비정상적인 사용자는 잘못 받아들이지 않도록 접근을 제어 할 수 있어야 한다[3].

한편, 정보통신기술의 발달로 얼굴을 보지 않고 본인확인을 하는 방법을 비대면 실명 인증 서비스라고 하고 한다[4]. 사용자 인증은 정보시스템 구축의 가장 기본이 된다[5]. 사용자 보안인증은 전자서명법에 따라 공인인증체계가 수립된 이후 은행과 같은 전자금융거래서비스, 전자정부 등 사용자 인증이 필요한 대고객 서비스에서 구축 및 사용되고 있다.

사용자 보안인증은 표준 TTAK,KO-12.0247 전자거래 보증 수준별 인증방법 요구사항에 따라 지식 기반, 소지 기반, 특성 기반, 행위 기반의 네 가지 방식으로 크게 분류된다. 지식 기반은 사전에 사용자들에게 공유된 정보를 사용자가 사용 시점에 발급자에게 제출하고 발급자가 이를 검증함으로써 인증을 수행하는 방법이다. 지식기반 인증방법으로는 비밀번호, 문답식 인증, 이미지 인증 등이 있다. 소지 기반은 사용자가 소지하고 있는 인증기기를 활용하여 사용자 인증을 수행하는 것이다.

소지기반인증도 크게 4가지 인증 방법으로 나누어진다. 첫 번째, OOB인증 방법은 전화승인, 스마트폰, 이메일, 문자(SMS)인증과 같이 사용자에게 메시지를 통해서

확인하는 방법이다. 두 번째는 OTP보안토큰 방식이다. 이는 일회용 비밀번호 방식으로 보안카드, 하드웨어 OTP발생기, 소프트웨어 OTP발생기 등이 있다. 세 번째는 PKI(Public Key Infrastructure) 토큰 인증방식으로서 공인인증서와 같은 보안토큰을 사용하는 방식이다. 네 번째는 IC카드(Integrated Circuit Card) 또는 신용카드 정보를 통한 인증 방법이다. 특성기반 인증 방법은 지문/홍채/얼굴 인식 등 생체정보를 활용한 인증방식으로 생체기반 인증 방법이라고도 한다. 행동기반 방식은 스마트폰, 스마트 패드 등이 일반화되면서 키보드 입력이나 서명을 하는 사용자의 행동 패턴을 분석하는 방식이다. 인증방식의 분류는 Table 1에 요약하였다.

한편 실제 보안인증에 있어서는 주 인증과 추가 인증으로 구분하여 두 번을 인증하는 방식이 많이 쓰인다. 주 인증방법은 사용자가 인증할 때 주된 방법으로 사용하는 방식으로 비밀번호, 공인인증서, OTP, 보안카드를 활용하는 방식이 주를 이루고 있다. 추가인증방식으로 많이 쓰이는 방법들로서는 문자나 ARS를 사용하여 본인임을 다시 한번 확인하는 2채널 인증이 있다.

Table 1. Requirements for e-authentication method of assurance level [5] Reinterpretation

Authentication method			Classification
Knowledge Base	Password Question and answer Authentication Image Authentication		Main Authentication
Possession Base	OOB Authentication	ARS SMS Smartphone-App Email	Additional Authentication
	OTP Security Token	Security Card List of Passwords S/W OTP Generator H/W OTP Generator Mixed OTP Generator	Main Authentication
	PKI Token	S/W Certificate H/W Security Token Transaction si-gnature token	Main Authentication
	Others	IC card Credit card	Main Authentication
Characteristic Base	FingerprintIris recognition Face recognition Iris recognition		Not Applicable
Behavior Base	Signature pattern Keyboard-Input Pattern		Not Applicable

2.2 위치기반기술

위치기반서비스(LBS, Location Based Service, 이하 LBS)는 이동통신망 또는 GPS(Global Positioning System) 등을 통해 얻은 위치정보를 바탕으로 여러 가지 서비스를 제공하는 시스템이다. 위치정보는 이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재했던 장소에 관한 정보로서 전기통신설비 및 전기통신회선설비를 이용하여 수집한 것을 의미한다[6].

위치정보를 측정하는 방식은 아래 Fig. 1과 같이 크게 네트워크 기반, 위성신호 기반, 와이파이 신호 기반, 혼합 측위 기반으로 구분된다[7].

측위 방식	설 명
네트워크 기반	이동통신사 기지국의 위치 값(Cell-ID), 기지국과 단말기 간의 거리 등을 측정하여 위치를 계산
위성 신호 기반	GPS(Global Positioning System) 위성에서 송신하는 신호를 바탕으로 위치를 계산
Wi-Fi 신호 기반	네트워크 기반의 일종으로 Wi-Fi AP(Access Point, 접속점)의 위치를 조회하여 단말기의 위치 값을 측정하는 방식. WPS(Wi-Fi Positioning System)라고 함
혼합 측위 기반	네트워크 기반·위성신호 기반·Wi-Fi 신호 기반 등의 위치를 조합하여 단말기의 위치 값을 측정. XPS(Hybrid Positioning System)라고 함

Fig. 1. Main Positioning System Methods [6]

LBS사업은 위치정보사업과 위치기반서비스사업으로 구분된다. 위치정보사업은 측위기술을 활용하여 위치정보를 수집하고, 이를 위치기반서비스 사업자에게 제공하는 사업이다[6]. 위치기반서비스사업은 위치정보사업자로부터 받은 위치정보를 이용하여 새로운 서비스를 제공하는 것이다[6]. 위치추적 서비스, 공공안전 서비스, 길찾기 서비스 등이 위치기반서비스사업들의 실제 사례들이다. 특히, 모바일 환경으로의 급속한 변화에 따라 위치기반 기술을 활용한 서비스들은 다양하게 개발되어 상용화되고 있다. 다음 Table 2는 위치기반기술 활용의 예시이다.

Table 2. Illustrative Cases of Location-Based Services [8]

Utilization field	Expectation effectiveness
Tracking the location of children or elderly people with dementia	Prevention of lost children, accident prevention
Tracking the location of Pet	loss, accident prevention
Car navigation	Identify the vehicle's path of travel

Identify the location of employees who work outside the office.	Effectively manage employees who work outside the office
Provides peripheral information for the current location.	Providing high value-added services by providing infor-mation on the surrounding- areas such as theaters, gas stations, restaurants, and department stores
police/security/military vehicle management	the prevention of crime
Provide location information of parcel/cargo	Reduction in fuel/traffic/ communication costs

2.3 위치기반 보안인증기술

소지기반, 지식기반, 행태기반, 특성기반의 보안인증 방식들은 완전히 신뢰할 수 없기 때문에 등장한 새로운 인증 유형이 위치기반인증 모델이다[3]. 위치기반 보안인증기술의 가장 큰 장점은 인가받은 사용자만이 네트워크에 접근할 수 있다는 점이다. 또한 위치 정보는 기밀 정보나 안전한 거래를 수행하기 위한 사용자들에게 추가적인 신원 보증수단으로 활용된다[3].

국내의 경우 위치기반 기술을 접목한 보안인증 방법으로 위치기반 Two-Factor L-OTP 프로토콜 연구가 있다[12]. 여기서는 시간 동기화를 통한 T-OTP(Time One Time Password) 기법과 위치기반 정보를 접목한 인증기법인 L-OTP(Location Based One Time Password) 프로토콜을 제시하고 있다. 여기서의 시나리오는 다음과 같다. 사용자는 자신이 OTP를 사용할 장소에 대한 위치정보를 인증 서버에 저장한다. 그 후 사용자는 조건을 만족하는 장소에 위치하고 OTP 생성이 필요한 순간에 위치정보 서버에 인증을 요청한다. 이때 서버는 비밀키로 서명된 위치정보와 단말기의 공개키로 암호화된 GPS정보, 시간정보를 사용자 단말기에 전송하게 된다. 이 과정에서 복호화된 T-OTP는 L-OTP를 생성한다[9]. 사용자는 이렇게 생성된 OTP를 인증에 사용하게 된다. 다음 Fig. 2는 위치기반 OTP 프로토콜의 구성도이다.

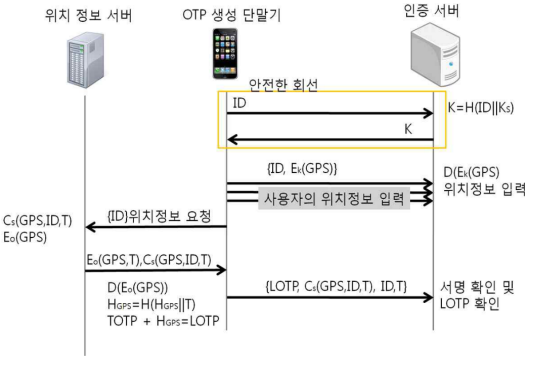

Fig. 2. Location-Based OTP Protocol Configuration Diagram [9]

L-OTP 프로토콜 방식은 새로운 개념의 OTP 동기화 기법이나 보안 관점에서 몇 가지 문제점이 나타난다. 첫째, GPS위치 정보를 이용하고 데이터를 암호화 한다 하더라도 결국 위치정보가 사전에 서버에 저장이 된다는 점이다. 암호화된 데이터를 복호화하기 위해서는 '키(key)'가 필요하다. 보안인증에 다양한 보안 솔루션이 적용 되었다 하더라도 키를 100%안전하게 관리한다고 장담할 수 없다. 키는 대부분 소프트웨어에 의해 만들어 지며, 생성된 키는 주로 기기의 메모리(NVM: Non-volatile Memory)에 저장되기 때문이다. 해커들은 주로 이 키를 노리고 있으며 언제든 해킹을 통해 유출될 수 있다는 위험성이 존재한다[10]. Fig. 3은 실시간 공격 유형의 단순 2채널 인증 공격의 예시이다. 국내에서 보안 강화를 위해 생체인증, 블록체인 방식 등 다양한 대안을 추진하고 있으나, 결국에는 원천 정보를 서버에 저장하여 입력된 정보와 대조하는 방식으로 저장된 정보의 해킹 위험과 복제가능성에 대한 우려가 해소될 수 없다.

둘째, 기존 위치 인증에 일반적으로 사용되는 GPS방식은 조작 위험에 노출되어 있다. GPS를 교란시키는 방법에는 재밍(전파 방해), 스푸핑(기만), 미코닝(시간차 전송)과 같은 다양한 기술들이 존재한다. 최근 GPS조작 어플리케이션이 출시될 만큼 GPS를 의도적으로 교란시키는 행위는 더 이상 어려운 기술이 아니다. 선행 연구에서 제시한 사용자의 GPS정보사용은 보안에 취약하다는 한계가 있다.

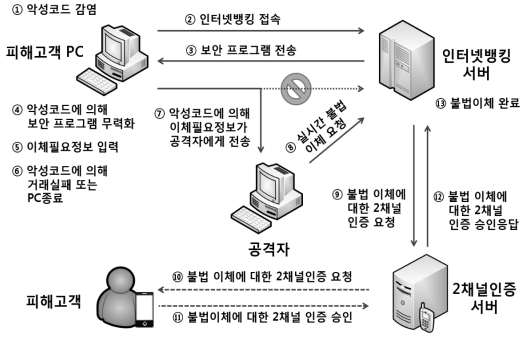

Fig. 3. Example of a simple two-channel authentication attack of a real-time attack type [11]

셋째, GPS는 위성 신호를 받아야하기 때문에 실내, 지하와 같은 환경에서는 GPS신호 수신이 불가능 하다. 만약 사용자가 실내에 위치해 있을 때 지도상에서 현 위치를 탐색해 보면 다른 위치를 가리키고 있거나 GPS 수신이 마지막으로 된 지역에 위치해 있는 것을 볼 수 있다. 보안인증은 개인의 신분 확인과 검증을 하는 과정이다. 때문에 어디에서든지 보안 인증 기술에는 강력하고 정확한 인증이 되어야 하는 관계로 여기에 보완이 필요하다.

3. 셀 브로드캐스팅 기술 활용 위치기반 보안인증

기존의 위치기반 보안인증 기술을 좀 더 발전시킨 것이 이동통신망의 셀브로드캐스팅 기술을 활용한 기술이다.

3.1 기술개발현황

본 연구의 위치기반 보안인증 기술은 셀 브로드캐스팅 방식을 기본으로 한 보안인증 기술이다. 기존 LBS기반 서비스가 사용하던 GPS신호 또는 와이파이신호 기반 방식과는 다른 셀 브로드캐스팅 서비스를 활용하였다. 셀 브로드캐스팅 서비스는 현재 국민의 안전을 위해 제공하는 재난문자 서비스에 사용하는 기술 방식으로 국내는 물론 국외에서도 위치인증방식에 사용된 적 없는 새로운 기술 방법이다.

현재 보안인증에 주로 사용되는 OTP인증방식은 사용자가 OTP기기를 가지고 있지 않더라도 제 3자가 기기에서 OTP인증번호를 생성해 알려주면 인증이 가능하다. 반면 셀 브로드캐스팅 기술을 활용한 보안인증 방식은 OTP인증번호를 생성할 때 사용자의 위치정보를 기반으로 생성한다. 때문에 인증번호를 입력할 때 사용자와 OTP기기의 위치가 동일해야만 인증이 가능하다. 단순히 인증번호만을 입력해서 인증이 되는 것이 아니라 인증번호와 사용자의 위치가 모두 일치해야만 인증이 가능한 기존보다 상위 개념의 보안인증 기술이다.

셀 브로드캐스팅 기술을 활용한 보안인증방식을 사용한다면 만약 해커가 해킹을 시도한다 하더라도 사용자가 위치를 변경하면 해커는 사용자의 위치를 다시 파악해야 하는 동시에 해당 위치로 이동을 해야 하는 어려움이 있다. 때문에 본 보안인증 방식은 외부로부터의 해킹이 거의 원천적으로 차단 가능하다. 또한 해커가 사용자의 위치정보를 알아냈을 경우 암호 확보를 위해서는 보안이 탑재된 위치암호 앱을 해킹한 후 보안 시스템이 매우 우수한 이동통신사 세 곳 모두 동시에 뚫어야 하는 거의 불가능에 가까운 난이도의 해킹이 필요하다[12].

즉, 본 연구의 보안인증 기술은 정보 수신 및 해킹이 어려운 위치기반과 기존의 암호정보를 보완적으로 결합하여 보안체계를 개선하였다. 아래 Fig. 4는 셀 브로드캐스팅 기술 활용 위치기반 보안인증의 시스템 개념도이다.

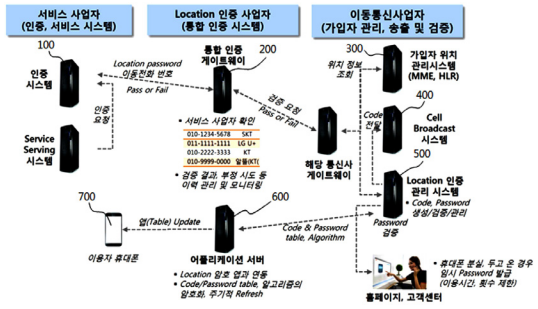

Fig. 4. Security Authentication System Conceptual Diagram [12]

본 기술의 목적은 ID, 패스워드와 같은 개인정보가 유출되어 해킹을 당한다 해도 금융거래 등 중요한 절차 중간에 위치정보에 기반한 인증번호를 입력하게 만들어 해킹의 피해를 낮출 수 있도록 하는 것이다. 비록 1단계 보안이 뚫린다 하더라도 인증 중간에 본 연구의 인증방법을 사용하면 해킹으로 인한 큰 피해를 막을 수 있다.

한편 본 연구에서 제시하는 셀 브로드캐스팅 기술 방법은 이동통신 기지국을 사용하기 때문에 사용자가 어느 곳에 위치해 있던 통신이 가능한 지역이라면 사용자의 위치 파악이 가능하다. 이는 GPS를 사용한 선행 기술 연구보다 고차원적 기술 방법이며, 지금까지 시도해 보지 않은 위치 인증 방식이다. 또한 본 기술의 개념은 항시 휴대하는 스마트폰 앱 형태로 탑재가 가능하여 범용적으로 사용이 가능하고 높은 보안성을 확보할 수 있다는 장점이 있다.

3.2 관련 서비스 모델의 진화

본 논문에서 기술하고 있는 셀브로드캐스팅 기반 보안인증은 2017년 1월 엘핀(L-Fin)을 창업한 박영경이 최초로 개발하였다. 본 기술을 개발하게 된 가장 큰 계기는 모바일 환경의 확산으로 인하여 앱 기반으로 모든 것을 할 수 있는 세상에서 기존에 PC에서 사용되는 인증 방법인 아이디, 패스워드 방식은 해킹의 위험에 쉽게 노출되어 있다는 점에 착안하였다. 이어서 카셰어링과 같은 무

인 렌터카 시스템이 도입되면서 운전면허증과 추가 사용자 확인 절차 없이 차량 대여가 가능해져서, 보안의 사각지대가 발생하고 있는 것이었다[13]. 카셰어링에 있어서 가장 큰 문제는 앱의 로그인 정보만 알고 있으면 누구든 차량을 이용할 수 있다는 점이다. 이용하려는 서비스 인증 또는 사용자인증을 보다 정확하게 수행을 하면서도 또한 해킹의 위협에서 벗어나게 할 수 있을까가 기술개발의 관건이었다.

여기서 기술의 기본 원리는 셀 브로드캐스팅 기술을 활용하는 것으로 사용자가 위치한 이동통신 기지국으로부터 일정 주기로 수신되는 고유의 정보(Code)를 활용하여 위치 암호를 생성한다. 생성된 암호는 전자금융은 물론 다양한 서비스의 추가 보안 인증 수단으로 활용된다. 아래 Fig 5는 셀브로드캐스팅 기반 위치보안인증 서비스 구성도이다.

Fig. 5. Configuration diagram of the security authentication service in L-Fin [12]

엘핀은 주 인증과 추가 인증 두 가지 방식으로 분류되는 보안 인증 방식 중 추가 인증 방식으로 시장에 진입하였다. 주 인증 방식이 아닌 추가 인증 방식으로 진입한 이유는 기존에 자리 잡고 있는 공인인증서, OTP카드를 대체하기에 신뢰도 측면에서 한계가 있다고 판단하였다. 박 대표는 기술에 대한 자신이 있었기 때문에 보조적 수단인 추가 인증 방식으로 접근하여 신뢰도를 쌓고 시장에서 인정을 받은 후 주 인증 방식으로 진입 해야겠다는 전략을 세웠다.

이후, 엘핀은 모바일 중심으로 변화되는 흐름에 따라 위치기반의 인증 및 보안의 중요성 증대를 예상하며 기술을 보안인증서 형태로 국한 시키지 않고 위치와 보안 서비스의 장점이 활용될 수 있는 목표 시장을 새로이 개발하고 비즈니스 모델을 달리 세분화하면서 기술을 더 개발, 확장하고 있다. 엘핀의 서비스는 다원적(Multi Factor)인증 시스템에 의한 높은 보안성과 다른 위치기반서비스 사업자가 제공하지 못하는 셀 브로드캐스팅을 활용한 위치 인증, 글로벌 시장에 빠르게 적용 가능한 확장성 등의 경쟁력을 바탕으로 사업자들의 니즈를 충족시키는 것을 목표로 서비스를 진화시키고 있다. 현재 엘핀 서비스의 주요 타겟은 B2B(Business to Business) 시장이다.

4. 적용사례연구

새롭게 개발된 본 기술을 적용하기 위하여 보안인증의 비즈니스 모델도 새롭게 개발 추진하고 있는데 대표적으로 근태(출결)관리 서비스, 아웃도어세일즈(Outdoor Sales), 여행 금융혜택서비스 및 유심기반 출금동의 서비스의 네 가지 비즈니스 모델을 여기 소개한다.

4.1 근태/출결 관리 시스템

근태 관리라 함은 지문인식기에 의한 출/퇴근 관리가 일반적으로 사용되고 있다. 하지만 지문인식기는 내근직 관리만 가능하다는 한계점이 있다. 한계점을 극복하기 위한 근태 관리 방식으로 최근 GPS 또는 와이파이를 사용한 어플리케이션 기반 시스템이 출시되고 있다. 이 방식은 내근직, 외근직 근로자 모두 관리가 가능하다는 장점이 있으나 GPS 방식의 경우 실내에서 측정이 되지 않으며, 쉽게 조작이 가능하다는 단점이 있다. 이에 엘핀은 코어 기술인 셀 브로드캐스팅 서비스와 무선인프라를 결합하여 기존 GPS 위주 근태 시스템의 한계를 극복하는 서비스를 구현했다. 아래 Fig. 6은 엘핀의 서비스와 타사 서비스를 비교한 그림이다.

타사	A업체	B업체	C업체
이용 기술	GPS 또는 무선랜(WiFi)	지문 인식기	블루투스 기반 비콘(Beacon)
제공 범위	내근직(GPS/WiFi) 외근직(GPS)	내근만 관리 가능 (외근 체크 불가능)	내근만 관리 가능 (외근 체크 불가능)
주요 기능	근태 관리 스케줄 관리	출입관리 근태관리	근태관리 급여 산정
장비 설치	X	O	O
장단점	GPS 오차 발생 고객사 시스템 연동 필요 (시스템 업데이트 시 추가 개발 필요)	상대적으로 고가 (장비가 50만원대) 민감한 생체(지문) 정보 관리 리스크	장비 설치 및 주기적인 배터리 교체 필요(1~2년 주기) 작은 커버리지로 다수 설치 필요

VS

엘핀 아임히어워크
LTE 등 기지국+WiFi/비콘 +GPS 복합 위치
내근직(기지국+WiFi/Beacon+GPS) 외근직(기지국+WiFi+GPS)
내외근 근태 관리 고객 방문 관리(출장 보고 및 비용 증빙)
X
높은 위치 정확도 및 신뢰도 동시 제공 (이동통신기지국은 조작 불가능, 기지국/WiFi를 통해 GPS 오차 차단) 빠른 서비스 연동 및 공급(SDK 제공) 핵심 기능 위주로 개발(불필요 기능 제거)

Fig. 6. Comparison of “I’m Here Work” Services from L-Fin with Third-Party

엘핀의 근태관리 시스템은 학교, 학원 등에서 출결 관리로 사용할 수 있는 ‘아임히어’와 직장에서 직원들의 근태 관리용으로 사용 가능한 ‘아임히어-워크’ 두 가지 서비스로 나뉜다. 본 시스템은 셀 브로드캐스팅 서비스, 와이파이, GPS 등의 신호를 결합한 혼합 측위기반 방식으로 위치 정보가 제공된다.

최근 대학이나 학원가에서 패스워드 입력 방식의 모바일 출결 시스템을 많이 사용하고 있다. 기존 패스워드 방식의 모바일 출결 시스템은 강의실에 있는 누군가가 패스워드를 유출하면 수강생이 강의실에 있지 않더라도 출석 인증이 가능하다. 반면 '아임히어'의 경우, 사전에 관리자가 각 강의실에 있는 네트워크 주소(MAC Address)를 수집한 뒤 강의실 관리 서버에 정보를 등록 하여 관리존(Zone)을 생성한다. 이후 수강생이 강의실(Zone)에 들어오면 앱 내에 있는 출석 버튼이 자동으로 활성화 되어 출석을 인증 하게 된다.

출석 인증 외에도 수업 시간 동안 앱이 백그라운드에서 작동하여 수강생이 강의실에 머물고 있는지 여부에 대한 체크도 가능하다. 만약 사용자가 강의실을 이탈할 경우 조퇴, 일탈 등으로 기록을 남겨 기존 출결 시스템과 차별화를 시켰다. '아임히어'는 A사의 생산직 위탁교육에서 실제 사용되었다. A사는 훈련생 중 30%만 최종 합격을 시키는데 교육 기간 동안 훈련생의 출결관리 및 성실성을 보기 위한 수단으로서 서비스를 사용했다.

한편 근태/출결 관리 시스템은 엘핀이 제공하는 앱을 사용해도 되지만 기존에 사용하는 앱이 있다면 적용 할 수 있도록 SDK를 제공한다.

Fig. 7. Service scenario for L-Fin's attendance management system

4.2 아웃도어세일즈 서비스

스마트폰 등 IT의 발달로 지점을 찾는 고객이 줄어들면서 최근 증권사들이 고객에게 직접 다가가는 서비스를 마련하고 있는 추세이다. 하지만 고객 정보 보호나 지점 외부 판매 등의 컴플라이언스(compliance) 이슈가 대두되고 있다[14]. 엘핀은 증권사들의 문제점을 파악하고 문제를 해결하기 위한 위치기반 인증서비스 모델을 새롭게 구현하였다.

셀 브로드캐스팅 서비스를 활용하여 금융사 업무 태블릿 컴퓨터(Tablet Computer)의 위치를 파악하고 지점 외부에 태블릿 컴퓨터가 위치하였을 때에는 고객의 개인정보 등 민감한 정보 접근을 막아 기능을 제한하는 방식이다. 서비스는 셀 브로드캐스팅 서비스를 활용한 위치인증과 AP(Access Point)를 결합하여 위치 커버리지를 정밀화 하였다. 또한 개인정보 유출 및 법적 리스크를 사전에 방지할 수 있도록 만들었다. 한국투자증권 전 지점에서 서비스를 상용화 시키고 안정적으로 운영 중이다.

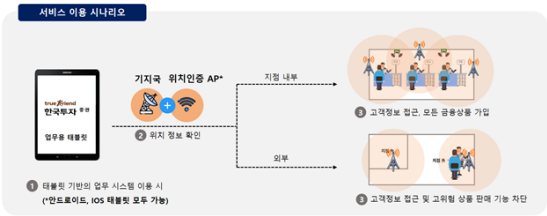

Fig. 8. Service Scenarios for Outdoor Sales

4.3 여행 금융 혜택 서비스

NH농협은행은 엘핀의 셀 브로드캐스팅 서비스 기술을 활용하여 'NH가고 싶은 대한민국 적금' 서비스를 2020년 8월 출시했다. NH 올원뱅크 고객을 대상으로 지역 방문(위치인증)에 따라 우대 금리 혜택을 제공하는 새로운 서비스이다. 본 금융 상품은 셀 브로드캐스팅 서비스를 사용해 고객이 지역에 위치에 있음을 인증하고, 우대금리를 적용해준다.

이 상품은 우리나라 전국을 9개 권역으로 나눈 뒤 고객이 여행을 하면서 인증한 권역 수에 따라 우대금리를 차등 제공는 것으로 설계되어 있다. 2개 권역에서 여행한 것을 위치기반으로 인증하면 예금 금리가 0.1%포인트가 올라가고, 3~4개 권역에서 인증하면 0.3%포인트, 5~6개 권역에서 한 기록이 있으며 1%포인트, 이런 식으로 우대금리를 적용하는 상품이다. 농촌에 기반을 두고 있어서 여행객들로 인한 농촌활성화 효과가 있음에 착안하여 여행과 금융을 콜라보한 새로운 비즈니스 모델이다.

Fig. 9. Financial Instruments Scenario for NH Nonghyup

4.4 유심(USIM)활용 출금 동의 서비스

유심 활용 출금동의 서비스는 민감한 개인정보인 CI값(주민번호 연계정보)를 활용하지 않는 출금동의 서비스이다. 기존에 출금 동의를 하기 위해서는 전자금융거래

법과 시행령에 근거하여 서면, 전자서명, 전화녹취, ARS 등 방법을 반드시 거쳐야 했다[15]. 이 과정에서 CI값이 활용되어 개인정보 유출에 대한 우려가 있다. 반면 엘핀의 서비스는 유심을 활용해 간편하게 본인 확인을 하고 출금 동의를 완료하는 것이다[15]. 입력한 이름, 생년월일 등의 정보와 휴대폰에 탑재된 유심의 가입 정보가 일치하면 인증 절차가 완료되는 시스템이다. 이는 기존과 동일한 인증 효과를 유지하면서, 보다 간편하게 출금 동의가 가능하며 개인정보 유출에 대한 우려도 감소 시켰다.

2019년도 금융위원회는 금융규제 샌드박스 시행 이후 '혁신금융서비스'로서 엘핀을 지정했다. 엘핀은 2년간 해당 서비스에 대한 배타적 운영권을 갖고 유심을 활용한 출금동의 서비스를 시작했다. 본 서비스는 현재 테스트 중이며 NH농협은행에서 정식 출시 예정이다.

Fig. 10. Service Scenario for USIM Utilization withdrawal

5. 결론

5.1 시사점

본 연구에서는 기존 시장에서 사용되는 일반적인 보안 인증보다 고도화된 셀브로드캐스팅 방식 위치인증기술의 개발에 대해서 보고하고 이와 관련하여 나타나고 있는 새로운 비즈니스 모델들을 예시하고 있다. 기존의 위치기반 서비스들이 위성통신이나 GPS에 근거한 것과는 달리 일반 핸드폰 통신에서 활용되고 있어서 그 범위와 상용성이 넓은 셀 브로드캐스팅 방식으로 위치기반인증을 하기 위한 기술적 메커니즘을 밝히고 있으며 이를 활용하여 개발되고 있는 새로운 비즈니스 모델들에 대해 연구했다는 것에 그 의의가 있다.

5.2 추가연구

추후 연구코로나19사태로 최근 다양한 분야의 기업들이 클라우드(Cloud) 또는 모바일에 기반을 둔 디지털 워크플레이스 환경을 빠르게 구축하여 업무의 생산성을 개선시키고 있다. 사용자는 더 이상 동일한 네트워크상에서 업무를 하지 않으며, 한 명의 사용자가 다양한 디바이스를 통해 업무를 보는 환경이 되었다. 2018년 HPE 이루바, 디지털 워크플레이스 연구 결과 발표에 따르면 비밀번호나 디바이스 공유 등의 위험한 행동을 한 적이 있다고 응답한 비율이 73%에 달해 직원들이 기업 데이터와 디바이스를 위험에 노출시키고 있음을 인정했다[16]. 직원의 25%가 지난 12개월 동안 안전하지 않은 개방형 와이파이에 연결한 적이 있으며, 20%는 여러 개의 어플리케이션과 계정에서 동일한 비밀번호를 사용한다고 답했다[16].

위의 조사 결과에서 보이는 바와 같이 원격 업무 보안 솔루션, 사용자 인증 등과 같은 사용자 접근에 대해 보다 강화된 인증 솔루션이 필요해 지고 있는 실정이다. 보안 측면에서 본 논문에서 연구하고 있는 시스템은 사용자 입장에서는 편리하고, 관리자 입장에서는 보다 정확하게 위치 정보를 얻을 수 있을 뿐만 아니라 보안성을 높일 수 있다는 점에서 긍정적이다.

최근 엘핀은 위치정보와 사진/생체 정보를 활용하여 크로스 체크하는 서비스 모델을 출시했다. 이러한 맥락에서 본다면 디지털 시대에 신뢰할 수 있는 전국적 전세계적 네트워크를 활용하는 본 셀브로드캐스팅 활용 위치기반인증기술은 IT환경이 다양하게 진화하면서 괄목할만한 기술이다. 공유 경제의 총아로 주목받고 있는 모빌리티에 있어서도 활용될 비즈니스모델이 나올 것으로 보이며 또한 사물인터넷의 경우에서 이를 활용한 지속적 인증 시스템의 필요성이 나타나고 있는 관계로 미래의 새로운 기술로 등장할 가능성이 높은 것으로 보인다.

References

[1] S. H. Jin, [Science Ongojisin]The Fourth Industrial Revolution and Huayibudong, Available From: https://www.etnews.com/20180218000060 (accessed Feb. 18, 2018)

[2] J. H. Kee, The Past and Present of Authentication Technology -Introduction to Concepts and Cases-, Weekly Technology Trend Report, IITP, Korea, pp.13-22.

[3] K. M. Choi, *Smartphone location-based authentication applied for the improvement of public cloud security,* Master's thesis, Dongguk University Graduate School of International Affairsand Information, Seoul, Korea, pp.15-16, 2013.

[4] H. J. Ann, *Non-facing authentication Security threat analysis and security measures: Establishment of checklist basis for minimizing non-facing authentication security threats,* Master's thesis, Konkuk University Graduate School of Information and Communication, Seoul, Korea, pp.4, 2019.

[5] S. Y. Kim, E-finance and Financial security2, p.160, Financial security institute, 2015, pp.59-94.

[6] Korea Communications Commission, A plan to promote the use of location information for fostering LBS industries and upgrading social safety nets (plan), pp.5-6, 2010.

[7] S. M. Kim, *Study on the Usage of Location-Based Services App on Smartphones: Focusing on the Perceived Risk,* Master's thesis, Hanyang cyber university Graduate School of Business, Seoul, Korea, pp.5, 2014.

[8] N. J. Park, Y. J. Song, K. Y. Moon, "Application of Certification and Security for Secure Location-Based Services", *Korea Institute Of Information Security And Cryptology,* 14, 3, pp.56-67, 2004.

[9] H. J. Seo, H. W. Kim, A Location based Two-Factor L-OTP Protocol. *The KIPS Transactions: PartC*, 18C, 5, pp.327-330, 2011.

[10] H. G. Youn, [Issue lighting] Attention to PUF technology in the coming IoT era, Available From: http://www.comworld.co.kr/news/articleView.html?idxno=49025 (accessed Jan. 12, 2021)

[11] H. W. Lee, H. G. Sine, "Consideration of strong user authentication methods for memory hacking attacks, *Korea Institute Of Information Security And Cryptology,* 23, 6, pp.67-75, 2013.

[12] Y. K. Park, Online Information Security System Utilizing Cell Broadcasting Service, The Korean Intellectual Property Office, Korea, pp.12-13, 2016.

[13] S. H. Yeom, Watch out for unlicensed car accidents in the coming holiday season, Available From: https://www.ijan.kr/news/articleView.html?idxno=2087091 (accessed July. 12, 2020)

[14] Hankyung Dotcom Newsroom, [securities firms working with startups] L-Fin's location-based authentication service is applied by Korea Investment &Securities, Available From: https://www.hankyung.com/economy/article/202008273705a (accessed Nov. 10, 2020)

[15] S. H. Yang, Even a father who is not good at Smartphones can do it in a minute. Available From: https://news.mt.co.kr/mtview.php?no=2020040309393048053 (accessed Dec. 01, 2020)

[16] IT World, HPE Aruba Announces Digital Workplace Research Results, Available From: https://www.itworld.co.kr/news/110660 (accessed Dec. 01, 2020)

최 정 문(Jeong-Moon Choi) [정회원]

- 2015년 2월 : 추계예술대학교, 영상비스니즈전공(경영학학사)
- 2020년 3월 ~ 현재 : 연세대학교 정보대학원 IoT서비스융합트랙 석사 재학 중
- 2020년 4월 ~ 현재 : ㈜다온에이치앤에스 대표이사

〈관심분야〉
스마트시티, 융합기술, 서비스혁신, 에너지IT, 기술경영

이 정 우(Jungwoo Lee) [정회원]

- 1982년 2월 : 연세대학교 영어영문학과 (인문학사)
- 1990년 2월 : 서강대학교 경영대학원(MBA)
- 1995년 5월 : 조지아주립대학교 컴퓨터정보시스템 (이학석사)
- 1998년 12월 : 조지아주립대학교 컴퓨터정보시스템 (경영학박사)
- 2001년 9월 ~ 현재 : 연세대학교 정보대학원 교수

〈관심분야〉
스마트기술응용, 서비스혁신, 워크 사이언스, 전자정부, 정보통신기술정책