Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.2, Apr. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.2.201

신뢰할 수 있는 공간에서 생체인식기반의 모바일 애플리케이션 사용자인증 기법*

이 태 경,[1†] 김 용 혁,[1] 임 을 규[2‡]
[1]한양대학교 컴퓨터·소프트웨어학과, [2]한양대학교 컴퓨터공학부

Biometric User Authentication Method of Mobile Application in Trustable Space*

Tae Kyong Lee,[1†] Yong Hyuk Kim,[1] Eul Gyu Im[2‡]
[1]Department of Computer and software, Hanyang University
[2]Division of Computer Science and Engineering, Hanyang University

요 약

모바일기기를 이용한 서비스가 증가함에 따라 개인정보 노출과 같은 보안위협이 증가하고 있다. 이러한 문제점을 해결하기 위해 생체정보와 같은 추가 인증을 통해 서비스의 안전성을 강화하기 위한 연구가 진행 중이다. 본 논문에서는 보안 강화연구의 목적으로 모바일 기기에서 활용할 수 있는 위치기반 사용자인증 시스템을 제안한다. 제안하는 위치기반 사용자인증 방식은 두 단계의 인증절차를 수행한다. 첫 번째 인증은 위치 인증으로써 현재 사용자가 애플리케이션을 신뢰할 수 있는 공간에서 접근하는지 확인하는 것이다. 이 때 사용하는 인증방식은 모바일 기기 주변의 Access Point 정보를 이용하는 위치기반 인증방식이다. 두 번째 인증은 신뢰할 수 있는 공간 인증을 통해 해당 공간에 대한 정상사용자를 확인하는 것이다. 이 방식은 사용자 생체정보를 기반으로 사용자인증을 수행한다. 제안한 인증시스템은 사용자가 신뢰할 수 있는 공간에서 개인의 생체정보를 입력함으로써 사용자 개인정보 노출의 위험도가 낮은 장점이 존재한다.

ABSTRACT

As services using mobile devices increase, exposure of personal information, and secure threats increase. In this paper, we propose a location-based user authentication system used in mobile device for tightening security. Our authentication system is performed to authenticate two steps. The first authentication is location authentication to ensure that the user accesses an application in trustable space. This authentication method uses an Access Point's information. The second authentication is trustable space authentication to confirm the normal user. This method is carried out the authentication by using biometric information from the user.

Keywords: Location-based Authentication, Access Point, Biometrics, Shaking Action

I. 서 론

오늘날 모바일기기의 확산으로 다양한 서비스를 제공하는 애플리케이션이 증가하고 있다. 이러한 애플리케이션을 사용하면서 발생하는 사용자의 개인정보는 모바일기기에 저장된다. 이로 인해 각종 보안위

Received(11. 16. 2016), Modified(1st: 02. 07. 2017, 2nd: 03. 14. 2017), Accepted(03. 16. 2017)
* 본 논문은 2016년도 하계학술대회에 발표한 우수논문을 개선 및 확장한 것임.
* 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2016-H8501-16-1013).
* 이 연구는 ETRI부설 국가보안기술연구소의 지원으로 수행되었음.
† 주저자, tt7899@hanyang.ac.kr
‡ 교신저자, imeg@hanyang.ac.kr(Corresponding author)

협으로 부터 기기 내의 사용자 개인정보가 유출될 수 있으므로, 모바일기기 내에 저장된 사용자정보를 보호하기 위해 악성코드 탐지 및 인증수단 개선과 같은 보안 해결책이 연구되고 있다.

본 논문에서는 사용자인증 연구의 일환으로 위치기반 사용자인증 방식에 대해 제안하였다. 모바일기기가 위치를 측정하는 방법은 네트워크 기반, 위성신호 기반, 그리고 AP(Access Point) 기반이 존재한다[1]. 첫째, 네트워크 기반의 위치측정은 이동통신사의 기지국 위치를 활용하여 모바일기기의 위치를 측정하는 기술이다. 기지국과 단말기 간의 신호의 방향이나 도달시간 등을 이용하여 단말기의 위치를 추정한다. 네트워크 기반의 위치정보 오차는 기지국이 비교적 많이 설치되어 있는 도심지에서는 300m이상, 교외지역에서는 수Km에 달할 정도로 오차범위가 크다.

둘째, 위성신호 기반 위치정보 측정은 인공위성으로부터 모바일기기까지 전파 도달시간을 측정하여 위성과 수신기간 거리를 파악하는 기술로서 미국에서 쏘아올린 GPS, 유럽 Galileo, 그리고 중국 COMPASS 등이 위치측정에 이용 중이다. 위성 신호 기반의 위치측정 기술은 GPS 위성을 기준으로 Standalone GPS, MS(Mobile Station)-Based GPS, MS-Assisted GPS 및 Hybrid 방식으로 구분할 수 있으며 오차는 약 50m에서 150m로 네트워크 기반의 측위 오차보다 정밀하지만 실내에서는 위성신호가 닿지 않아 사용할 수 없는 단점을 가지고 있다.

셋째, AP를 이용한 위치정보 측위는 모바일기기 주변의 Wi-Fi 정보(AP의 MAC주소, 전파세기 등)를 Wi-Fi AP의 위치정보 데이터베이스(AP MAC 주소, 위치값 등)를 활용하여 위치를 측정하는 방식으로 Wi-Fi AP의 설치가 많은 도심지, 실내 등에서 비교적 정확한 위치를 측정할 수 있는 장점이 존재한다. 그러나 사전에 Wi-Fi AP의 위치정보 데이터베이스 구축을 위해 많은 시간과 비용이 소요되고 위치측정 시 AP의 신호세기 변화에 민감하게 반응하는 단점이 존재한다.

본 논문에서는 AP의 정보 기반의 위치정보를 사용한다. AP는 도심 등을 중심으로 전국적으로 폭넓게 분포되어 있다. 또한 네트워크와 GPS기반의 방식에 비해 정확한 위치를 측정할 수 있는 장점이 있다. 또한 앞서 언급한 바와 같이 AP를 이용한 위치정보 측정은 사전에 데이터베이스 구축해야하는 단점이 존재하지만, 본 논문에서 제안하는 시스템은 사용자의 특정한 위치정보만 필요하므로 별도의 데이터베이스 구축 비용이 소요되지 않는다.

사용자가 AP를 이용하여 특정한 위치를 등록하게 되면, 등록된 위치에서만 애플리케이션이 실행된다. 본 논문에서는 신뢰 가능한 공간을 통한 사용자인증 방식을 TSA (Trustable Space Authentication)이라 정의한다. Trustable Space는 사용자가 인증을 위해 등록한 위치이다. 만약 비정상사용자가 정상사용자의 기기를 탈취하여 등록하지 않은 공간에서 애플리케이션을 실행한다면, 신뢰할 수 없는 공간으로 판단하여 애플리케이션이 정상적으로 수행되지 않는다. 또한 비정상사용자가 우연히 신뢰할 수 있는 공간에서 애플리케이션을 실행하더라도 해당 공간에 대한 인증을 수행해야하므로 비정상사용자의 접근이 난해하다.

본 논문의 구성은 다음과 같다. 2장에서는 인증시스템과 관련된 연구를 소개한다. 3장에서는 본 논문에서 제안한 인증시스템의 개요를 보이며, 4장과 5장에서는 등록절차와 인증방법을 설명하고, 6장에서는 실험 및 결과를 설명한다. 7장에서는 AP정보 관리방법과 AP정보를 조작했을 때의 대응책을 보이며, 8장과 9장에서는 향후연구 및 결론을 설명한다.

II. 관련연구

위치정보 기반의 사용자인증 방식은 해외에서 다수 연구되었다. Feng Zhang 외 2인은 위치기반 스마트폰 사용자 인증 시스템을 제안하였다[2]. 해당 시스템에서 위치 정보를 얻기 위해 활용하는 정보는 GPS와 AP 정보이다. 주로 GPS 정보를 활용하며 이에 추가적으로 AP 정보를 사용하여 위치 정보를 획득한다. 해당 논문은 사용자의 위치 정보 획득에 대한 암호화 과정이 존재하지 않아 사용자 위치정보 탈취에 취약한 단점이 존재한다.

Shraddha D. Ghogare 외 3인은 위치기반 사용자 인증 시스템을 제안하였다[3]. 해당 논문의 사용자 인증 방식은 지문 인식과 GPS를 통한 위치 정보를 활용하였다. 그러나 해당 인증 방식은 위치 정보를 활용하나 지문 인식에 의존적이라는 한계가 존재한다.

Hideyuki Takamizawa 외 1인은 iPad 및 스마트폰에 대한 위치 기반 사용자 인증 시스템을 제안하였다[4]. 해당 사용자 인증 방식은 실제 주소지의

GPS 정보와 iPad 및 스마트폰의 GPS 정보를 비교하여 사용자 인증을 하는 방식이다. 해당 방식은 GPS의 오차로 인해 인증 정확도가 감소하는 한계점이 존재한다.

Wayne Jansen 외 1인은 모바일기기의 위치 기반 사용자 인증 시스템을 제안하였다[5]. 해당 연구에서의 사용자 인증 방식은 신뢰할 수 있는 구역마다 Policy beacon이라는 장치를 설치하여 사용자의 모바일기기가 Policy beacon 근처에 있을 경우 사용자의 접근을 허용하는 방식이다. 해당 방식은 AP 기반 인증과 달리 위치마다 Policy beacon을 설치해야하므로 비용적인 측면의 한계가 존재한다.

이태경 외 2인은 Access Point 정보를 활용하여 모바일 애플리케이션의 사용자인증 시스템을 제안하였다[17]. 사용자가 주변의 AP를 등록하여 신뢰할 수 있는 공간으로 설정한 후, 등록된 AP의 전파범위 내에서만 애플리케이션이 실행될 수 있도록 하였다. 그러나 공격자가 사용자의 기기를 탈취하여 신뢰할 수 있는 공간에서 애플리케이션을 실행시킬 경우 정상적으로 접근할 수 있다는 한계가 존재한다. 본 논문에서는 이러한 상황을 고려하여 신뢰할 수 있는 공간에서도 인증을 수행할 수 있도록 하였다.

또한, 생체기반의 사용자인증에 대한 연구도 활발히 진행되고 있다. Nishkam Ravi 외 3인은 모바일기기의 가속도 센서를 이용하여 모바일기기 사용자의 행동을 분류하는 알고리즘을 연구하였다[6]. 해당 연구에서 분류하는 행동은 걷기, 뛰기, 계단 오르내리기 등이다. 사용자의 행동을 분류하기 위해 해당 연구에서는 평균, 표준편차, 에너지, 그리고 상관계수 속성을 활용하였다.

이태경 외 2인은 모바일기기의 가속도센서를 이용한 사용자인증 시스템을 제안하였다[9]. 사용자가 기기를 손에 쥐고 특정 패턴을 반복함으로써 사용자 고유 정보를 생성할 수 있다. 이러한 정보를 통해 사용자인증을 수행하였다. 그러나 모바일기기의 회전방향을 고려하지 않아 사용자 분류에 더 높은 오차가 발생할 가능성이 있다.

Kunnathu. Noufal은 모바일기기의 가속도 센서를 이용하여 모바일기기 사용자가 전화할 때의 행동을 분류하는 알고리즘을 연구하였다[7]. 해당 연구에서는 사용자의 행동을 분류하기 위해 각 축에 대하여 평균, 분산, 중력 등의 속성을 활용하였다. 행동 분류 알고리즘은 MLP 알고리즘을 사용하였으며 해당 알고리즘의 정확도는 91.43%로 나타났다. 앞선 가속도센서를 이용한 사용자인증 연구의 경우 특정 상황에서의 잡음을 제거하지 못한 한계가 존재한다. 그러나 본 연구에서는 특정시점에서의 잡음을 제거하기 위한 연구를 진행하였다.

기존연구의 경우 GPS를 통해 위치를 등록한 후 인증을 시도하지만, 건물 내부 등에서는 정확한 위치를 판단할 수 없기 때문에 인증의 정확도가 감소한다. 또한 생체정보만을 이용하여 인증 방식을 연구한 기존연구의 경우, 생체정보를 입력받을 때의 잡음 등을 고려하지 않았다. 이에 따라 사용자분류 정확도가 실제 시스템에서 안정적으로 활용할 수 있는 결과가 도출되지 않기도 하였다.

본 연구에서는 위치정보와 사용자의 생체정보를 융합한 사용자인증 시스템을 설계하였다. 위치정보의 경우 AP 정보를 사용함으로써 GPS를 이용한 방식보다 상대적으로 오차가 작다는 장점이 있다. 기존연구는 사용자가 신뢰할 수 있는 공간에만 존재한다면 애플리케이션이 정상 동작한다는 단점이 존재한다. 이에 본 논문에서는 사용자가 신뢰할 수 있는 공간에 존재하여도 해당 공간에 대한 사용자 개인의 생체정보를 입력해야 애플리케이션이 정상 작동하도록 하였다.

III. 사용자인증 시스템 개요

본 논문에서 제안하는 사용자인증 시스템은 3가지 인증을 복합적으로 사용하며 Fig. 1. 과 같다. 1차 인증은 일반적으로 사용하는 문자 기반 암호 방식으로써 아이디와 패스워드로 구성된다. 다양한 서비스에서 보편적으로 사용하는 인증방식이며, 본 논문에서는 1차 인증 정보를 서버와 통신 및 저장하는 과정에서 모두 암호화한 것으로 가정하였다.

2차 인증은 신뢰할 수 있는 공간(Trustable Space)에서 인증을 수행하는 것이다. 이 방식은 사용자가 신뢰할 수 있는 공간에서 애플리케이션을 실행하고자 할 때 사용되는 인증방식이다. 이를 위해 사용자는 우선 사용자가 신뢰할 수 있다고 판단되는 공간을 등록한다. 신뢰할 수 있는 공간을 탐색하기 위해 현재 사용자 주변의 AP 정보를 이용한다.

3차 인증은 2차 인증을 보완하는 방식으로써 비정상 사용자가 악의적 혹은 우연적으로 정상 사용자의 신뢰공간에서 인증을 수행하는 것을 방지하기 위한 것이다. 이 방식은 사용자의 생체정보를 이용하여 신뢰할 수 있는 공간을 정상 사용자만 인가할 수 있도록 한 것이다. 즉, 비정상 사용자가 정상 사용자가

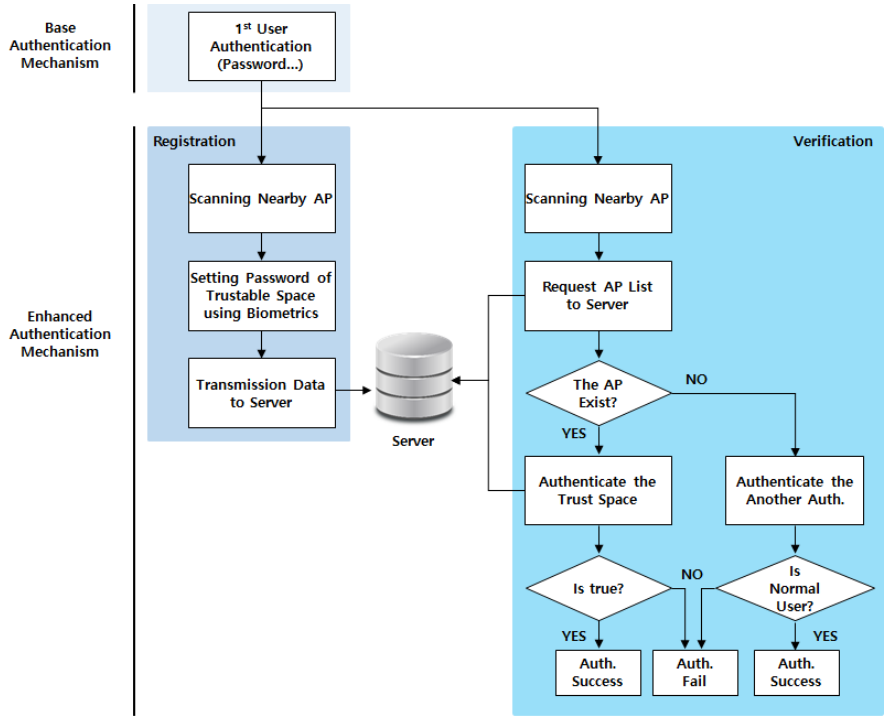

Fig. 1. Authentication system flow chart that we have proposed

등록한 신뢰할 수 있는 공간에서 애플리케이션 실행을 시도하더라도 3차 인증을 수행해야만 정상적으로 동작하도록 설계되어 있다.

3차 인증에서 사용하는 생체정보는 다음과 같은 비정상 접근도 차단할 수 있다. 비정상 사용자가 애플리케이션을 동작시키기 위해 새로운 공간을 등록할 때, 생체정보를 등록해야 한다. 그러나 등록하고자 하는 생체정보가 기존 정상 사용자의 생체정보와 상이할 경우 다른 사용자로 판단하여 등록 및 접근을 거부한다.

인증부분에 대해 요약하면 다음과 같다. 첫째, 사용자주변의 AP를 탐색한다. 탐색한 AP목록을 서버에 전송하고, 서버에 해당 AP가 존재하는지 확인한다. 만약 존재하지 않는다면 신뢰할 수 없는 공간으로 판단하여 추가적인 인증을 수행할 수 있도록 유도하거나 애플리케이션을 제약적으로 실행시킨다. 하지만 신뢰할 수 있는 공간이라 판단되면 사용자에게 현 위치에서 등록한 생체인증을 수행할 수 있도록 한다. 이때, 등록한 정보와 일치하면 애플리케이션 접근을 허가하고, 그렇지 않으면 거부한다.

1차 인증, 2차 인증, 그리고 3차 인증을 수행할 때의 모든 과정에서는 암호화하여 전송한다. 다음 4장과 5장에서 등록부분과 인증부분에 대해 자세히 설명한다.

IV. 신뢰할 수 있는 공간의 등록

4.1 수동등록

사용자가 현 위치에서 애플리케이션이 동작하기 원할 주변 AP 정보를 등록해야 한다. 즉 사용자만의 신뢰할 수 있는 공간을 설정해야 한다. 등록과정은 Fig. 2.와 같다.

첫째, 2차 인증으로써, 모바일기기는 주변 AP 정보를 탐색한다. AP 정보를 탐색하는 과정에서 신호세기가 강한 순으로 상위 3개 이하의 AP 정보를 추출하며, 신호세기 측정은 RSSI(Received Signal Strength Indicator)를 이용한다. 탐색한 AP 정보가 3개 미만일 경우 신호 세기와 관계없이 모든 AP 정보를 추출한다.

둘째, 3차 인증으로써, 등록하고자 하는 공간에 대해 사용자의 생체기반 정보를 통해 해당 공간의 접근을 제어한다. 이 방식은 사용자가 신뢰할 수 있는 공간에서 애플리케이션을 실행시키더라도 해당 공간

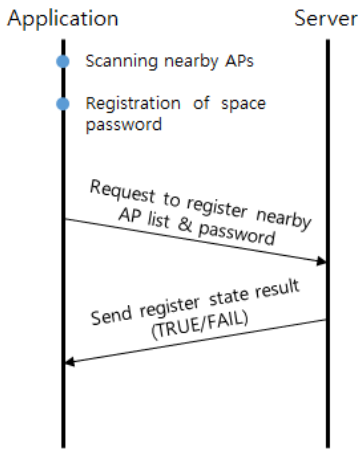

Fig. 2. Flow chart of trustable space's registration

에서 등록한 생체기반 정보(터치정보, 디바이스 흔들기 등)가 다를 경우 인증에 실패하게 된다. 문자기반 암호방식은 1차 인증(아이디, 패스워드)에서 사용하고, 하나이상의 신뢰공간에 대한 암호를 등록해야 하므로 간편하면서 신뢰할 수 있는 인증방식인 생체기반 인증을 사용한다. 자세한 설명은 5장에서 언급한다.

셋째, 탐색한 AP 정보를 1차 인증으로 사용하는 사용자계정(아이디, 패스워드)과 신뢰할 수 있는 공간에 대한 생체기반 정보를 서버로 전송한다. 전송과정에서는 모든 정보를 암호화하여 스니핑 공격이나 중간자 공격 등으로부터 보호한다. 또한 서버는 수신한 정보를 데이터베이스에 저장하고 결과를 애플리케이션에 송신한다. 데이터베이스 상에서도 모든 정보를 암호화하여 저장한다.

4.2 자동등록

AP를 이용한 위치등록 방법은 사용자가 직접 현 위치의 AP를 수동으로 등록하는 방법과 애플리케이션이 자동으로 등록하는 방법으로 구분된다. 수동등록은 앞 절에서 언급한 방식이며, 본 절에서는 자동등록 방식에 대해 기술한다.

본 논문에서 제안하는 자동등록 방식은 와이파이를 사용하는 사용자의 행동패턴과 관련 있다. 일반 사용자는 가정집, 학교, 그리고 회사 사무실과 같이 신뢰할 수 있는 공간 또는 자주 머물러 있는 공간에서 와이파이를 실행한 후 인터넷을 사용한다. 이러한 특징을 이용하여 사용빈도가 높은 AP들에 한하여 해당 위치를 자동 등록한다. 자동으로 사용빈도가 높은 AP를 등록하기 위해 애플리케이션은 사용자가 와이파이를 실행하거나 와이파이 정보가 변경될 때마다 해당 AP 정보를 기기 내부에 저장한다. 누적된 AP 정보를 통해 일정 횟수 이상 이용한 AP를 신뢰할 수 있는 공간으로 판단하여 사용자의 생체정보를 입력 받은 후, 해당 AP 목록을 서버에 전송한다.

4.3 신뢰할 수 있는 공간에 대한 생체기반 정보 등록

사용자가 신뢰할 수 있는 공간을 등록할 때, 해당 공간에 대한 사용자 고유의 암호를 설정해야 한다. 즉, 등록과정에서 신뢰할 수 있는 공간과 해당 공간에 대한 암호를 같이 등록하고, 인증할 때 역시 해당 공간에서 사용자 고유의 패스워드를 이용해야 한다. 예컨대, 사용자와 친밀한 주변 사람이 정상 사용자의 기기를 탈취하여 1차 인증을 통과한 후, 사용자가 자주 머물러 있는 공간에서 애플리케이션을 실행한다면 불가피하게 인증에 성공할 수밖에 없다. 이러한 문제점으로 인해 3차 인증이 필요하고, 이 인증이 신뢰할 수 있는 공간에 대한 인증이다.

전체 3가지 인증을 거쳐 애플리케이션을 실행할 경우, 사용자의 편의성이 저하될 수 있다. 신뢰성과 편의성은 트레이드오프관계이므로 신뢰성과 편의성을 최대한 모두 높일 수 있는 인증방법을 채택해야 한다. 따라서 본 논문에서는 생체기반인증 방식을 공간 암호인증에 활용하였다.

생체기반인증 방식은 홍채인식, 지문인식, 그리고 얼굴인식과 같은 정적인증방식이 존재하며, 걸음걸이, 터치패턴, 그리고 디바이스 움직임과 같은 동적 인증방식이 존재한다. 동적 생체정보 인증방식은 다시 명시적 인증방식과 암시적 인증방식으로 구분된다. 명시적 인증방식은 터치패턴, 디바이스 움직임 패턴 등이 존재하며, 암시적 인증방식은 걸음걸이, 배터리 사용패턴을 이용한 방식이다. 명시적 인증방식은 비교적 인증과정이 간단한 반면에 암시적 인증방식은 장기적인 데이터가 필요로 하다. 최대한 간편하고 신속한 인증방식을 위해, 본 논문에서는 명시적 인증방식 중 디바이스 흔들림을 사용하였다. 특히 사용자가 위치하는 신뢰공간마다 다른 생체정보가 있을 것이라는 가정 하에 각 공간에 따른 인증방식을 사용하였다.

V. 신뢰할 수 있는 공간에서의 인증

5.1 위치 인증

AP를 이용한 사용자인증 방식은 Fig. 3.과 같다. 우선 사용자가 애플리케이션을 실행한 후 아이디와 패스워드를 입력하여 1차 인증을 수행할 때, 현재 사용자가 신뢰할 수 있는 공간에서 애플리케이션을 실행하였는지 확인한다(2차 인증). 이를 위해 Fig. 3.과 같이 모바일기기는 주변 AP 목록을 검색한다. 만약 모바일기기의 네트워크 연결이 와이파이가 아닐 경우 일시적으로 와이파이를 실행하여 주변 AP 정보를 탐색한다. 탐색 후, 등록방식과 동일하게 와이파이 신호세기가 강한 3개 이하의 AP를 선정한다. Fig. 4.는 모바일기기 주변에 AP1과 AP2가 존재하며, 사전에 등록된 AP가 AP1임을 나타낸다.

이후에 1차 인증 정보(사용자 계정)와 2차 인증 정보(AP 목록)를 서버에 암호화하여 전송하고 서버는 수신한 정보를 복호화하여 현재 위치에서 등록된 AP 정보 존재여부를 데이터베이스 내에서 탐색한다.

$$AP_i \in \{AP_1, AP_2, \cdots, AP_n\}, (1 \le i \le n) \qquad (1)$$

서버에서 현재 사용자가 신뢰할 수 있는 공간에

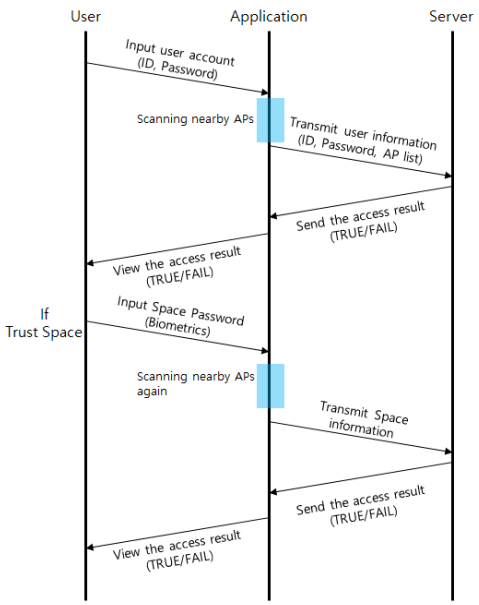

Fig. 3. Flow chart of trustable space's Authentication

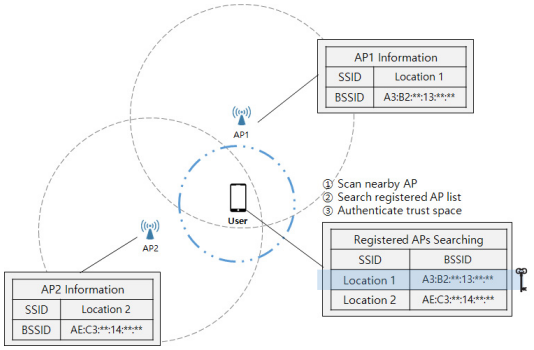

Fig. 4. Searching of AP list in trustable space

위치하는지 확인하는 방법은 식 (1)과 같다. 집합 내의 각 원소는 한 사용자가 등록한 n개의 AP 전체 목록이며, AP_i는 현재 사용자가 위치해 있는 AP이다. 서버에서는 3개 이하의 수신된 AP 목록 중에 적어도 하나 이상 등록된 AP 정보가 데이터베이스에 존재할 경우, 신뢰할 수 있는 공간에서 애플리케이션을 실행한 것으로 판단하여 3단계 인증절차를 수행할 수 있도록 한다. 만약 등록된 AP 정보가 서버에 존재하지 않다면 정상적으로 애플리케이션을 실행할 수 없거나 추가 인증을 수행해야 한다. 예를 들어, Fig. 4.처럼 기존에 신뢰할 수 있는 공간으로 등록된 부분은 AP1의 Location 1이다. 따라서 Location 1의 전파영역에 내에서 등록했던 공간인증을 수행하게 되면, 정상적인 애플리케이션이 수행된다.

사용자가 등록한 신뢰할 수 있는 공간은 AP의 전파영역과 등록한 AP의 개수에 따라 달라지며, 이에 따른 인증구역도 달라진다. 예를 들어 Fig. 5.와 같이 사용자가 Location 4에서 공간을 등록하였을 경우, 앞선 등록과정 설명에서와 같이 사용자 주변의 와이파이 신호세기가 강한 최대 3개의 AP를 등록하게 된다. 따라서 등록되는 신뢰할 수 있는 공간은 Location 4 뿐만 아니라 Location 1 부터 Location 8까지 등록된다. 즉, 사용자는 Location 8에서 인증이 가능하지만, AP1, AP2, 그리고 AP3의 전파영역 외에서는 인증이 불가능하다. 예를 들어, Location 9는 3개의 AP전파영역에 외부에 위치하므로, 신뢰할 수 있는 공간이 아니라 판단하게 된다.

경우에 따라 Fig. 6.과 같이 애플리케이션이 신뢰 공간 인증을 위해 AP를 탐색하는 도중에 사용자가 기기를 가지고 신뢰할 수 있는 공간을 이탈하는 경우

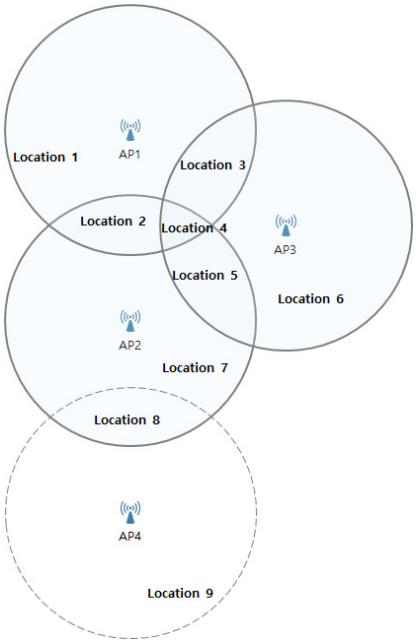

Fig. 5. Example of Detected AP area

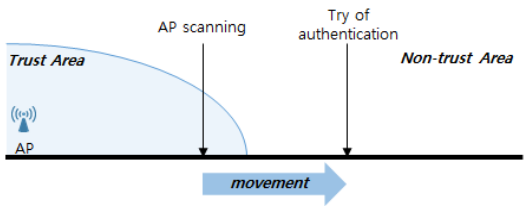

Fig. 6. Try of authentication in non-trust area

문제가 발생한다. 즉, 인증 지연시간으로 인해 신뢰 공간 외부에서 인증이 성공할 수 있는 문제이다. 이 때문에 3차 인증을 수행하기 전에, 주변 AP를 재탐색하여 해당 AP목록을 서버에 전송한다.

5.2 신뢰할 수 있는 공간에서 생체기반 인증

위치 인증이 완료된 후, 신뢰할 수 있는 공간으로 판단되면 사용자에게 기존에 해당 영역에 등록한 생체기반 정보를 입력할 수 있도록 한다. 본 논문에서는 사용자가 제한된 시간에 모바일기기를 특정한 형태로 반복해서 흔듦으로써 공간에 대한 인증, 즉 3차 인증을 수행할 수 있도록 하였다. 기기의 흔들림을 통한 공간 인증을 위해 기기가 어느 방향으로 움직이는지와 회전방향이 어떤지를 확인할 필요가 있다. 따라서 우리는 가속도센서를 통해 움직이는 방향을 측정하고, 가속도센서와 자기장센서를 이용하여 회전 각도를 측정하였다.

5.2.1 사이클 추출

사용자 특징정보를 추출하기 위해 선행적으로 처리해야할 부분은 가속도 데이터로부터 사이클을 추출하는 것이다[8]. 가속도 데이터로부터 사이클을 추출하기 위해 3축의 가속도 정보 중에서 x축을 기준으로 사이클을 추출하였다. 사이클의 구분은 x축 가속도 데이터가 음수에서 양수로 변경되는 시점을 사이클의 초깃값으로 설정하였고, 다시 음수에서 양수로 변경되는 시점을 끝점으로 설정하여 하나의 사이클로 결정하였다.

5.2.2 사용자 특징정보

사이클 구분이 완료된 후, 각 사이클로부터 특징정보를 추출한다. 사전에 정의한 특징정보는 하나의 사이클에 대해 가속도 센서와 회전 3축, 총 6축에 대해 최댓값, 최솟값, 평균, 표준편차, 그리고 사이클의 길이다. 또한 식 (2)와 같이 사이클 내 3축의 벡터 크기 평균을 추가하여 총 26개의 특징정보를 추출하였다.

$$MAG_{avg} = \sqrt{\frac{1}{N}\sum_{k=i}^{n}\left(x_k^2 + y_k^2 + z_k^2\right)} \quad (2)$$

다음 Table 1. 은 26개의 특징정보를 나타낸 것이다.

본 논문에서는 26개의 특징정보 중에서 유용한 특징정보를 선정하여 사용자분류 과정에서 발생하는 오버헤드를 축소할 수 있도록 하였다. 이를 위해 통계학에서 사용하는 주성분 분석(PCA, Principal Component Analysis)[10]을 이용하였다. 주성분 분석은 고차원의 데이터를 저차원의 데이터로 환원시키는 방법이다. 즉, 26개의 고차원 특징정보를 저차원의 특징정보로 축소하여 높은 분류정확도와 신속한 인증이 수행될 수 있도록 하였다. 다음 식 (3)은 26개의 특징정보 중에서 유용한 특징정보를 추출하기 위한 식이다.

$$FS_i \in \{w_1F_1, w_2F_2, w_3F_3, \cdots, w_{26}F_{26}\} \quad (3)$$

Table 1. List of 26 Features (SD : Standard Deviation)

Feature Type	X-coordinate value	Y-coordinate value	Z-coordinate value
Acceleration	Max	Max	Max
	Min	Min	Min
	Mean	Mean	Mean
	SD	SD	SD
	The length of cycle		
	Average of magnitudes		
Rotation	Pitch Max	Roll Max	Azimuth Max
	Pitch Min	Roll Min	Azimuth Min
	Pitch Mean	Roll Mean	Azimuth Mean
	Pitch SD	Roll SD	Azimuth SD

$$NF_k = FS_x + FS_y + FS_z + FS_p + FS_q \quad (4)$$
$$(1 \le x, y, z, p, q \le 16)$$

식 (3)의 F_i는 특징정보를 나타내고, w_i는 해당 특징정보에 대한 가중치를 나타내며, FS_i는 각 특징정보와 가중치를 곱한 것을 벡터로 표현한 것이다. 이후 식 (4)와 같이 식 (3)의 벡터 내에서 일부 원소를 추출한 후, 합산하여 새로운 특징정보로 선정한다. NF_k는 새로운 특징정보를 나타낸다. 새로운 특징정보 선정 기준은 6장에서 다룬다.

5.2.3 비정상 사이클 제거

공간인증을 위해 제한된 시간동안 모바일기기를 반복적으로 흔들 경우 인증시간 전후로 비정상 사이클이 발생한다. 또한 특정한 구간에서도 전반적인 사이클 형태와 상이한 사이클이 형성되기도 한다. 이러한 비정상 사이클은 공간인증을 위한 사용자 분류정확도를 감소시킬 수 있다. 따라서 본 논문에서는 비정상 사이클을 제외시켰다.

$$\sigma(x_{each\ cycle}) \le c \times E\left(\left(\sigma(x_{each\ cycle})\right)\right) \quad (5)$$

비정상 사이클을 배제하기 위해 식 (5)와 같이 전체 사이클에 대한 표준편차의 평균을 계산한다. 이후에 하나의 사이클 표준편차가 전체 사이클의 표준편차 평균의 $c\%$ 미만일 경우 비정상 사이클로 판단한다. 상수 c는 실험을 통해 도출하였으며, 50%일 때, 분류정확도가 가장 높은 것으로 파악하였다.

VI. 실험 및 결과

6.1 실험 방법

실험 애플리케이션이 설치된 기기(삼성 갤럭시 노트4, 안드로이드 6.0.1 버전)를 사용하여 30명을 대상으로 실험을 진행하였다. 2차 인증 실험을 위해 와이파이가 실행되었을 때와 실행되지 않았을 때를 고려하였다. 특히 와이파이가 실행되지 않았을 경우, 자동으로 와이파이를 실행하여 AP목록을 수집하고 서버에 전송할 수 있는지 확인하였다. 다만 모바일 네트워크 연결이 해제되었을 경우(비행기 모드 등)는 배제하였다. 뿐만 아니라 자동등록이 정상적으로 수행되는지 확인할 수 있도록 하였다. 3차 인증의 경우 실험대상자에게 5초간 기기를 일정한 패턴으로 흔들도록 하였다. 기기를 흔드는 동안 실험대상자의 이동을 금지하였다.

6.2 위치기반 인증 실험결과

위치기반 인증은 사용자가 기존에 등록한 위치, 즉 신뢰할 수 있는 공간에서 애플리케이션을 실행하는지를 파악하는 것이다. 이를 위해 실험대상자에게 수동으로 신뢰할 수 있는 공간을 등록하게 하였다. 이후, 등록한 위치에서 인증을 시도하여, 모두 정상적으로 수행되는지 확인하였다.

본 인증 시스템은 신호세기가 강한 AP 정보 3개 이하를 서버에 전송하여, 신뢰할 수 있는 공간인지 판단한다. 이 때문에 등록한 AP로부터 신호세기가 약한 곳으로 이동하여 인증을 시도하였을 때, 신호세기가 강한 AP들에 의해 인증이 실패하였다. 즉, 등록한 AP의 전파영역 내에 존재하나, 신호세기가 강한 AP에 의해 신뢰할 수 없는 공간으로 오판한 것이다.

6.3 신뢰할 수 있는 공간의 인증 실험결과

공간 인증을 위해 실험에서 수집한 데이터베이스 파일을 기반으로 사용자특징정보 추출 및 비정상 사

이클 제거를 수행하였다. 이후 분류정확성 평가를 위해 데이터마이닝 오픈소스도구인 Weka[11]를 이용하였다. 본 논문에서는 SMO(Sequential Minimal Optimization)[12], Logistic[13], Simple Logistic, Random Forest[14], J48[15], 그리고 MLP(Multi-Layer Perceptron)[16] 알고리즘을 이용하였다.

또한 Weka에서 주성분 분석 기능을 제공하므로, 이를 통해 식 (3), (4)와 같이 유용한 특징정보만 선정하여 분류정확도를 평가하였다. 선정된 특징정보 중에서도 다음 식을 이용하여 특징정보를 엄선하였다.

$$\sigma(NF_k) \geq MAX(\sigma(NF_{SET})) \times threshold \quad (6)$$

식 (6)의 $\sigma(NF_k)$는 새로운 특징정보의 표준편차이며, $MAX(\sigma(NF_{SET}))$는 각 특징정보의 집합 중에서 표준편차가 가장 큰 특징정보의 값을 나타낸다. 본 논문에서 임계값(threshold)은 0.5로 고정하였다. 식 (6)에 부합하는 특징정보만을 사용하여 분류정확도를 측정하였다. 다음 Table 2. 는 비정상 사이클 제거비율이 75%일 때를 사용하는 특징정보를 나타낸 것이다.

본 논문에서는 사용자분류 정확도와 EER(Equal Error Rate), 분류 모델링 시간을 파악하였다.

Table 2. Feature list by equation (6) and the abnormal cycle removal rate (%)

Removal Rate	Features
75%	-0.322pitchMean-0.317azimuthMax+0.294Ymin-0.283XstdDev-0.264rollMin
	0.428Xmagnitude-0.371rollStdDev+0.317rollMean-0.315azimuthStdDev-0.262Zmin
	0.382Ymax+0.375rollMax+0.358YstdDev-0.324pitchStdDev+0.259Length
	-0.41rollMin+0.387Ymean-0.313pitchStdDev+0.266Ymax+0.228XstdDev
	-0.6Zmax-0.42ZstdDev+0.393azimuthMin-0.33Zmean-0.245azimuthMax.
	0.482pitchMin+0.482pitchMax+0.341Xmin+0.262azimuthMean+0.244Xmean

EER은 오인식률과 오거부율이 같아지는 비율을 의미한다. FAR은 정상 사용자의 생체정보가 아닌 것을 정상사용자의 것으로 잘못 판단하는 확률을 의미한다. 또한 오거부율은 사용자의 생체정보를 본인이 아닌 것으로 잘못 판단하는 확률을 의미한다. 일반적으로 EER이 낮은 인증수단은 유용한 인증수단으로 분류된다. 본 논문에서 분류 모델링 시간을 파악하는 이유는 사용자인증 시스템의 성능과 관련이 있다. 알고리즘의 분류 모델링 시간이 길면 인증과정이 오래 걸리므로 인증 시스템으로는 부적합하다. 따라서 분류 모델링 시간이 짧고, EER이 낮고, 분류정확도가 높은 알고리즘을 선택하여 인증 시스템에서 사용할 수 있도록 한다.

6.3.1 비정상 사이클 분류에 따른 분류 정확도

본 논문에서는 정확한 사용자 분류를 위하여 비정상 사이클을 제거하는 과정을 추가하였다. 수집된 실험 데이터를 기반으로 비정상 사이클 제거 비율에 따른 분류정확도를 측정하였다. Table 3. 은 식 (5)의 상수 C를 50%, 75%, 그리고 85%로 나누어 6개의 알고리즘에 따른 분류정확도를 나타낸 것이다. 비정상 사이클 제거비율을 50% 미만으로 사용하지 않는 이유는 비정상적으로 분류정확도가 높게 나올 수 있기 때문이다. 만약 이러한 비정상 사이클을 제거하지 않거나 제거비율이 낮다면 의도하지 않은 비정상 사이클을 정상 사이클로 인지할 수 있다. 반면에 비정상 사이클 제거비율을 90% 이상으로 사용하지 않는 이유는 정상 사이클을 비정상 사이클로 판단하여 제거할 수 있기 때문이다.

비정상 사이클을 85%로 제거하였을 경우 알고리

Table 3. Classification accuracies by the classification algorithms and the abnormal cycle removal rate (%)

Algorithm	50%	75%	85%
J48	87.66	88.89	82.92
Logistic	96.75	93.65	95.30
Simple Logistic	97.84	97.02	95.79
MLP	98.70	97.02	96.29
SMO	70.78	62.50	56.19
Random Forest	96.97	95.44	86.13
Average	91.45	89.09	85.44

Table 4. Classification accuracies, Equal Error Rate, and Modeling time by the classification algorithms

Algorithm	EER (%)	Modeling Time (s)
J48	6.0	0.02
Logistic	0.2	0.65
Simple Logistic	0.4	0.59
MLP	0.4	3.05
SMO	2.0	0.56
Random Forest	0.1	0.14
Average	1.52	0.83

즘의 분류정확도가 평균 85.44%가 나타났다. 75%로 제거하였을 경우 89.09%가 나타났으며, 50%로 제거하였을 경우 평균 분류정확도가 91.45%로 가장 높게 나타났다.

Table 4.는 비정상 사이클을 50%로 제거하였을 때의 분류정확도, EER, 그리고 분류 모델링 시간을 나타낸 것이다. 각 분류알고리즘의 EER 평균은 1.52%가 나타났으며, 모델링 시간은 평균 0.84초로 나타났다. 앞서 언급한 바와 같이 높은 분류정확도와 낮은 EER 값, 그리고 적은 분류 모델링 시간을 갖는 최적의 분류 알고리즘은 Random Forest이다. 그 뒤를 이어 Simple Logistic 알고리즘과 Logistic 알고리즘이 사용자인증에 적합한 알고리즘으로 나타났다.

VII. AP정보 관리 및 AP정보 조작 대응

사용자는 여러 위치에서 등록한 AP 정보를 확인할 수 있으며, 원하는 신뢰할 수 있는 공간을 수정 및 삭제할 수 있다. Table 5. 는 사용자가 등록한 AP 정보 예시를 보여준다. 사용자에게 SSID, 등록 날짜, IP를 보여줌으로써 어떠한 AP들이 등록되었는지 확인할 수 있게 한다. 또한 사용자는 AP 목록 중에서 삭제하기 원하는 위치의 AP를 선택하여 해당 위치를 제거할 수 있다. Table 5.에서 Auto 항목은 사용자가 신뢰할 수 있는 위치를 자동으로 등록한 것인지 혹인 수동으로 등록한 것인지를 나타낸다. 자동으로 등록하였을 경우 'T'로 표시하며, 수동으로 등록하였을 경우 'F'로 표시한다.

본 시스템의 데이터베이스에서는 IP주소와 MAC 주소를 결합하여 킷값으로 사용한다. 그러나 일반적으로 AP의 IP주소는 DHCP를 통해 할당받으므로 공인 IP를 이용한 경우보다 IP 갱신 횟수가 빈번하게 발생한다. 이는 신뢰할 수 있는 공간의 킷값이 빈번하게 변경될 수 있음을 의미한다. 이에 본 시스템에서는 AP의 공인 IP와 MAC주소를 킷값으로 사용하고, DHCP로부터 할당받은 유동 IP를 추가적으로 관리한다. 즉, 유동 IP가 변경되어도 공인 IP가 변경되지 않았을 경우에는 해당 공간의 유동 IP만 변경하면 된다. 그러나 공인 IP가 변경되었을 경우에는 유동 IP와 함께 변경되므로 이에 대한 고려는 향후 연구에서 진행하도록 한다.

AP 정보를 이용한 위치기반 사용자인증 방식은 등록된 위치가 아닌 곳에서 애플리케이션 실행할 수 없다. 그러나 공격자가 비인가 된 AP 정보를 등록된 AP 정보로 수정할 경우 애플리케이션 실행이 가능하다. 이러한 AP 정보 조작에 대응하기 위해 Table 5.와 같이 AP의 MAC 주소와 공인 IP 주소를 대응하여 위치등록 및 인증을 수행할 수 있도록 하였다. 만일 AP의 MAC 주소가 변조되더라도 IP 정보가 다를 경우 신뢰할 수 없는 AP라고 판단한다.

Table 5. Example of AP list in database

SSID	DATE	MAC	IP	AUTO
SSID1	DATE1	MAC1	IP1	T
SSID2	DATE2	MAC2	IP2	F
SSID3	DATE2	MAC3	IP3	F
SSID4	DATE2	MAC4	IP4	F

VIII. 향후연구

본 장에서는 인증시스템에서 보완돼야할 것을 서술한다. 앞서 7장에서 언급한 바와 같이 AP 정보는 AP의 공인 IP 주소와 MAC 주소를 결합하여 관리한다. 그러나 일반적인 AP의 경우 고정 IP를 사용하는 것이 아닌 DHCP를 통해 IP를 배정받아 사용하고 있다. 이 경우, AP의 MAC 주소, 고정(외부) IP, 그리고 DHCP로부터 배정된 유동 IP를 결합하여 사용할 수 있다. 만약 AP가 재부팅되는 확률이 낮다고 가정한다면, 유동 IP가 변경될 가능성 또한 낮다. 향후 연구에서는 MAC주소, 고정IP, 그리고 유동 IP를 결합하였을 때의 인증과정이 무결한지 실

험할 수 있도록 한다. 추가로 AP가 위장되었을 경우 자동등록 방식에서도 AP정보 조작에 대응할 수 있는지, 재전송 공격과 같은 통신과정에서 발생할 수 있는 공격방식들에 대한 안전성을 실험할 수 있도록 한다.

IX. 결 론

최근 모바일기기를 이용한 서비스가 증가함에 따라 모바일 보안위협도 증가하고 있다. 기기가 탈취되거나 비인가 사용자가 애플리케이션을 접근할 경우 개인정보 노출 위협이 발생한다. 이러한 문제점을 방지하고자 본 논문에서는 AP 정보를 이용한 위치기반 사용자인증 강화 시스템을 제안하였다.

이 방식은 사용자가 신뢰할 수 있는 공간을 등록하여 해당 위치에서만 애플리케이션이 동작하는 방식이다. 사용자가 신뢰할 수 있는 공간을 등록한 후, 해당 공간에 대한 인증을 수행하기 위하여 사용자의 생체정보를 이용하였다. 본 논문에서는 모바일기기의 움직임을 통한 신뢰 공간 인증을 수행할 수 있도록 하였다. 인증방식은 신뢰할 수 있는 공간 내에서 애플리케이션이 동작할 경우, 주변의 AP를 탐색하여 신뢰공간인지를 확인한 후, 일치한다면 해당 공간에 대한 생체정보인증을 수행함으로써 애플리케이션 접근을 승인할 수 있도록 하였다.

기존연구의 경우 GPS를 이용하기 때문에 공간에 대한 오차가 크다. 그러나 본 연구에서는 AP 정보를 사용하기 때문에 GPS를 이용한 방식보다 상대적으로 공간 오차 범위가 작다는 장점이 존재한다. 또한, 기존연구는 사용자가 신뢰할 수 있는 공간에만 존재한다면 애플리케이션이 정상 동작한다. 그러나 비정상 사용자가 악의적 또는 우연적으로 정상 사용자가 신뢰할 수 있는 공간에서 애플리케이션을 실행시킨다면 인증에 성공하게 된다는 단점이 존재한다. 따라서 본 논문에서는 사용자가 신뢰할 수 있는 공간에 존재하여도 해당 공간에 대한 사용자 개인의 생체정보를 입력해야 애플리케이션이 정상 작동한다.

References

[1] 2014 Mobile Internet Usage Survey Summary Report, Korea Internet & Security Agency : www.kisa.or.kr/uploadfile/201412/ 201412291354455289.pdf

[2] Zhang, Feng, Aron Kondoro, and Sead Muftic, "Location-based authentication and authorization using smart phones, Trust, Security and Privacy" 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 1285-1292, June. 2012.

[3] Ghogare, S. D., Jadhav, S. P., Chadha, A. R., and Patil, H. C., "Location based authentication: A new approach towards providing security." International Journal of Scientific and Research Publications, 2.4, pp.1-5, 2012.

[4] Takamizawa, Hideyuki, and Noriko Tanaka, "Authentication system using location information on ipad or smartphone" International Journal of Computer Theory and Engineering, 4.2, pp.153-157, 2012.

[5] Jansen, Wayne, and Vlad Korolev, "A location-based mechanism for mobile device security." Computer Science and Information Engineering, 2009 WRI World Congress on. IEEE, Vol. 1, pp. 99-104, Mar. 2009.

[6] Ravi, N., Dandekar, N., Mysore, P., and Littman, M. L, "Activity recognition from accelerometer data" AAAI. Vol. 5, pp. 1541-1546, 2005.

[7] Kunnathu, Noufal, "Biometric User Authentication on Smartphone Accelerometer Sensor Data." Proceedings of Student-Faculty Research Day, CSIS, Pace University, 2015.

[8] Derawi, Mohammad O., Patrick Bours, and Kjetil Holien, "Improved cycle detection for accelerometer based gait authentication." Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on. IEEE, pp. 312-317. 2010.

[9] Tae Kyong Lee, Jun Hyoung Kim, Eul Gyu

Im, "User Authentication Using Accelerometer Sensor of Mobile Device" Korea Computer Congress, 2016.
〔10〕 Jolliffe, Ian, "Principal component analysis." John Wiley & Sons, Ltd, 2002.
〔11〕 Witten, I. H., Frank, E., Trigg, L. E., Hall, M. A., Holmes, G., and Cunningham, S. J., "Weka: Practical machine learning tools and techniques with Java implementations." 2009.
〔12〕 Cao, L. J., Keerthi, S. S., Ong, C. J., Zhang, J. Q., Periyathamby, U., Fu, X. J., and Lee, H. P., "Parallel sequential minimal optimization for the training of support vector machines." IEEE Transactions on Neural Networks, 17.4, pp. 1039-1049 July. 2006,
〔13〕 Logistic Algorithm, http://weka.sourceforge.net/doc.dev/weka/classifiers/functions/Logistic.html. (last visited on 13 Sep 2016)
〔14〕 Liaw, A., and Wiener, M., "Classification and regression by randomForest." R news, 2.3, pp. 18-22, Dec. 2002.
〔15〕 Patil, T. R., and Sherekar, S. S., "Performance analysis of Naive Bayes and J48 classification algorithm for data classification." International Journal of Computer Science and Applications, 6.2, pp. 256-261, Apr. 2013.
〔16〕 Yang, Z. R., "Multi-layer Perceptron." Machine Learning Approaches To Bioinformatics. World Scientific, pp. 133-153, 2010.
〔17〕 Tae Kyong Lee, Wang Le, Eul Gyu Im, "Enhanced Location-based User Authentication On Mobile Application Using Access Point Information." Conference on Information Security and Cryptography, 2016.

〈저자소개〉

이 태 경 (Tae Kyong Lee) 학생회원
2015년 2월: 광운대학교 컴퓨터소프트웨어학과 졸업
2015년 3월~현재: 한양대학교 컴퓨터소프트웨어학과 석사과정
〈관심분야〉 개인정보보호, 클라우드보안, 시스템보안

김 용 혁 (Yong Hyuk Kim) 학생회원
2016년 2월: 한양대학교 컴퓨터공학부 소프트웨어전공 졸업
2016년 3월~현재: 한양대학교 컴퓨터소프트웨어학과 석사과정
〈관심분야〉 악성코드 분석, 개인정보보호, 시스템보안

임 을 규 (Eul Gyu Im) 종신회원
1992년 2월: 서울대학교 컴퓨터공학과 학사
1994년 2월: 서울대학교 컴퓨터공학과 석사
2002년 2월: University of Southern California, 컴퓨터공학과 박사
2005년 3월~현재: 한양대학교 컴퓨터공학부 교수
〈관심분야〉 악성코드 분석, 소프트웨어보안, 펌웨어보안, 클라우드보안