The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 1, pp.11-18, Feb. 29, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.1.11
JIIBC 2020-1-2

LSTM 신경망을 활용한 맥락 기반 모바일 사용자 인증 기법

Context-Aware Mobile User Authentication Approach using LSTM networks

남상진*, 김순태**, 신정훈***

Sangjin Nam*, Suntae Kim**, Jung-Hoon Shin***

요 약 본 연구에서는 모바일 환경에서의 기존 맥락인증기법의 부족한 성능을 보완하고자 한다. 사용된 데이터는 GPS, CDR(Call Detail Record), App usage이며 GPS의 처리과정에서 인구밀집지역의 타인을 세밀하게 구분하고자 GPS밀도에 따른 지역구분을 시행하였다. 또한 전처리에서 데이터 수집에서 발생할 수 있는 결측치를 처리한다. 인증 모델은 두 개의 LSTM(Long-Short Term Memory)와 그들 결과를 종합하는 하나의 ANN(Artificial Neural Network)로 구성하며 이를 통해 최종적으로 인증 점수를 산출한다. 본 논문에서는 기존 연구와의 정확도를 비교하고 타인을 구별해내는데 필요한 인증 시도 횟수를 비교하여 평균 11.6%의 정확도 향상과 검증 데이터의 약 60%에 대하여 더 적은 시도에 구별해 낼 수 있었다.

Abstract This study aims to complement the poor performance of existing context-aware authentication techniques in the mobile environment. The data used are GPS, Call Detail Record(CDR) and app usage. locational classification according to GPS density was implemented in order to distinguish other people in populated areas in the processing of GPS. It also handles missing values that may occur in data collection. The authentication model consists of two long-short term memory(LSTM) and one Artificial Neural Network(ANN) that aggregates the results, which produces authentication scores. In this paper, we compare the accuracy of this technique with that of other studies. Then compare the number of authentication attempts required to detect someone else's authentication. As a result, we achieved an average 11.6% improvement in accuracy and faster detection of approximately 60% of the experimental data.

Key Words : Context-aware Authentication, Context Data, Mobile Application User Authentication,

*준회원, 전북대학교, 소프트웨어공학과
**정회원, 전북대학교, 소프트웨어공학과
***정회원, 전북대학교, 소프트웨어공학과
접수일자: 2019년 12월 10일, 수정완료: 2020년 1월 10일
게재확정일자: 2020년 2월 7일

Received: 10 December, 2019 / Revised: 10 January, 2020 / Accepted: 7 February, 2020
***Corresponding Author: shinjh@jbnu.ac.kr
Dept. of Software Engineering, Jeonbuk National University, Korea

Ⅰ. 서 론

2000년대 이르러 스마트폰의 보급이 활성화된 이래로 스마트폰의 사용량은 크게 증가했다.[1] 2019년 Few research center의 세계 스마트폰 사용자 수 조사 결과에 따르면 한국의 스마트폰 사용자는 74%에서 91%까지 증가했다. 또한 2017년 한국의 스마트폰 사용량을 조사한 내용[2]에 따르면 주중 1일 평균 24.7회, 1회 평균 7.2분 사용한다. 따라서 하루 중 약 3시간은 스마트폰을 이용할 정도로 현대인에게 스마트폰은 필수적인 기기라는 것을 확인할 수 있다. 이러한 스마트폰의 앱은 사용자에게 서비스를 제공하기 위해서 다양한 사용자 인증 기법을 사용하고 있다.

모바일 기기에서 주로 쓰이는 사용자 인증 기법에는 ID/Password[6], OTP(One-Time Password), Digital Certification, 생체인증기법 등이 있다. 이러한 기존 기법들은 각각 문제점을 가지고 있다. 첫 번째로 ID/Password 기법은 사용자가 설정해놓은 Password와 인증 시점에서 기입한 Password와 비교하는 기법이다. 간단하여 널리 쓰이고 있으나 사용자가 Password를 계속해서 기억해야만하고 만약 잊게 된다면 몇 가지 절차를 통해서 재설정해야 한다는 불편함이 있다. 이를 해결하고자 일관된 Password를 사용한다면 기법의 보안성이 떨어진다.[3,8] 두 번째로 OTP는 짧은 시간만 유지되는 Password를 사용하는 방법으로 사용자가 소유한 토큰이나 앱을 통해서 인증 요청 시 임의의 Password를 전송하고 비교하는 방법이다.[9] 이는 토큰을 구매하는 비용이나 Password를 전송하는 과정에서 비용이 발생하며 OTP를 요청하기 위해서 별도의 정보를 기입해야하기 때문에 사용성이 좋지 않다. 세 번째로 Digital Certification기법[8]은 한국에서 높은 보안성을 요구하는 서비스를 위해서 사용되는 경우가 많으며 인터넷 뱅킹을 통해 발급받을 수 있다. 해당 기법은 발급과 갱신에 있어서 많은 과정을 거치기 때문에 불편함을 야기하고 보관에 유의해야하며 비밀번호 또한 기억하고 있어야한다. 이러한 단점으로 인해 2018년 9월 폐지 절차를 밟고 있으나 현재까지 사용되고 있다. 위에 나열한 세 가지 기법의 문제를 해결하고자 스마트폰의 센서를 활용한 생체인증기법이 현재 스마트폰 사용자 인증의 주류로 자리잡았다. 이 기법은 기존 기법과 다르게 사용자가 기억할 정보나 입력프로세스가 없기 때문에 사용성이 크게 증가했지만 지금에 이르러 홍채, 지문, 안면 인식에 있어서 생체정보의 탈취 문제가 대두되고 있다. 더불어 활용되는 센서에 따라 광량, 습도, 안경 등의 외부 환경 요소가 인증에 영향을 미치면서 몇몇 상황에서는 본인 인증에 성공하지 못하는 문제점도 발생하고 있다.[10,11]

이와 같이 기존의 인증 기법에 사용성, 비용과 같은 문제가 존재하기 때문에 최근에 이르러 맥락인증기법(Context-aware Authentication)에 대한 연구가 진행중이다.[4,5,7] 맥락인증기법은 사용자의 과거 행동패턴과 인증시점에서의 행동패턴을 비교하는 방식이다. 이는 사람에 따라서 주중, 주말 또는 시간에 따라 활동이 다르다는 것을 배경으로 한다. 진행되는 연구에 따라서 사용하는 정보와 인증 모델은 다르지만 기존 기법과 비교하여 사용성이 높아졌다는 것은 긍정적이다. 하지만 여전히 본인과 타인을 구분하는 것과 관련하여 보안 성능이 좋지 못하다는 문제가 있다. 이에 따라 다음과 같은 Research Question을 정의한다.

1. 제안한 기법의 정확도가 기존 연구결과보다 높은가.
2. 타인의 인증실패까지 인증 요청 수는 기존 연구결과보다 적은가.

본 연구는 맥락인증기법의 성능 향상을 목적으로 한다. 연구에서 사용하는 데이터는 GPS, CDR 그리고 App Usage이며 인증 성능을 위해서 기존 연구를 통해 인증에 영향력이 큰 데이터인 GPS데이터에 대한 추가적인 전처리를 진행한다.[5] 또한 기존 연구에서 활용하고 있는 단순한 인증 모델이 아닌 맥락 데이터와 같이 시계열 데이터에 효과가 검증된 인공신경망인 LSTM를 활용한다.[13]

기법은 네 가지 절차로 이루어진다. 첫 번째 단계에서 GPS의 전처리를 진행한다. 이 단계는 수집된 GPS를 인구 밀집 지역과 비-밀집지역으로 구분하고 밀집 여부에 따라서 GPS의 구역을 세밀하게 나누는 것이 목표이다. 두 번째 단계는 GPS, CDR, App Usage의 공통적인 전처리를 수행한다. 이 단계에서는 각 데이터의 시간별 빈도를 집계하고 GPS-CDR, GPS-APP Usage와 같이 동시에 발생할 수 있는 것끼리 묶어 훈련데이터를 구성한다. 이 결과를 입력데이터로, 세 번째 단계에서 인증 모델은 본인과 타인을 구분하는 학습을 진행한다. 인증 모델은 두 개의 다른 LSTM과 LSTM들의 결과를 종합하는 ANN(Artificial Neural Network)로 구성된다. 마지막으로 인증 요청시 학습된 모델이 인증 점수를 산출한다. 출력된 인증 점수는 다양한 기준치를 통해 인증 성공 또는 실패로 판정된다.

본 논문은 다음과 같은 순서로 구성된다. 2장에서는

맥락인증기법의 관련 연구와 그 결과에 대해서 요약한다. 다음으로 3장에서 LSTM networks를 활용한 모바일 사용자 인증 기법을 제안한다. 4장에서는 Research Question에 따른 실험을 설정하고 검증한다. 마지막으로 5장에서 논의와 함께 본 논문을 마무리한다.

II. 관련 연구

Elaine Shi 등[5]은 맥락 데이터를 통한 통계적 모델을 제안한다. 해당 연구는 맥락 데이터를 시간에 따른 조건부 확률로 바라보며 스마트폰을 사용하면서 발생하는 이벤트를 Good event와 Bad event로 나누어 각 인증 점수를 계산하고 추가적으로 사용자의 시간에 따른 위치를 인증 점수로 계산하여, 이 셋의 평균을 최종 인증 점수로 산출한다. 결과적으로 타인의 인증임을 파악하는 데 얼마나 많은 시도가 필요한지 검증하여 최소 3회에서 많게는 16번이 필요함을 밝혔다. 다른 연구들과는 다른 추가적으로 인증 모델에 대한 검증에 Informed User와 Uninformed User를 구분하여 실험해야 한다는 의견을 제시한다.

H. Witte 등[12]의 연구는 Location, Call과 더불어 Voice와 같은 Biometric data를 추가적으로 사용하며 이를 입력으로 SVM을 활용하여 사용자를 구분하는 실험을 진행한다. 실험 결과로 15명을 대상으로 20초마다 수집된 데이터를 사용했으며 평균 57.1의 F1-Score를 얻었다. 이는 User Authentication 기법으로 활용하기에는 부족한 성능이며 Biometric data를 수집하기 위해서는 data type에 따른 센서가 항상 활성화되어야 하기 때문에 추가적인 자원 소모도 존재한다는 문제가 있다.

Eiji Hayashi 등[7]은 Naïve Bayes Classifier와 GPS data를 활용한 사용자 인증에 대한 연구를 진행한다. 인증 시점에서 사용자의 위치가 어떤 장소인지에 따라서 맥락인증기법을 사용할지 다른 인증 기법(PIN, ID/Password, Questionnaire)을 사용할지 결정된다는 특징이 있다. 이때 Classifier 생성에 있어서 GPS에 따른 장소가 라벨링(Home, Caffe etc.)이 되어있어야 한다는 한계점이 존재한다. 제안하는 방법의 실험은 18명의 지원자를 통해서 진행되었으며 사용 후 설문조사를 통해 해당 기법이 편리하고 유용하다는 결론을 냈다.

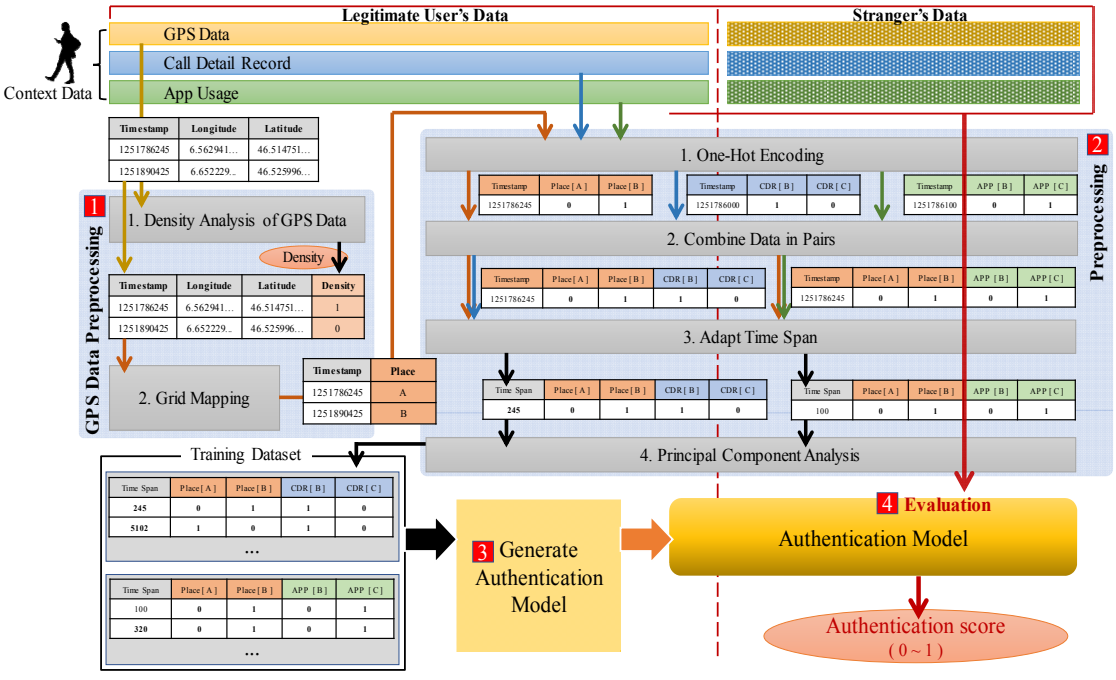

그림 1. LSTM 신경망을 활용한 맥락 기반 모바일 사용자 인증 기법
Fig. 1. Context-Aware Mobile User Authentication Approach using LSTM networks

Ⅲ. LSTM 신경망을 활용한 맥락 기반 모바일 사용자 인증 기법

본 장에서는 LSTM 신경망을 활용한 맥락 기반 모바일 사용자 인증 기법에 대해서 논의한다. 기법은 그림 1과 같이 네 단계로 구성되어 있다. 첫 단계인 GPS Data Preprocessing단계에서는 GPS에 대해서만 밀도 분석 및 GPS를 장소로 표현하며, 두 번째 단계인 Preprocessing단계에서는 GPS, CDR, App usage로부터 인증 모델의 입력 데이터를 생성한다. 세 번째인 Generate Authentication Model단계에서는 두 개의 LSTM networks와 한 개의 ANN으로 구성되며 인증 점수를 산출하는 신경망 모델을 학습시킨다. 마지막 단계인 Evaluation단계는 사용자의 데이터에 다른 사용자의 데이터를 결합한 테스트 데이터에 대해서 모델의 성능을 검증한다. 다음 각 절에서 세부 단계에 대한 내용을 기술한다.

$$\alpha = \begin{cases} 3, & \begin{matrix} MVN.pdf(longitude_i, latitude_i) \\ \geq mean(MVN.pdf(Longitude, Latitude)) \end{matrix} \\ 2, & \begin{matrix} MVN.pdf(longitude_i, latitude_i) \\ < mean(MVN.pdf(Longitude, Latitude)) \end{matrix} \end{cases} \quad (1)$$

1. GPS Data Preprocessing

GPS는 기존 연구[5]를 통해 다른 맥락 데이터와 비교해 인증에 많은 영향을 주는 데이터이다. 또한 시간에 따른 통화 대상 및 사용한 앱의 이벤트 빈도를 계산하는 것과 달리 일반적으로 GPS는 소수점 10번째 자리까지 표현되기 때문에 빈도 집계를 위해 GPS를 장소로 표현할 필요가 있다. 이러한 이유로 우리는 그림2와 같이 GPS에 대해서 별도의 전처리를 실시한다. 다음 각 절에서 Density Analysis of GPS Data단계와 Grid Mapping 방법에 대해서 설명한다.

가. Density Analysis of GPS Data

이 단계는 사용자의 이동 반경이 유동 인구가 많은 장소에 있을 때 해당 장소를 더 세분화함으로써 인증 성능

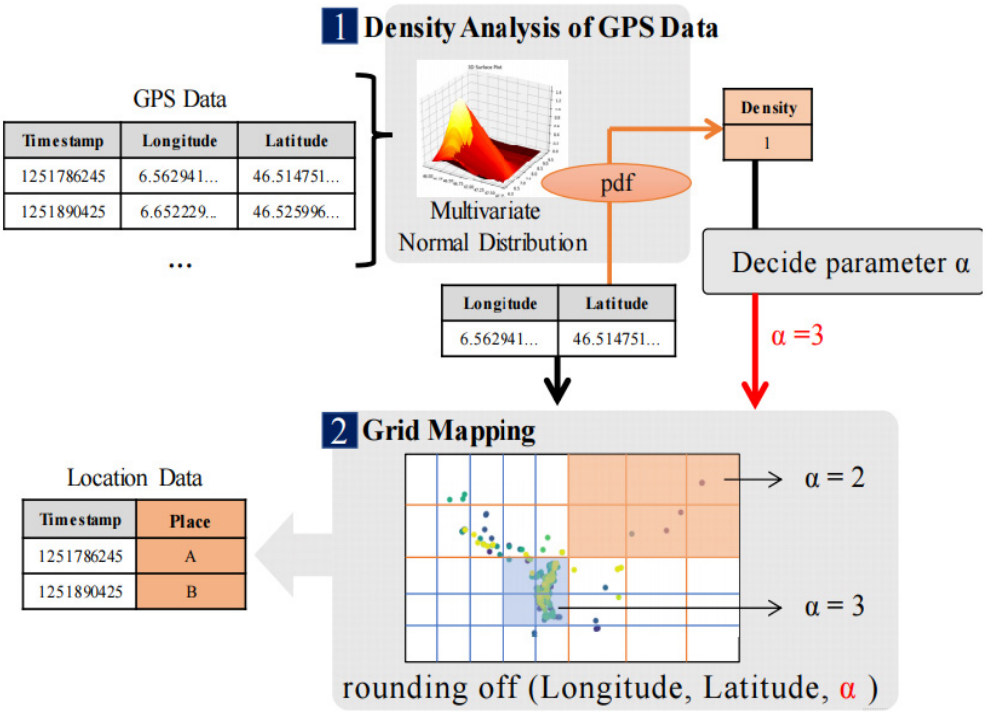

그림 2. GPS 데이터 전처리 과정
Fig. 2. GPS Data Preprocessing

을 높이고자 실시한다. 이를 위해서 MVN(Multivariate Normal Distribution)과 PDF(Probability Density Function)을 사용한다. MVN은 Normal Distribution과 다르게 여러 변수가 존재할 때 사용할 수 있으며 각 변수를 모두 고려하여 데이터의 밀도를 산출한다. 따라서 전체 GPS Dataset를 입력으로 MVN을 생성하고 각 GPS를 입력으로 PDF가 결과를 산출하면 그 위치의 밀도를 구할 수 있다. 이 수치는 식(1)에 따라 파라미터 α를 계산하는데 사용하며 α는 GPS Data를 장소로 표현하는 과정에 사용된다. 이때 $longitude_i$와 $latitude_i$는 i번째 GPS이며 $Longitude$와 $Latitude$는 GPS Dataset의 전체를 의미한다.

나. Grid Mapping

Grid Mapping단계는 1.1절에서 구한 파라미터 α에 따라서 전체 GPS Dataset을 장소로 표현한다. 이 단계는 전체 GPS Dataset에 대해서 $longitude_i$와 $latitude_i$를 소수점 α자리까지 표현되도록 반올림을 한다. 따라서 그림2의 2.Grid Mapping의 도식과 같이 데이터가 밀집된 위치는 장소가 더 좁은 지역을 의미하게 되며 데이터를 더 세밀하게 판단하게 된다. 결과적으로 시간에 따라 사용자가 어느 장소에 있었는지 표현되는 Location Data를 얻을 수 있다.

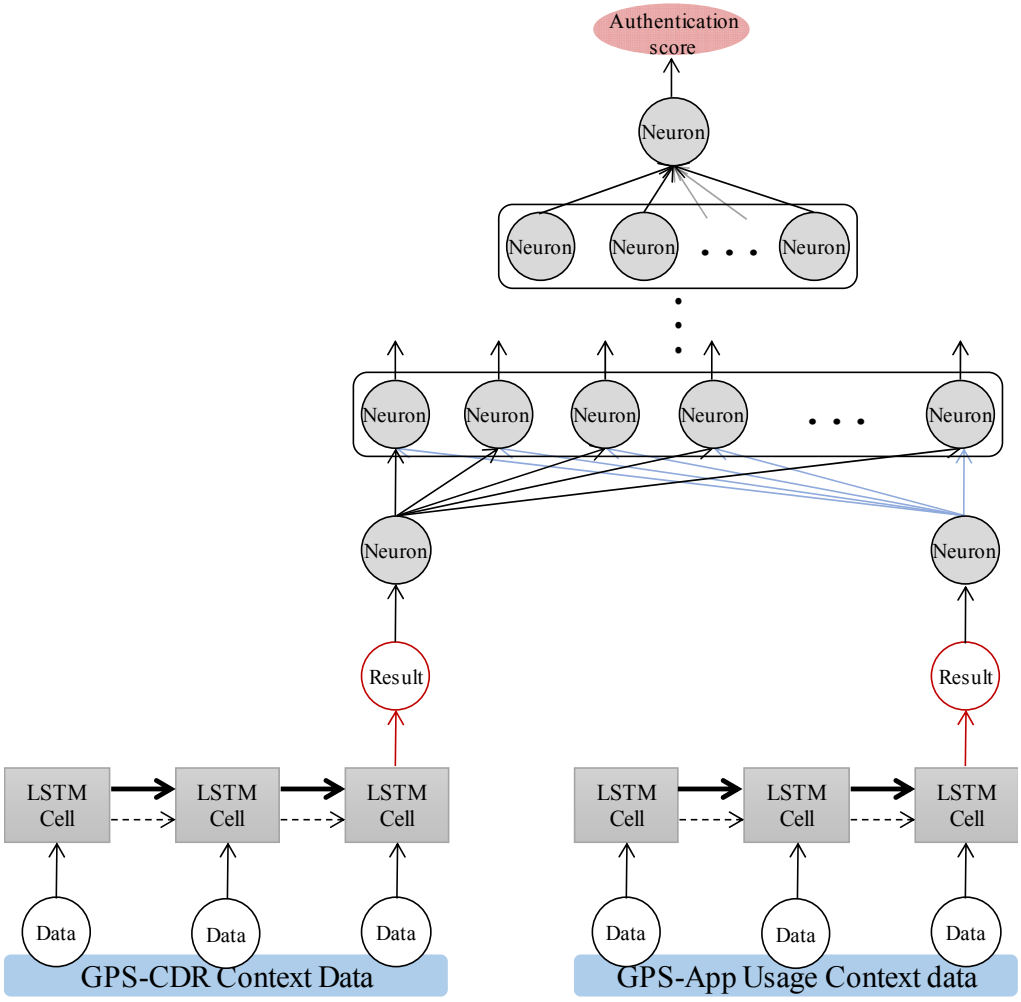

그림 3. 사용자 인증 모델 도식
Fig. 3. User Authentication Model

2. Preprocessing

이번 단계에서는 1절의 결과인 Location Data와 CDR, App usage에 대해서 공통된 전처리를 수행한다. 세부 단계는 총 네 단계로 구성되어 있다. 첫 단계는 One-Hot Encoding단계로 맥락 데이터의 벡터 차원을 전체 장소, 전체 대상, 전체 앱의 개수로 차원으로 확장하고 각 시간에 해당하는 요소에 1의 값을 부여하고 나머지 요소에 0을 부여하는 과정이다. 결과적으로 Location Data, CDR, App usage은 시간에 따른 1과 0으로 표현된다. 두 번째 단계인 Combine Data in Pairs단계에서는 Location Data와 CDR, Location Data와 App usage를 결합한다. 이는 대체로 동시에 수행하지 않는 통화와 앱의 사용을 서로 다른 신경망에서 처리하여 각 신경망이 해당 데이터에 특화시키기 위해 진행한다. 따라서 그림1의 Combine Data in Pairs의 출력처럼 두 데이터셋을 출력한다. 세 번째 단계인 Adapt Time Span은 데이터 수집에 오류가 있어 결측치가 발생하는 경우, 비어있는 데이터를 신경망이 학습하면 성능에 좋지 않기 때문에 수집된 데이터를 순차적으로 입력하는 대신 앞선 데이터와의 시간 간격을 추가하여 시간적 의미를 강조하기 위해서 진행된다. 마지막 단계에서는 주성분분석(Principal Component Analysis)을 수행한다. 세 번째 단계까지 처리된 데이터의 차원은 지금까지 사용자가 방문한 위치의 수와 통화 대상수 혹은 사용한 앱의 수를 더한 값이기 때문에 규모가 크고 Time Span, 위치 그리고 대상 혹은 앱이라는 세 개의 요소 말고는 전부 0값을 취했기 때문에 희소행렬이다. 따라서 인증 모델의 성능 향상을 위해서 주성분분석을 진행하여 Time Span을 제외한 20개의 차원으로 축소한다. 위와 같은 전체 Preprocessing과정을 거치면 인증 모델의 입력 데이터셋이 완성되게 된다.

3. Generate Authentication Model

이번 절에서는 사용자 인증을 수행하는 인증 모델을 생성하는 과정에 대해 논의한다. 본 연구가 대상으로 하는 맥락 데이터는 시간에 따른 사용자의 행동 패턴을 표현하고 있기 때문에 시계열 데이터(Sequence Data)이다. 시계열 데이터의 처리에 있어서 LSTM network가 좋은 성능을 가지고 있다는 것은 많은 연구를 통해서 잘 알려져 있다.[13] 따라서 우리는 LSTM을 활용하여 사용자의 맥락 데이터를 대상으로 하는 신경망을 구성한다. 2절에서 설명한 것과 같이 인증 성능을 위해서 두 개의 LSTM networks로 구성되며 두 개의 출력을 하나의 인증 점수로 산출하기 위해 그림3과 같이 ANN과 연결한다. 인증 모델의 세부 구성은 표1과 같다. 이 신경망을 사용자의 맥락 데이터로 학습하는 것으로 인증 모델을 생성한다.

표 1. 사용자 인증 모델의 파라미터
Table 1. User Authentication Model's parameters

Parameter		Value
LSTM networks	Depth(# of Layers)	4
	Width(# of Neuron)	2, 64, 62, 1
	Normalization	BatchNormalization
	Activation Function	ReLu
ANN	Depth(# of Layers)	1
	Width(# of Neuron)	24
	Normalization	None
	Activation Function	ReLu

Ⅳ. 실험 및 결과

1. Experiment Setting

실험에서 사용한 사용자 맥락 데이터는 Mobile Data Challenge에서 제공받은 데이터이다. 해당 데이터는 약 200명의 데이터를 수집한 것으로 최대 2 년의 사용자별 모바일 사용기록을 가지고 있다. 실험 대상은 전체 사용자 중 데이터양의 수가 많은 순서로 표2와 같이 6명의 데이터를 사용하였으며 GPS Data, CDR, App usage의 데이터 수가 20개보다 작은 사용자는 제외하여 선정했다. 학습 데이터를 생성하기 위해서 각 사용자 데이터에 다른 사용자 4명의 데이터를 각각 결합하여 총 24명의 데이터를 생성하고 사용자 본인의 데이터에는 1값을 다른 사용자의 데이터에 0값을 Label로 부여했다. 이를 통해 각 사용자의 인증 모델을 학습시켰다. 실험은 정의한 Research Question에 대응하여 진행하였다.

2. Experiments Result

관련 연구[8]는 Naive Bayse 공식을 활용하여 사용자를 분류하는 기법을 소개하고 있다. 표2은 본 연구에서 사용한 Mobile Data Challenge의 데이터를 활용하여 Naive Bayse 분류와 본 연구 기법의 사용자 인증 정확도를 비교한 결과이다.

표 2. 실험 결과 1
Table 2. Experiments No.1 Result

USER	ADV USER	OUR APPROACH ACCURACY	NAIVE BAYSE ACCURACY
5993	5927	0.6963	0.18
	5976	0.7605	0.7614
	5966	0.7283	0.7271
	6178	0.7399	0.2548
	mean	0.73125	0.48082
6178	5927	0.7103	0.8261
	5976	0.5997	0.2241
	5966	0.7372	0.7387
	5993	0.7528	0.2470
	mean	0.7	0.50897
6003	5927	0.7907	0.8157
	5976	0.665	0.2128
	5966	0.6506	0.284
	5993	0.661	0.7535
	mean	0.69182	0.5165
5927	5976	0.6538	0.5022
	5966	0.6394	0.465
	5993	0.5843	0.3318
	6178	0.6385	0.6648
	mean	0.629	0.49095
5976	5927	0.7289	0.2643
	5966	0.5716	0.62
	5993	0.5551	0.5171
	6178	0.5518	0.5397
	mean	0.60185	0.48527
5966	5927	0.7553	0.7559
	5976	0.6887	0.5703
	5993	0.555	0.6517
	6178	0.5843	0.3425
	mean	0.64582	0.5801

표 3. 실험 결과 2
Table 3. Experiments No.2 Result

USER	ADV USER	OUR APPROACH Detect Time	NAIVE BAYSE Detect Time
5993	5927	31	552
	5976	46	470
	5966	41	16
	6178	142	503
6178	5927	3	0
	5976	3	2
	5966	21	196
	5993	41	119
6003	5927	27	35
	5976	31	44
	5966	27	35
	5993	29	16
5927	5976	0	12
	5966	0	14
	5993	16	12
	6178	21	12
5976	5927	0	10
	5966	5	10
	5993	0	10
	6178	0	10
5966	5927	183	44
	5976	1	16
	5993	81	35
	6178	471	44
mean		50.83	92.38

실험을 통해서 본 논문에서 제안한 기법이 약 평균 11.6%의 정확도 향상이 있었음을 알 수 있다. 일부 사용자 데이터의 경우 Naive Bayse Classifier가 더 높은 것도 있으나 최악의 경우 18%의 낮은 정확도를 보인다. 결과적으로 해당 실험을 통해서 기존 맥락 인증 기법과 비교해 정확도를 향상시켰으며 안정성도 더 높은 것을 확인할 수 있다.

Research Question 2에 대한 실험은 학습된 인증 모델이 타인의 인증 시도를 인식하는데 몇 번의 시도가 필요한지 계산하는 것으로 결과는 표3와 같다.

표3에 보여지는 것과 같이 본 연구의 기법은 평균 50번의 시도가 필요하며 Naive Bayse Classifier는 평균 92번의 시도가 필요했다. 또한 24번의 실험에서 15번의 결과에서 본 기법의 성능이 더 좋았으며 그 중 5번은 타인의 데이터 첫 번째에서 인증을 실패했다. 따라서 Research Question 2에 대해서 성능이 향상했다고 볼 수 있다.

V. 결 론

본 연구에서는 MVN과 Grid Mapping 그리고 LSTM networks를 활용한 인증 모델을 활용한 모바일 사용자 인증 기법을 제안하였다. 최소 약 1000여개의 데이터가 수집된 사용자 6명을 대상으로 두 개의 실험을 통해 검증을 수행하였으며 평균 정확도 약 66.67%로 11.6%의 성능 향상을 보였으며 타인의 인증 시도에서 비교적 빠르게 인증을 거부해낼 수 있었다.

비록 현재 결과가 바로 적용할 만큼 높지는 않으나 실험에 사용한 데이터의 결측치가 매우 많은 점, 그리고 기존 연구들에 비해 더 적은 수의 Feature를 활용하여 더 높은 성능을 냈다는 점에서 긍정적인 결과라고 판단한다. 향후 연구에서는 Feature의 수를 늘리고 추가한 Feature에 대한 데이터를 분석 및 전처리 기법에 대해 조사할 것이다.

References

[1] Laura Silver, "Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally", Pew Research Center, Feb.2019
https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally

[2] Narae Um, "A Survey on the Actual Condition of Overreliance on Smartphone in 2017". National Information Society Agency, pp. 66-67, 2018.
https://www.nia.or.kr/site/nia_kor/ex/bbs/View.do?cbIdx=65914&bcIdx=19592&parentSeq=19592

[3] Herley C., "So long, and no thanks for the externalities: the rational rejection of security advice by users", In Proc. Of SACMAT, pp. 113-144, 2009.
DOI:
https://www.nspw.org/papers/2009/nspw2009-herley.pdf

[4] Feng Zhang, Aron Kondoro, Sead Muftic, "Location-based Authentication and Authorization Using SmartPhone", TrustCom, pp. 1285-1292, 2012.
DOI:10.1109/TrustCom.2012.198

[5] Elaine Shi, Yuan N., Markus J. and Richard C., "Implicit Authentication through Learning User Behavior", ISC, pp. 99-113, 2010.
DOI:https://doi.org/10.1007/978-3-642-18178-8_9

[6] Jung-gun Lim, Chang-suk Choi, Tae-eun Park, Hyo-sun Ki, Beongku An, "Android Based Mobile Combination Login Application", JIIBC, pp. 151-156, 2013.
DOI:http://dx.doi.org/10.7236/JIIBC.2013.13.3.151

[7] Eiji H., Saivik Das, Shahriyar A., Jason Hong and Ian Oakley, "CASA:Context-Aware Scalable Authentication", SOUP, 2013.
DOI:10.1145/2501604.2501607

[8] Lamport, Leslie. "Password authentication with insecure communication." Communications of the ACM, pp. 770-772, 1981.
DOI:10.1145/358790.358797

[9] Huang, Chun-Ying, Shang-Pin Ma, and Kuan-Ta Chen, "Using one-time passwords to prevent password phishing attacks." Journal of Network and Computer Applications, Vol. 34, pp.1292-1301, 2011.
https://doi.org/10.1016/j.jnca.2011.02.004

[10] Xi, Kai, et al, "A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment." Security and Communication Networks. Vol.4, pp.487-499, 2011.
DOI: https://doi.org/10.1002/sec.225

[11] Neha Kak, Rishi Gupta, "Iris Recognition System", International Journal of Advanced Computer Science and Application, Vol.1, pp.34-40, 2010.
DOI:10.14569/IJACSA.2010.010106

[12] H. Witte, C. Rathgeb and C. Busch, "Context-Aware Mobile Biometric Authentication based on Support Vector Machines", ICEST, pp.29-32, 2013.
DOI:10.1109/EST.2013.38

[13] Sepp Hochreiter, Jurgen Schmidhuber, "LONG SHORT-TERM MEMORY", Neural Computation, Vol.9, pp.1735-1780, 1997.
DOI:10.1162/neco.1997.9.8.1735

저 자 소 개

남 상 진(준회원)

- 2018. 3 ~ : 전북대학교 석사재학
- 2018. 2 : 전북대학교 학사
- Email : sangjin9301@gmail.com

김 순 태(정회원)

- 2014 ~ : 전북대학교 소프트웨어공학과 부교수
- 2010 : 서강대학교 공학박사
- 2007 : 서강대학교 공학석사
- Email : stkim@jbnu.ac.kr

신 정 훈(정회원)

- 1992 ~ : 전북대학교 소프트웨어공학과 교수
- 1999 : 충북대학교 공학박사
- 1991 : 충북대학교 공학석사
- Email : shinjh@jbnu.ac.kr