이상 탐지 모델을 활용한 사용자 행위 기반의 VR기기 사용자 인증 모델 연구

전우진[1], 김형식[2]
[1]성균관대학교 전자전기컴퓨터공학과 박사과정
[2]성균관대학교 전자전기컴퓨터공학과 교수
dnwls0116@naver.com, hyoung@skku.edu

A Study on VR Device User Authentication Model based on User Behavior using Anomaly Detection Model

Woo-Jin Jeon[1], Hyoung-Shick Kim[2]
[1,2]Dept. of Electrical and Computer Engineering, Sungkyunkwan University

요 약

VR 기술의 발전은 다양한 분야에서 사용자에게 몰입감 있는 가상 현실 경험을 제공하지만, VR기기 내부에 사용자의 생체 데이터 및 금융정보와 같은 민감한 정보들이 저장되어 새로운 보안 문제를 야기하고 있다. 이에 따라 PIN, 패스워드 등과 같은 기존의 인증 방식이 VR 기기에 적용되고 있지만 이들은 shoulder-surfing attack 공격 취약하며 VR 환경에서 사용하기에 불편한 인터페이스를 가지고 있다. 따라서 본 논문에서는 이상 탐지 모델을 활용하여 외부 추론 공격에 강인하며 VR 환경에 적합한 사용자 행위 기반의 VR기기 사용자 인증 모델을 구현한다. 특정 task를 수행하는 동안 사용자의 행위 데이터를 수집 및 feature 데이터를 추출하고, 정상으로 라벨링 된 사용자의 데이터로 이상 탐지 머신러닝 모델들을 학습 후 정상 데이터와 비정상 데이터를 이용하여 인증 모델의 성능을 평가하였다. OC-SVM이 87.72%의 F1-score로 세 모델 중 가장 높은 성능을 보임을 확인하였으며, 향후 인증 모델 성능 향상을 위한 계획을 제시하였다.

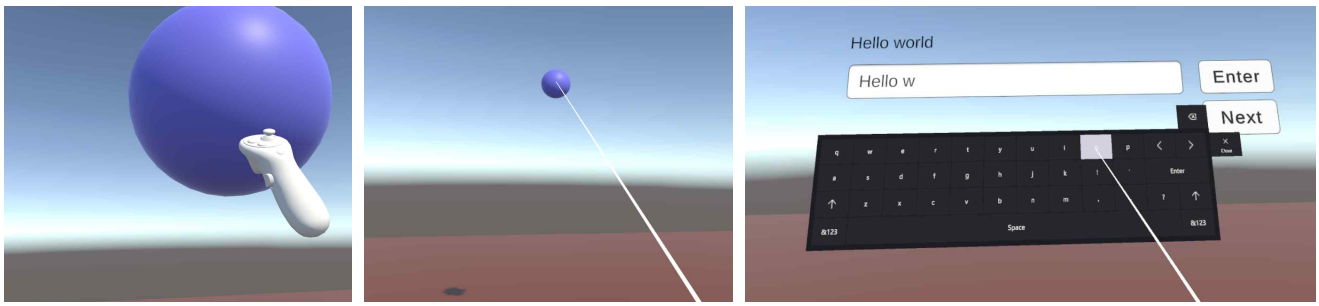
1. 서론

최근 몇 년 동안 가상 현실(Virtual Reality, VR) 기술은 급속한 발전과 함께 상용화되어 왔다. 컴퓨터 및 통신 기술의 발전에 힘입어 현재에도 교육, 의료, 비즈니스, 국방, 엔터테인먼트 및 소셜 네트워크 등 여러 분야에서 현실과 거의 구분할 수 없는 몰입적인 경험을 사용자들에게 제공하기 위해 지속적인 VR 기술 발전 가능성이 기대되고 있다.

VR의 발전은 동시에 VR 사용자의 개인정보 위협을 야기하고 있다. 사용자의 몰입감 있는 가상 현실 체험을 위하여 VR기기는 사용자의 행위 정보, 아이 트래킹, 음성 등 다양한 생체 정보 데이터를 저장하고 있으며, VR 내 결제를 위한 금융정보들도 함께 저장되어 있다. 이러한 사용자의 개인정보를 VR기기에 무단 접근하는 외부 공격자들로부터 보호하기 위한 기술의 필요성이 대두되고 있다 [1].

VR기기 사용자 인증은 위와 같은 보안 문제를 해결할 수 있는 기술로 기기 착용자가 등록된 사용자인지 확인하여 외부인이 VR기기에 저장된 개인정보에 무단으로 접근하는 것을 방지한다. 현재 여러 상용 VR기기에서 PIN, 패스워드, 패턴 입력과 같은 인증 기법들이 사용되고 있지만, 이들은 shoulder-surfing attack 공격에 취약[2]하며 VR 환경에서 사용되기에 불편한 인터페이스를 가지고 있다.

본 논문에서는 [3]에서 활용한 task들을 이용하여 VR기기 사용자 인증 모델을 구현한다. 등록된 사용자와 미등록된 사용자를 분류하기 위하여 이상치(outlier)를 탐지하는 모델들인 OC-SVM (One Class Support Vector Machine), OC-kNN (One Class k-Nearest Neighbors), 그리고 Isolation Forest를 사용한다. VR 환경에서 사용자가 각 task를 진행하는 동안 사용자의 행위 데이터를 수집하고, 수집된 데이터로부터 feature를 추출하여 각 모델을 학습하였다. 학습된 모델들의 성능을 측정하기 위하여 precision, recall, 그리고 F1-score 값을 계산하였다. 그 결과, OC-SVM이 87.72%의 F1-score로 세 모델 중 가장 높은 성능을 보여주었다.



(그림 1) 좌측부터 Grabbing, Pointing, Typing task

2. 사용자 행위 데이터 추출 앱 설계

본 연구에서는 Unity 3D를 이용하여 [3]에서 제안된 3개의 task를 직접 구현하였으며, VR기기는 Meta Quest Pro를 활용하였다. 각각의 task는 가상 환경에서 일정 거리에 있는 공을 컨트롤러로 직접 붙잡는 grabbing, 컨트롤러의 ray를 이용하여 일정 거리에 있는 공을 붙잡는 pointing, 컨트롤러의 ray를 이용하여 가상 키보드로 문장을 입력하는 typing으로 구성되어 있다 (그림 1).

Grabbing에서는 사용자로부터 0.5m 거리에서 1.5m 높이를 중심으로 하는 지름이 0.7m인 원의 둘레 위에 공이 일정 순서대로 나타난다. 사용자가 공에 컨트롤러를 가져다 댄 후 클릭하면 다음 공이 나타나며, 총 13개의 공이 한 세션 동안 나타난다. 공의 지름이 0.15m일 때 10세션 그리고 0.3m일 때 10세션씩, 사용자별로 총 20세션을 수행하였다.

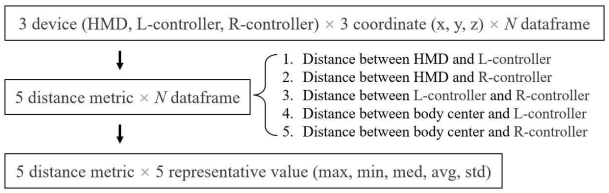
Pointing에서는 사용자로부터 일정 거리에서 1.5m 높이를 중심으로 하는 지름이 2m인 원의 둘레 위에 공이 일정 순서대로 나타난다. 사용자가 ray를 공에 일치시키고 클릭하면 다음 공이 나타나며, 총 13개의 공이 한 세션 동안 나타난다. 사용자로부터의 거리가 2m일 때 10세션 그리고 4m일 때 10세션씩, 사용자별로 총 20세션을 수행하였다.

Typing에서는 사용자로부터 3.75m 거리에 가상 키보드가 존재하며, 사용자는 ray의 클릭을 통해 주어진 문장을 입력한다. 한 세션 동안 하나의 문장을 입력하며, 총 15개의 다른 문장이 주어진다. 사용자별로 문장마다 한 세션씩, 총 15세션을 수행하였다.

총 10명의 피험자가 참여하였으며, task가 진행되는 동안 사용자가 착용하고 있는 HMD(Head Mounted Display)와 좌우 컨트롤러의 위치 좌표(x, y, z)를 90Hz 샘플링 레이트로 수집하였다.

3 Feature 추출 및 모델 학습

그림 2는 수집된 데이터로부터 feature 값을 추출하는 과정을 보여주는 그림이다. 먼저 각 데이터



(그림 2) Feature 추출 과정

프레임별로 장치 간 좌표값을 이용하여 HMD와 왼쪽 컨트롤러 사이의 거리, HMD와 오른쪽 컨트롤러 사이의 거리, 왼쪽 컨트롤러와 오른쪽 컨트롤러 사이의 거리, 왼쪽 컨트롤러와 몸 중심과의 거리, 그리고 오른쪽 컨트롤러와 몸 중심과의 거리를 계산한다. 각 컨트롤러와 몸 중심과의 거리는 HMD와 각 컨트롤러의 y 좌표를 제외한 x, z 좌표를 이용한 거리 계산으로 구하였다. 그 후 한 세션 동안의 각 거릿값의 최대, 최소, 중간, 평균, 표준편차를 계산하여 총 25개의 feature를 추출하였다.

Pointing에서 참가자마다 20개의 데이터를 가지며, 모델 학습 및 테스트를 위하여 참가자들은 차례대로 한 명은 정상, 그 외에는 비정상으로 라벨링 되었다. 정상 데이터에서 랜덤하게 선별한 10개의 데이터로 학습 데이터셋을 구성 및 모델을 학습하였으며, 나머지 10개의 정상 데이터와 비정상 데이터에서 랜덤하게 뽑은 10개의 비정상 데이터를 합한 20개의 데이터로 테스트 데이터셋을 구성 및 모델을 테스트하였다. 이때 비정상 데이터 선별 시 비정상으로 라벨링 된 9명의 참가자로부터 최소 1개씩은 데이터가 선별되도록 하였다. 위와 같은 과정을 정상으로 라벨링 된 참가자마다 총 100번을 수행하였고 전체 평균값으로 결과를 구하였다. Grabbing에서도 똑같은 과정으로 모델을 학습 및 테스트하였다.

Typing에서는 참가자마다 15개의 데이터를 가지며, 참가자들은 차례대로 한 명은 정상, 그 외에는 비정상으로 라벨링 되었다. 정상 데이터에서 랜덤하게 선별한 5개 데이터로 학습 데이터셋을 구성 및 모델을 학습하였으며, 나머지 10개의 정상 데이터와 비정상 데이터에서 랜덤하게 뽑은 10개의 비정상 데

<표 1> 이상 탐지 모델 및 Task별 성능 평가

Model	Task	Precision (%)	Recall (%)	F1-score (%)
OC-SVM	Grabbing	83.12	93.92	87.85
	Pointing	87.09	93.16	89.55
	Typing	78.79	95.30	85.76
OC-kNN	Grabbing	93.52	70.02	77.02
	Pointing	98.67	58.52	72.76
	Typing	92.63	73.93	80.22
Isolation Forest	Grabbing	77.01	90.33	82.69
	Pointing	79.46	93.17	85.36
	Typing	79.34	94.89	85.87

이터를 합한 20개의 데이터로 테스트 데이터셋을 구성 및 모델을 테스트하였다. 위와 같은 과정을 정상으로 라벨링 된 참가자마다 총 100번을 수행하고 전체 평균값으로 결과를 구하였다.

Scikit-learn 라이브러리를 활용하여 OC-SVM, OC-kNN, 그리고 Isolation Forest를 학습하였다. 각 모델 학습 시 OC-SVM의 매개변수로 커널은 rbf, gamma는 scale, nu는 0.2를, OC-kNN의 매개변수로 k는 8, distance metric은 Euclidean Distance, threshold는 0.5를, Isolation Forest의 매개변수로 n_estimators_num는 10을 설정하였다.

4 결과

본 논문에서는 precision, recall, 그리고 F1-score를 평가 지표로 사용하여 VR기기 사용자 인증 모델의 성능 평가를 진행하였다. 실험 결과는 표 1에 나와 있으며 모델 및 각 task별로 성능 평가를 진행하였다. 평균적으로 OC-SVM은 87.72%, OC-kNN은 76.67%, 그리고 Isolation Forest는 84.64%의 F1-score 성능을 보이며 OC-SVM이 세 모델 중 제일 좋은 성능을 보여주었다.

OC-SVM과 Isolation Forest는 precision이 다소 낮지만 recall에서 높은 점수를 보여주었으며, 이를 통해 두 모델은 정상 사용자의 데이터는 정상 사용자라고 잘 판단하였지만 비정상 사용자의 데이터를 정상 사용자라고 잘못 판단하는 경향이 있음을 볼 수 있다. 이는 등록되지 않은 사용자가 VR기기에 접근하는 문제가 발생할 수 있다. 반대로 OC-kNN은 precision이 높고 recall이 낮은 성능을 보여주었으며, 이를 통해 정상 사용자의 데이터를 비정상 사용자라고 잘못 판단하는 경향이 있음을 볼 수 있다. 이는 정상 사용자의 VR기기 접속을 방해하여 사용자의 usability에 문제를 야기할 수 있다.

5. 결론 및 향후 계획

본 논문에서는 이상 탐지 모델인 OC-SVM, OC-kNN, Isolation Forest를 이용하여 행위 기반의 VR기기 사용자 인증 모델을 구현하였다. 본 논문에서 구현된 인증 모델은 OC-SVM이 87.72%의 F1-score를 달성하지만, precision이 다소 낮으며 실제 VR 기기에 적용되기에는 부족한 성능이다. 향후 해당 방식에서 발전시켜 사용자 행위 데이터 수집 시에 기기별 회전 좌표, 속도, 각속도 등을 추가로 수집하고, 새로운 feature들을 추가로 도입 및 선별하여 인증 모델의 성능을 향상시킬 계획이다.

Acknowledgments

이 논문은 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원 (RS-2023-00229400, 안전한 메타버스 환경을 위한 사용자 인증 및 프라이버시 보호 기술 개발, 50%)과 2024년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (No. 2022-0-01199, 융합보안핵심인재양성, 50%)

참고문헌

[1] Stephenson, S., et al. “Sok: Authentication in Augmented and Virtual Reality”, In 2022 IEEE Symposium on Security and Privacy (SP), 2022, pp. 267-284.

[2] George, C., et al. “Seamless and Secure Vr: Adapting and Evaluating Established Authentication Systems for Virtual Reality”, NDSS, 2017.

[3] Pfeuffer, Ken, et al. “Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality”, Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019, pp. 1-12.