머신러닝 기반 오픈뱅킹 사용자 시퀀스 이상 탐지 모델 설계 및 검증

김건민[1], 김예진[1], 곽지호[2], 김경백[3]
전남대학교 소프트웨어공학과[1]
전남대학교 인공지능학부[2]
전남대학교 인공지능융합학과[3]
E-mail: 204869@jnu.ac.kr, ye031010@jnu.ac.kr, 214490@jnu.ac.kr, kyungbaekkim@jnu.ac.kr

Design and Evaluation of an ML-Based Anamoly Detection Framework for User Behavior Sequences in Open Banking

Geonmin Kim, Yejin Kim, Jiho Kwak, Kyungbaek Kim
Dept. of Software Engineering
Dept. of Artificial Intelligence
Dept. of Artificial Intelligence Convergence

Abstract

This study proposes a behavior sequence-based anomaly detection framework designed for Open Banking environments. Unlike conventional event-level detection methods, the proposed approach models user activities – such as login, inquiry, and transfer – as temporal sequences. By applying a sliding window and extracting statistical features, we train and evaluate multiple classifiers, including Logistic Regression, Random Forest, and XGBoost, using F1-score based threshold optimization. Experimental results demonstrate the framework's effectiveness in detecting sophisticated threats that may bypass traditional security systems.

I. 서론

핀테크(Financial Technology)[1] 산업은 금융과 정보기술의 융합을 통해 기존 금융 서비스의 경계를 허물고, 보다 편리하고 빠른 서비스를 제공하는 방향으로 발전해왔다. 모바일 뱅킹, 디지털 결제, 로보어드바이저를 통한 투자 자문, P2P 대출 서비스 등은 모두 핀테크의 대표적 산물이다. 이 과정에서 오픈뱅킹(Open Banking) 제도의 도입은 핀테크 산업 발전의 중요한 전환점이 되었다. 오픈뱅킹은 금융기관 데이터에 접근할 수 있도록 표준화된 API를 도입하고[2], 이를 통해 제 3자 서비스 제공자(Third Party Providers, TPPs)가 사용자의 은행 계좌 정보에 접근하거나 결제 요청을 수행할 수 있도록 허용함으로써, 금융 서비스 간 경계를 허물고 생태계 확장성을 크게 높였다.

그러나 오픈뱅킹의 편리성과 개방성 이면에는 다양한 보안 위협이 존재한다[3][4]. 금융기관 내부에 국한되었던 데이터 접근 권한이 외부로 확장되면서, 사용자 정보가 의도치 않게 노출되거나, 악의적인 행위자가 정상 사용자의 신원을 가장하여 금융 시스템에 접근할 가능성 또한 높아졌다. 특히 표면적으로는 정상적인 인증(Authentication) 과정을 통과한 사용자일지라도, 실제 행동 패턴을 분석하면 비정상적인 특성을 보이는 경우가 있다. 이는 전통적인 인증 및 권한 부여 체계만으로는 탐지하기 어려운 문제다.

오픈뱅킹 환경에서의 보안 위협은 외부 공격자뿐만 아니라, 정상 사용자가 인증정보를 탈취당하는 경우에도 발생할 수 있다. 더욱이 오픈뱅킹 API 특성상 다양한 서비스가 연계되면서 트래픽 형태가 복잡하고 이질적으로 되어, 단순 요청-응답 단위의 이상탐지 방법만으로는 정교한 위협을 효과적으로 식별하기 어렵다.

최근에는 이상 접근을 탐지하고, 보안성을 강화하기 위해 머신러닝 기술을 활용한 다양한 연구가 진행되고 있다[5]. 이에 본 연구는 기존 FDS(Fraud Detection System)의 특징적 패턴 기반 탐지 방식[6]에 착안하여, 사용자 행동 시퀀스의 시간적 연속성과 의미적 흐름을 반영한 새로운 이상행동 탐지 체계를 제안한다. 사용자 행동 중심의 보안 탐지 접근법을 설계하고, Logistic Regression, Random Forest, XGBoost 모델을 적용하여 성능을 비교·분석함으로써 오픈뱅킹 환경에 가장 적합한 모델을 탐색한다.

이를 통해 단일 이벤트 기반 탐지 방식의 한계를 극복하고, 오픈뱅킹의 다양한 거래 시나리오 속에서도 이상행동을 효과적으로 식별하는 것을 목표로 한다. 구체적으로 사용자 행동 시퀀스를 체계적으로 수집·모델링하고, 정상 흐름에서 벗어나는 이상 패턴을 실시간으로 탐지할 수 있는 체계를 구축한다. 단편적인 API 요청 분석을 넘어, 전체적인 행동 흐름을 분석함으로써 오픈뱅킹 보안성을 근본적으로 강화하고, 금융 서비스에 대한 사용자 신뢰를 제고하고자 한다.

II. 사용자 행동 분석의 필요성

오픈뱅킹은 본질적으로 데이터의 개방성과 상호운용성을 기반으로 한다. 과거 금융기관 내부망에 국한되었던 고객 정보가 외부 제3자에게 제공되면서, 사용자 편의성은 향상되고, 서비스 혁신이 이뤄졌다[7]. 사용자는 더 이상 하나의 은행 플랫폼에 종속되지 않고, 다양한 핀테크 서비스를 통해 송금, 투자, 대출 등 여러 금융 활동을 수행할 수 있다. 이러한 변화는 핀테크 생태계의 폭발적 성장을 이끈 핵심 요인 중 하나로 평가된다.

그러나 금융 데이터의 개방은 동시에 새로운 보안 위협을 수반하게 되었다[8][9][10]. 오픈 API를 통해 금융 데이터에 접근할 수 있다는 점은 악의적인 행위자에게도 침투 기회를 제공한다. 이들은 취약한 제3자 제공자를 노려 인증 정보를 탈취하거나, 정상 사용자로 위장해 민감한 금융 정보에 접근할 수 있다. 특히 사용자 인증 체계가 강화되었다 하더라도, 인증 이후의 행동을 감시하지 않는다면, 해당 사용자가 실제로 정상적인 행위를 하고 있는지 판단하기 어렵다.

기존의 보안 체계는 대부분 인증과 권한 부여에 초점을 맞추고 있다. 사용자가 적절한 자격 증명을 제출하면, 시스템은 이를 신뢰하고 요청을 처리한다. 그러나 최근의 보안 사고들은 이 구조가 충분하지 않다는 점을 여실히 보여준다. 인증정보가 탈취되었거나, 내부자 위협이 발생한 경우, 전통적인 보안 장치는 쉽게 무력화된다. 더 이상 단순히 "누가 요청했는가"를 확인하는 것을 넘어, "요청자가 어떤 행동을 하고 있는가"를 정밀하게 분석할 필요가 있다.

이러한 맥락에서 사용자 행동 분석(User Behavior Analytics, UBA)의 필요성이 부각된다. 사용자는 금융 서비스를 이용할 때 일정한 행동 패턴을 보인다. 예를 들어, 일반적인 사용자는 오전 중에 로그인하여 계좌를 조회하고, 소액 송금을 수행하거나 투자 현황을 확인하는 등의 행동을 반복한다. 반면 계정을 탈취한 공격자는 특정 시간대에 다량의 송금 요청을 시도하거나, 정상적인 흐름과는 무관하게 고액 송금만 반복적으로 수행하는 등 비정상적인 패턴을 보이기 쉽다. 사용자 행동 분석은 이러한 정상적 패턴과 비정상적 패턴을 식별하는 것을 목표로 한다. 이는 단순히 요청 건수를 세는 것이 아니라, 행동의 순서, 시간 간격, 맥락을 종합적으로 고려한다. 예를 들어, 계좌 조회 후 일정 시간 내에 소액 송금이 이뤄지는 것은 정상적인 흐름일 수 있지만, 별다른 조회 없이 바로 고액 송금을 시도하는 경우는 위험 신호로 간주될 수 있다.

III. 사용자 행동 기반 이상 탐지 체계

본 연구는 오픈뱅킹 환경에서의 보안 위협을 정밀하게 탐지하기 위해, 단일 이벤트 기반이 아닌 사용자 행동의 시계열적 흐름에 주목하였다. 오픈뱅킹은 고도로 연결된 API 기반 생태계를 구성하며, 사용자의 금융 활동이 단일 행위 단위가 아닌 연속된 행위 흐름으로 이뤄진다는 점에서 기존의 단편적 탐지 방식만으로는 정교한 공격 시나리오를 식별하는 데 한계가 존재한다. 이에 본 연구는 사용자 행동 시퀀스의 시간적·의미적 패턴 전체를 분석 단위로 삼아, 이상행동을 탐지할 수 있는 체계적인 방법론을 제안하고, 이를 실험적으로 구현하여 성능을 검증하였다.

3.1 시뮬레이션 기반 오픈뱅킹 사용자 로그 생성

본 실험은 오픈뱅킹의 주요 행동 시나리오를 재현한 시뮬레이터를 기반으로 구성되었다. 특히, 인증 이후 사용자 행동 흐름(로그인, 조회, 송금 등)에 초점을 맞춰 실제 시스템에서 유사하게 발생할 수 있는 보안 위협 패턴을 모델링하였다. 총 400명의 가상 사용자를 생성하고, 이 중 250명은 정상적인 사용 흐름을 따르는 일반 사용자로, 150명은 계정이 탈취되어 비정상적인 행동을 수행하는 공격자로 설정하였다. 각 사용자는 로그인, 계좌 조회, 소액 송금, 고액 송금 등의 행동이 부여되며, 이들은 시간 순서에 따라 연결된 시퀀스로 구성된다.

정상 사용자는 대체로 오전 시간대에 로그인하여 계좌를 조회하고, 이후 특정 간격을 두고 송금이나 투자 관련 행위를 수행하는 등 일관되고 반복적인 패턴을 보인다. 반면 공격자는 비정상적으로 짧은 시간 내에 고액 송금을 연속적으로 시도하거나, 평소 활동하지 않던 시간대에 다량의 요청을 수행하는 등 이상행동을 나타내도록 설계되었다. 또한 현실적인 상황을 반영하기 위해 20%의 라벨 노이즈를 삽입하여 일부 정상 행동이 공격으로, 일부 공격 행동이 정상으로 표시되도록 하였으며 전체 로그는 시계열 정렬 후 학습용(80%)과 테스트용(20%)으로 분할되었다.

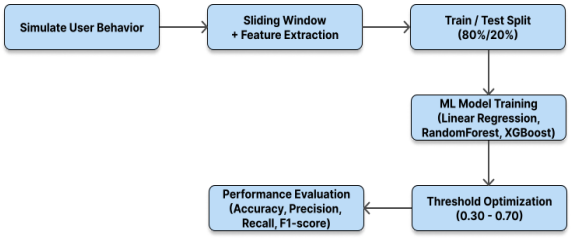

그림 1. 사용자 이상행동 탐지 모델 실험 방법

3.2 사용자 행동 시퀀스의 구조화 및 특징 추출

생성된 로그는 단순 이벤트 단위가 아닌, 일정 길이의 행동 시퀀스로 재구성되었다. 본 연구에서는 시퀀스 길이 5를 기준으로 슬라이딩 윈도우 기법을 적용하여, 사용자 행동의 흐름을 시간 순서에 따라 연속된 구간으로 분할하였다. 각 시퀀스는 사용자의 5개 연속 행동으로 구성되며, 이에 대해 다음과 같은 정량적 특징(feature)을 추출하였다: (1) 송금 금액의 최대값, (2) 송금 금액의 평균값, (3) 두 행동 간 시간 간격의 최대값, (4) 시간 간격의 평균값. 이들은 단일 이벤트의 정태적 정보가 아닌, 시간 흐름과 행동 간 상호작용을 반영하는 요약 통계로서 이상행동 판단에 핵심적 지표로 작용한다.

3.3 이상행동 탐지 모델 구성 및 임계값 최적화

이상행동 분류에는 Logistic Regression, Random Forest, XGBoost 세 가지 대표적인 분류 모델을 적용하였다. 모든 모델은 클래스 불균형을 보정하기 위해 balanced class weight를 설정하고, 동일한 훈련 데이터(80%)로 학습되었다. 검증 데이터(20%)를 이용하여 F1-score를 기준으로 최적의 임계값을 탐색하였으며, 임계값을 0.30부터 0.70까지 0.01 간격으로 조정하며 F1-score를 계산하였다. 이 중 가장 높은 점수를 기록한 값을 최종 임계값으로 선정하였다.

IV. 실험 및 결과

평가 지표는 Accuracy, Precision, Recall, F1-score를 중심으로 설정하였다. 이중 F1-score는 Precision과 Recall의 조화 평균으로, 보안 시스템에서 가장 중요한 탐지 정확도와 탐지 누락 방지를 동시에 고려할 수 있는 핵심 지표이다. 또한 Accuracy는 전체 예측 중 맞은 비율, Precision은 탐지된 이상 중 실제 이상일 확률, Recall은 전체 이상 중 탐지된 비율을 의미한다.

	Accuracy	Precision	Recall	F1
Logistic Regression	**0.9604**	**0.9737**	**0.9860**	**0.9798**
Random Forest	0.8767	0.8870	0.9847	0.9333
XGBoost	0.8794	0.9197	0.9450	0.9322

표 1. 각 모델 별 성능 측정 결과

	Average	Standard Devation
Accuracy	0.9608	±0.0078
Precision	0.9762	±0.0069
Recall	0.9823	±0.0076
F1-Score	0.9789	±0.0065

표 2. LogisticRegression 모델의 15회 반복 실험 결과

실험 결과는 세 모델 모두 이상행동 탐지에 높은 성능을 보였으나, Logistic Regression 모델이 평균적으로 가장 우수한 F1-score (0.9798)를 기록하였다. 특히 Precision과 Recall 간 균형이 뛰어났으며, 이는 실시간 응답성과 정밀 탐지를 동시에 요구하는 보안 시스템에 적합함을 보여준다. 또한 15회에 걸친 반복 실험에서도 성능 편차가 작게 나타나, 모델의 일관성과 신뢰도를 입증하였다.

반면, Random Forest와 XGBoost는 상대적으로 높은 Recall을 유지했음에도 불구하고, 일부 실험에서 Precision이 낮아지는 경향을 보였다. 이는 특정 이상행동 유형에 보다 민감하게 반응함을 시사하며, 모델의 탐지 특성이 사용 환경에 따라 달라질 수 있음을 보여준다. 따라서 이러한 특성은 향후 환경에 최적화된 모델을 선택시 중요한 판단기준이 될 수 있다.

V. 결론 및 향후 연구 방향

본 연구는 오픈뱅킹 환경에서 사용자 행동의 시계열적 흐름을 기반으로 이상행동을 탐지하는 새로운 방법론을 제안하고, 이를 시뮬레이션 로그 기반 실험을 통해 실증적으로 검증하였다. 기존 단일 이벤트 기반 탐지 방식의 한계를 극복하기 위해, 사용자 행동 시퀀스

를 중심으로 금액, 시간 간격 등 의미 있는 피처를 정량화하고, 임계값 튜닝 기법을 활용하여 고정밀 이상 탐지 체계를 구축하였다.

실험 결과, Logistic Regression은 높은 F1-score와 해석 용이성 측면에서 우수한 성능을 보였으며, Random Forest와 XGBoost는 복잡한 행동 패턴 탐지에 더 효과적인 특성을 나타냈다. 이러한 모델 간 비교는 실제 사용 환경에 따라 적절한 탐지 체계를 선택하는 데 실증적 기준을 제공하며, 특히 Logistic Regression은 정량적 성능뿐 아니라 반복 실험 간의 일관성을 통해 실용성과 신뢰성을 함께 입증하였다.

향후 연구는 다음과 같은 방향으로 확장될 수 있다. 첫째, 실제 오픈뱅킹 API 호출 로그를 수집하거나, 산업 파트너로부터 비식별화된 실 데이터를 제공받아 본 시스템의 현실 적용 가능성을 평가할 수 있다. 둘째, 기존의 머신러닝 모델을 넘어 Transformer, LSTM 등 다양한 시계열 특화 모델을 적용하여 탐지 성능을 고도화할 수 있다. Transformer는 행동 간의 문맥적 관계 및 장기적 상호작용을 모델링하는 데 강점을 가지며, LSTM은 시계열 간 장기적 의존성을 학습하는 데 적합하다. 셋째, 실시간 탐지 시스템과의 연동을 통해 이상행동 탐지 후 즉각적인 대응(계정 차단, 알림 전송 등)이 가능한 실시간 보안 체계로의 발전도 기대된다.

본 연구는 단순히 높은 수치적 성능을 보이는 이상 탐지 모델을 제안하는 것을 넘어, 오픈뱅킹이라는 고도로 연결된 금융 환경의 특성을 반영한 새로운 탐지 프레임워크를 제시하였다. 향후 본 체계는 금융을 넘어 헬스케어, 공공 API, 에너지 등 시계열 사용자 로그가 생성되는 다양한 분야 확장될 수 있으며, 디지털 인프라 전반의 보안성과 신뢰성 향상에 기여할 수 있을 것이다.

Acknowledgement

본 과제(결과물)는 교육부와 한국연구재단의 재원으로 지원을 받아 수행된 첨단분야 혁신융합대학사업의 연구결과입니다(34%). 이 논문은 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원-지역지능화혁신인재양성사업의 지원을 받아 수행된 연구임(IITP-2025-RS-2022-00156287, 33%). 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 인공지능융합혁신인재양성사업 연구 결과로 수행되었음(IITP-2023-RS-2023-00256629, 33%)

참고문헌

[1] N. Kapoor, T. Kapoor, D. R. Sisodiya and J. Sushma, "Impact of Fintech: Revolution in Banking and Financial Industry," 2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, 2024, pp. 1-6

[2] D. Fett, P. Hosseyni and R. Küsters, "An Extensive Formal Security Analysis of the OpenID Financial-Grade API," *2019 IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, USA, 2019, pp. 453-471

[3] A. O. Ogunleye et al., "Analysing the Cybersecurity Concerns Associated with Fintech Innovations. A Systematic Review," 2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON), Ado Ekiti, Nigeria, 2024, pp. 1-5

[4] S. Mehrban et al., "Towards Secure FinTech: A Survey, Taxonomy, and Open Research Challenges," in IEEE Access, vol. 8, pp. 23391-23406, 2020

[5] D. Behbehani, N. Komninos, K. Al-Begain and M. Rajarajan, "Open Banking API Security: Anomalous Access Behaviour," 2023 International Conference on Innovations in Intelligent Systems and Applications (INISTA), Hammamet, Tunisia, 2023, pp. 1-4

[6] 유시완(Si-wan Yoo). "전자금융 불법이체사고 방지를 위한 실시간 이상거래탐지 및 분석 대응 모델 연구." 정보보호학회논문지 26.6 (2016): 1513-1526.

[7] 오상승,정경찬,and 조근태. "한국형 오픈뱅킹 API 플랫폼의 활성화 요인에 대한 고찰." 지급결제학회지 15.1 (2023): 107-130

[8] L. Singh, A. Chirputkar and P. Ashok, "Risk Management in the Digital Age: Fintech Security Strategies," 2024 1st International Conference on Sustainable Computing and Integrated Communication in Changing Landscape of AI (ICSCAI), Greater Noida, India, 2024, pp. 1-7

[9] R. Lomas and Reeta, "AI-Driven FinTech Solutions for Financial Inclusion: A Study on MSME Sector Empowerment," 2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N), Greater Noida, India, 2024, pp. 1887-1891

[10] S. AlBenJasim, T. Dargahi, H. Takruri, and R.Al-Zaidi, "FinTech Cybersecurity Challenges and Regulations: Bahrain case study," Journal of Computer Information Systems, pp. 1 - 17, Sep. 2023