http://www.jsebs.org
pISSN 2288-3908
eISSN 2765-3846

The Journal of Society for e-Business Studies
Vol.27, No.2, May 2022, pp.65-77
https://doi.org/10.7838/jsebs.2022.27.2.065

머신러닝을 이용한 선불전자지급수단의 이상금융거래 탐지 연구

A Study on the Fraud Detection for Electronic Prepayment using Machine Learning

최병호(Byung-Ho Choi)*, 조남욱(Nam-Wook Cho)**

초 록

전자금융서비스가 활성화됨에 따라 전자금융 거래 건수와 거래액은 매년 증가하고 있으며, 선불전자지급 과정에서의 사이버 금융범죄도 증가하고 있다. 본 논문에서는 머신러닝 알고리즘을 이용한 선불전자지급수단의 이상금융거래 탐지모델을 제시한다. 이를 위하여 실제 선불전자거래 데이터를 익명화하여 수집하였으며, 데이터의 효과적인 특성을 추출하기 위한 전처리 작업을 수행하였다. 제안된 모델은 거래내역 기반과 이용자 ID 기반 접근법을 이용하였다. 거래내역 기반 모델 분석에서는 원데이터 기반 거래내역 분석과 특성 항목을 추가한 2차 분석을 수행하였으며, 이용자 ID 기반 모델에서도 도메인 특성에 맞는 특성 항목을 추출하여 분석에 활용하였다. 이상치 탐지를 위해 의사결정나무, 인공신경망 및 서포트 벡터 머신 알고리즘을 활용하여 비교 분석하였다. 분석결과 거래내역 기반의 탐지모델보다 이용자 ID 기반의 탐지모델이 선불거래지급수단 이상탐지에 더 효과적임을 확인할 수 있었으며, 이용자 ID 기반 모델에서는 신경망 알고리즘이 가장 좋은 성능을 나타내었다. 제안된 방법론은 향후 이상금융거래 탐지시스템 분석에 활용함으로써 전자금융사고 피해를 줄이는데 기여할 수 있을 것으로 기대된다.

ABSTRACT

Due to the recent development in electronic financial services, transactions of electronic prepayment are rapidly growing, leading to growing fraud attempts. This paper proposes a methodology that can effectively detect fraud transactions in electronic prepayment by machine learning algorithms, including support vector machines, decision trees, and artificial neural networks. Actual transaction data of electronic prepayment services were collected and preprocessed to extract the most relevant variables from raw data. Two different approaches were explored in the paper. One is a transaction-based approach, and the other

이 논문은 2022년도 정부(산업통상자원부)의 재원으로 한국산업기술진흥원의 지원을 받아 수행된 연구임 (P0017123, 2022년 산업혁신인재성장지원사업).

* First Author, Ph.D. Student, Department of Industrial & Information Systems, Graduate School of Public Policy and Information Technology, Seoul National University of Science & Technology (dadao001@seoultech.ac.kr)

** Corresponding Author, Professor, Department of Industrial & Information Systems Engineering, Seoul National University of Science & Technology(nwcho@seoultech.ac.kr)

Received: 2022-02-24, Review completed: 2022-05-04, Accepted: 2022-05-06

is a user ID-based approach. For the transaction-based approach, the first model is primarily based on raw data features, while the second model uses extra features in addition to the first model. The user ID-based approach also used feature engineering to extract and transform the most relevant features. Overall, the user ID-based approach showed a better performance than the transaction-based approach, where the artificial neural networks showed the best performance. The proposed method could be used to reduce the damage caused by financial accidents by detecting and blocking fraud attempts.

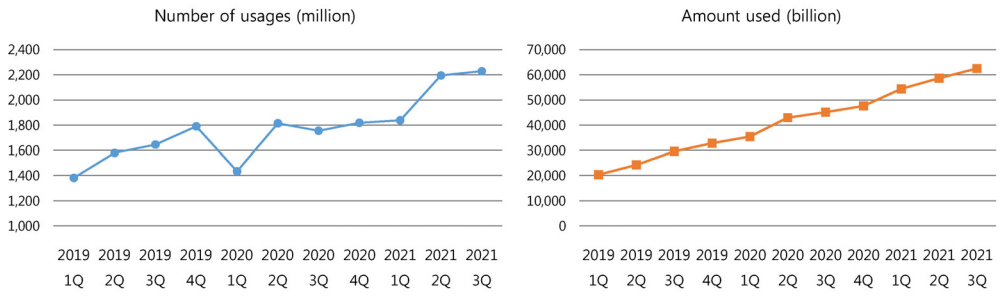
키워드 : 선불전자지급수단, 전자금융사기, 핀테크 보안, 이상금융거래탐지, 머신 러닝
Electronic Prepayment Means Electronic Financial Frauds, Fintech Security, Financial Fraud Detection, Machine Learning

1. 서 론

전자금융서비스가 활성화됨에 따라 전자금융거래 건수와 거래액은 매년 증가하고 있다. 한국은행 경제통계시스템에 따르면 2021년 3분기 전자지급결제대행(신용카드, 계좌이체, 가상계좌 포함)의 이용 건수는 18억 9천만 건으로 나타나 2020년 3분기(14억 7천만 건) 대비 28.6% 증가하였다. 인터넷뱅킹 이용 건수는 2020년 3분기 13억 9천만 건에서 2021년 3분기 15억 8천만 건으로 13.7% 증가하였다. 선불전자거래지급수단도 다른 전자금융서비스와 마찬가지로 매년 이용 건수와 이용금액이 증가하고 있다. <Figure 1>은 선불전자거래지급수단의 최근 3년간 이용 건수와 이용금액을 나타낸다[1].

전자금융서비스가 활성화됨에 따라 이를 악용한 금융범죄도 급속하게 증가하고 있어 이에 대한 대책 마련이 시급하다. 경찰청 통계자료에 따르면 사이버 금융범죄는 2019년 10,542건 발생했으며 2020년에는 20,248건으로 92.1% 증가하였다[10]. 2022년 1월 4일 휴대전화를 잃었다가 2022년 1월 5일 0시 17분부터 0시 51분까지 7차례에 걸쳐 카카오페이의 선불전자지급수단에 580만 원이 충전되고 24번에 걸쳐 약 577만 원이 이체된 사건이 발생하였다. 하지만 유사 사건이 발생한 네이버페이의 경우 이상금융거래 탐지시스템을 통해 피의자의 충전금 이체 시도를 이상금융거래로 감지하고 충전금 190만 원을 이체할 수 없도록 차단하였다[19]. 이처럼 이상금융거래 탐지시스템의 필요성은 지속해서 증가하고 있다. 최근 선불전자지급수단 거래를 기반으로 순차분석을 통한 이상금융거래 탐지 연구가 발표된 바 있으나 관련 연구는 아직도 부족한 실정이다[3].

본 논문에서는 선불전자지급수단의 금융거래 데이터를 기반으로 서포트 벡터 머신(Support Vector Machine; 이하 SVM), 의사결정나무, 인공신경망 알고리즘을 활용하여 효과적인 이상금융거래 탐지 방안을 제시하고자 한다. 이를 위하여 실제 선불전자지급수단의 거래데이터를 익명화하여 수집하고, 거래내역 기반 탐지모델과 이용자 ID 기반 탐지모델의 특성에 맞는 변수를 선택한 후 머신러닝 알고리즘을 통해 이상금융거래 탐지를 분석하였다. 본 연구는 머신러닝을 통해 거래내역 기반의 예측모델과 이용자별 이상금융거래 예측모델의 탐지 효과성을 비교 분석하였다는 데 의의가 있다.



〈Figure 1〉 Electronic Prepayment Service Usages (Quarterly)

제안된 방법론은 향후 이상금융거래 탐지시스템 분석에 활용함으로써 전자금융사고 피해를 줄이는데 기여할 것으로 기대된다.

본 논문의 구성은 다음과 같다. 제2장에서는 SVM, 의사결정나무 및 신경망에 대한 이론적 배경과 관련 연구를 소개하였다. 제3장에서는 연구방법을 설명하고, 제4장에서는 머신러닝 알고리즘별 거래내역과 이용자 데이터를 분석하여 이상치 탐지 유효성을 검증하였다. 제5장에서는 결론과 향후 연구 방향에 관해 기술하였다.

2. 이론적 배경

2.1 선불전자지급수단의 범죄이용

선불전자지급수단을 범죄에 이용하는 경로는 크게 두 가지로 나뉠 수 있다. 첫 번째는 정상 이용자 ID를 도용하여 해당 계정에 접속한 후 충전금을 환금성 상품으로 구매하는 데 사용하거나 자금을 이체하는 경우이며 이때 피해자는 서비스 회원이다. 두 번째는 범죄자가 계정을 개설하고 타인에게 충전을 유도한 후 충전금을 사용하는 경우이며 이때 피해자는 충전금을 입금한 제3자가 된다. 첫 번째 사례는 거래내역을 기반으로 이상금융거래 탐지를 통해 실시간 차단하는 정책을 고려할 수 있고, 두 번째 사례는 이용자 ID 기반 탐지모델링을 고려할 수 있다. 본 논문에서는 전자거래지급수단의 이상거래 탐지를 위해 거래내역 기반의 모델과 이용자 ID 기반 모델을 제시한다.

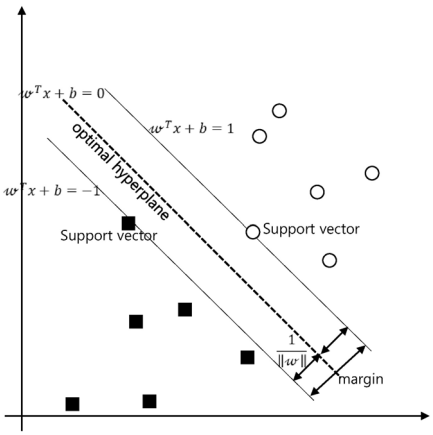
2.2 머신러닝 알고리즘

2.2.1 서포트 벡터 머신(Support Vector Machine)

서포트 벡터 머신(Support Vector Machine; SVM)은 Cortes와 Vapnik에 의해 처음 제안되었다[5, 20]. SVM은 이진 분류문제에 널리 사용되며, 두 개의 범주를 최적으로 분리해 낼 수 있는 초평면을 찾는 것을 목적으로 한다[7, 21].

SVM은 선형분류모델과 비선형분류모델로 나뉠 수 있다. <Figure 2>는 선형 분류모델에서 2개의 클래스를 분리한 초평면과 서포트 벡터에서 초평면에 달하는 거리의 합인 마진을 나타낸다. 초평면은 식 (1)과 같은 수식으로 나타낼 수 있다. 여기서 w는 가중치 벡터, x는 입력 벡터, b는 기준치이다[4, 7, 9, 25].

$$w^T x + b = 0 \quad (1)$$



〈Figure 2〉 Linear Support Vector Machine

학습데이터 집합물 D={$(x_1, y_1), (x_2, y_2), \cdots, (x_i, y_i)$}라고 할 때, $y_i = +1$ 이면 $w^Tx_i + b \rangle 0$ 이고, $y_i = -1$ 이면 $w^Tx_i + b \langle 0$이다.

$$\begin{cases} w^Tx_i + b \geq +1, & y_i = +1; \\ w^Tx_i + b \leq -1, & y_i = -1. \end{cases} \quad (2)$$

최대 마진 초평면을 구하는 식은 (3)과 같다.

$$f_{(x)} = w^Tx + b \quad (3)$$

선형 분리가 불가능한 패턴은 커널 함수 $K(x_i, x_j) = \phi(x_i)^T \cdot \phi(x_j)$를 사용하여 저차원에서 발생한 문제를 높은 차원의 공간으로 변환하고 선형 초평면을 사용하여 데이터를 분류할 수 있다. 이러한 비선형문제를 효율적으로 푸는 데 많은 도움이 된다[9]. 일반적으로 많이 사용되는 커널 함수는 다항식(Polynomial) 커널 함수, 가우시안(Gaussian) 커널 함수(RBF, Radial Basis Function), 시그모이드(Sigmoid) 커널 함수 등이 있으며 표현 식은 <Table 1>과 같다[4, 8, 9, 25].

〈Table 1〉 SVM Kernel Function

Type of Kernel	Kernel Function	Parameter
Linear	$K(x_i, x_j) = x_i^T x_j$	
Polynomial	$K(x_i, x_j) = (x_i^T x_j + 1)^d$	d ≥ 1
Gaussian (RBF)	$K(x_i, x_j) = \exp\left(-\frac{\|x_i - x_j\|^2}{2\sigma^2}\right)$	σ > 0
Sigmoid	$K(x_i, x_j) = \tanh(\beta x_i^T x_j + \theta)$	$\beta \rangle 0$, $\theta \rangle 0$

일부 데이터가 잘못된 쪽의 마진에 위치하여 선형적으로 분리할 수 없는 경우 슬랙 변수(slack variable)를 도입하여 문제를 해결할 수 있다. 즉 초평면의 잘못된 쪽에 데이터가 있다면 C값을 변경해서 페널티를 조정하는 것이다. 본 논문에서는 예측모델의 최적화를 위해 C 상숫값을 증가시키면서 학습을 진행하였다[11].

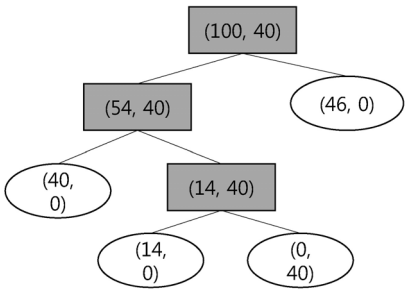
2.2.2 의사결정나무(Decision Trees)

의사결정나무(Decision Trees)는 표본집단을 특정 기준값으로 이분화하는 과정을 반복하여 트리 형태를 형성함으로써 분류 또는 회귀분석을 수행하는 분석방법이다. 의사결정나무를 생성하는 가장 대표적인 알고리즘은 CART(Classification and Regression Trees), CHAID(CHi-square Automatic Interaction Detection), C4.5 등이 있다. <Figure 3>은 주어진 데이타를 이분화 과정을 반복해서 분류하는 의사결정나무의 예를 보여주고 있다[2, 9].

트리를 형성하는 과정에서 이분화하는 방법을 분지 기준(splitting criterion)이라 하며, 기준을 설정하기 위해서는 불순도 함수를 사용한다. 불순도 함수에는 지니 지수(Gini index)와

엔트로피 지수(Entropy index)가 널리 사용된다. 본 연구에서는 지니 지수식을 사용하였으며, 식은 식 (4)와 같다.

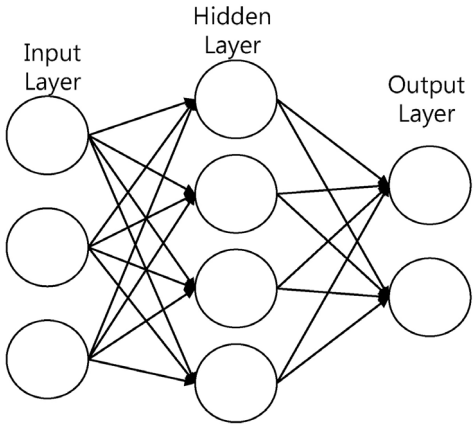
$$G(p_1,...,p_J)=1-\sum_{j=1}^{J}p_j^2=\sum_{j=1}^{J}p_j(1-p_j) \quad (4)$$



〈Figure 3〉 Structure of Decision Tree

2.2.3 인공 신경망(Artificial Neural Networks)

인공 신경망(Artificial Neural Networks, 이하 신경망)은 인간의 신경망을 흉내 낸 머신러닝 기법이다[14]. 신경망의 구조는 <Figure 4>와 같이 입력층, 은닉층, 출력층으로 구성된다.



〈Figure 4〉 Structure of the Neural Network

신경망에 입력이 주어지면 은닉층에 전달되며, 은닉층 노드는 주어진 입력에 따라 활성화되어 출력값 계산 후 출력층에 전달한다. 출력층은 최종 출력값을 계산하며 이 값이 최종 예측 결과가 된다. 각 화살표에는 가중치가 부여되며 입력층 노드 i와 은닉층 노드 j를 연결한 화살표에 가중치는 w_{ji}가 된다. 입력값을 x_1, x_2, …, x_i, …, x_n 이라고 하면 은닉층 노드 j로 가중합은 $net_j=\sum x_i w_{ji}+w_{j0}$ 와 같다. 은닉층 노드 j가 활성 함수를 통해 출력값을 출력층에 전달하게 되며 많이 사용되는 시그모이드 함수식은 식 (5)와 같다[11, 24].

$$sigmoid(net_j)=\frac{1}{1+e^{-x}} \quad (5)$$

시그모이드 함수는 0~1 사이의 출력을 내보내는 함수이다.

2.3 SMOTE(Synthetic Minority Over-sampling Technique)

머신러닝 알고리즘 적용과정에서 데이터 불균형이 심하거나 데이터의 수가 현저히 적을 때 예측모델에서 다양한 문제가 발생할 수 있다. SMOTE는 비율이 낮은 범주에 속한 데이터에서 랜덤 샘플링을 통해 원래 수보다 많은 데이터를 생성함으로써 문제를 해결하는 대표적인 오버샘플링 기법이다. 데이터를 생성하는 방법은 원본데이터에서 하나의 데이터 샘플을 선택한 후 가장 가까운 최근접 이웃을 식별한다. 선택한 데이터 샘플과 k개 이웃간 선형관계를 형성한 후 샘플들 간의 거리를 계산한다. 계산된 거리에 0과 1사이 난수를 곱한 후 새로운

샘플 위치를 식별한다. 이러한 과정을 적절한 오버샘플링 데이터 수에 도달할 때까지 반복한다[17].

2.4 이상치 탐지 관련 연구

이상치 탐지 연구는 금융, 제조, 및 정보통신 침해사고 분석 등 다양한 분야에서 활용되었다. 금융 분야 이상치 탐지 연구는 다음과 같다. Han et al.[6]은 모바일 결제 환경에서 다양한 알고리즘의 앙상블 기법을 활용하여 탐지 모듈을 2단계로 분리함으로써 탐지 속도와 정확도를 향상시키는 방안을 연구하였다. Park et al.[15]은 은행의 금융사고 데이터로 이상징후 패턴 탐지 규칙을 설정하고, 의사결정나무를 사용하여 탐지 규칙을 정규화하는 방안을 제안하였다. Park et al.[16]은 현금 인출기의 카메라를 통해 이용자의 얼굴 및 얼굴 특징점을 영상신호처리 방법과 SVM으로 분석하여 얼굴이 식별 가능한 경우에만 금융거래할 수 있도록 하는 시스템을 개발하였다. Choi and Cho[3]는 이용자별 선불전자지급수단의 거래내역 순서를 나열하고 부정이용자의 순차패턴 탐지 룰을 만든 후 순차패턴 알고리즘 분석을 통한 이상금융거래 탐지모델을 제안하였다.

제조 분야에서는 이상치를 판별하여 기계의 고장진단 및 예측 연구에 활용하였다. Hwang[7]은 SVM을 이용하여 고속철도 궤도의 이상 데이터와 정상 데이터 간의 관계를 파악하여 자동으로 궤도 이상 유무를 판단하는 방법을 제안하였다. Yang et al.[23]은 센서에서 발생하는 대표적인 고장 유형을 SVM과 Convolutional Neural Netowrks(CNNs)를 적용하여 검출하고 분류하는 연구를 수행하였다. Lee et al.[12]은 정상상태 기어펌프의 데이터와 마모된 기어펌프의 데이터를 분류하여 기어펌프의 고장을 예측하였다.

정보통신 침해사고 분석의 이상치 탐지 연구 사례는 다음과 같다. Yang and Seo[22]은 네트워크 기반의 침입 탐지시스템에서 훈련되지 않은 새로운 침입을 정상 인스턴스로 변경하여 탐지하는 방안을 연구하였다. Lee and Kook[13]은 연구에서 이미 알려진 소규모 실행 파일의 특징을 데이터마이닝 기법으로 분석하여 알려지지 않은 악성코드 탐지에 활용할 수 있는 모델을 제안하였다.

살펴본 바와 같이, 기존 연구에서는 다양한 분야에서 이상치 탐지 연구를 수행하고 있으나, 선불전자지급수단의 이상금융거래 탐지 연구는 미흡한 실정이다.

3. 연구방법

본 연구에서는 거래내역 기반과 이용자 ID 기반의 이상금융거래 탐지 분석모델을 제시한다. 거래내역 기반 모델은 거래내역의 이상치를 탐지하는 모델이며, 이용자 ID 기반 모델은 부정 이용자 ID를 탐지하는 모델이다.

연구에 사용된 데이터는 선불전자거래 업체로부터 2018년 7월부터 2019년 7월까지 추출된 선불전자지급수단의 충전, 온라인쇼핑 구매, 인출, 환불 등의 거래내역 총 13,965건이며, 이중 정상거래 데이터는 12,886건이며, 이상금융거래 데이터는 1,079건이다. 실제 거래데이터의 경우 이상 금융거래데이터의 비율이 현저히 낮아서 데이터 불균형 문제가 발생한다. 따라서 전문가가 선별한 이상거래 목록에서 이상금융거래 데이터를 따로 추출함으로써 데이터 불균

형 문제를 최소화하였다. 이상금융거래 데이터 레이블링은 관련 산업전문가가 수행하였다. 추출된 정상 이용자 ID는 386개이며, 부정 이용자 ID는 39개이다. 부정 이용자 ID 개수의 불균형을 보완하기 위해 SMOTE 알고리즘 이용하여 부정 이용자 ID 수를 39건에서 195건으로 오버 샘플링하였다. 연구를 위한 학습 및 테스트 데이터 비율은 <Table 2>와 같이 7:3 비율로 하였다. 비교실험을 위해 의사결정나무, 신경망, SVM 알고리즘을 활용하였다.

머신러닝 알고리즘 적용에 앞서 도메인 특성(feature)에 맞는 변수를 선택하고 가공하였다. <Table 3>은 거래내역 기반 이상금융거래 탐지 접근법에 활용된 변수들을 나타낸다.

거래내역 기반 1차 분석모델에서는 거래일차, 거래 요일, 이용시간, 이용시간 범위, 서비스 코드, 거래금액 정보를 활용하였다. 분석항목 중 코드값은 선불전자지급수단을 이용한 서비스를 국세청 '귀속업종분류코드' 기준으로 작성하였고, 거래금액은 9단계로 분류하였다. 1단계는 0~3,000원, 2단계는 3,001원~5,000원, 3단계는 5,001원~10,000원, 4단계는 10,001원~30,000원, 5단계는 30,001원~50,000원, 6단계는 50,001원~100,000원, 7단계는 100,001원~150,000

〈Table 2〉 Analysis Data

		Fraud (FRD)	Normal (NOR)	Total	Ratio to Total
Transaction Data	Training Data	755	9020	9775	69.96%
	Test Data	324	3866	4190	30.04%
	Total	1,079	12,886	13,965	100%
User ID Data	Training Data	136	273	409	69.91%
	Test Data	59	117	176	30.09%
	Total	195	390	585	100%

〈Table 3〉 Description of Transaction Data Structure

	Feature	Data Range	Description
Original Transaction Data	Day_diff	Number	Difference between the transaction days
	Day_week	1~7	Transaction day of the week
	Time1	0~24	Transaction time (24h)
	Time2	1~8	Time range(3h)
	Code	Code Number	Transaction code
	Amount_range	1~9	Transaction amount
Additional Features	Withdrawal	0 or 1	Binary (Yes: 1, No: 0)
	Refund	0 or 1	
	Online-mall	0 or 1	
	Accommodation	0 or 1	
	Financial transaction	0 or 1	

원, 8단계는 150,001원~300,000원, 9단계는 300,000원 초과 금액을 기준으로 하였다.

2차 분석에서는 이상금융거래 탐지를 정교화하기 위해 정상 및 부정거래 차이가 나타났던 현금인출, 환불, 쇼핑몰이용, 숙박 이용, 금융거래 등 5개의 특성을 추가하였다.

이용자 ID 기반 접근법에서는 <Table 4>와 같이 이용자 ID를 기준으로 12개 특성을 추출하였다. 전체 서비스에 대한 이용 건수 및 전체 거래의 평균 이용액, 금융거래 이용 건수 및 금융거래 이용 평균 거래금액, 출금 이용 건수 및 출금 평균 이용금액, 환불 이용 건수 및 환불 이용 평균 금액, 숙박 이용 건수 및 숙박 평균 이용금액, 쇼핑몰 이용 건수 및 쇼핑몰 평균 구매금액을 활용하였다. 거래금액은 거래내역 기반 모델과 마찬가지로 9단계로 구분하여 처리하였다.

〈Table 4〉 Description of User ID Data Structure

	Feature	Data Range
Items	Total number of services	Number
	Average transaction amount(service)	1~9
	Total number of financial services	Number
	Average financial transaction amount	1~9
	Total number of withdrawals	Number
	Average withdrawal amount	1~9
	Total number of refunds	Number
	Average refund amount	1~9
	Total number of accommodations	Number
	Average amount of accommodation	1~9
	Total number of shopping uses(Open market)	Number
	Average amount for shopping (Open market)	1~9

본 연구에서 활용된 도구는 R 4.0.5버전과 데이터 불균형의 개선에 “DMwR” 패키지의 SMOTE 알고리즘을 이용하였다. 머신러닝 알고리즘 중 SVM의 경우 e1071패키지의 SVM 알고리즘을 사용하였고, 의사결정나무의 경우 “rpart”패키지의 CART(Classification and Regression Trees) 알고리즘을 사용하였으며, 신경망 모형에는 “nnet”패키지의 nnet함수의 신경망 알고리즘을 활용하였다[18].

4. 분석 결과

4.1 거래내역 기반 이상금융거래 탐지결과

본 연구에서는 거래데이터 9,775건을 의사결정나무, 신경망 및 SVM 알고리즘으로 각각 학습시킨 후 테스트데이터 4,190건을 예측모델에 활용하였다. <Table 5>는 거래내역을 기반으로 하는 1차 분석 결과이며, 분석의 초점이 이상금융거래 탐지에 있으므로 Fraud를 Positive로, Normal을 Negative로 정의하였다.

SVM의 경우 C=41에서 최적의 이상치 탐지결과를 보였으며, 정밀도(Precision)는 59.7%이며, 재현율(Recall)은 58.6%, 정확도(Accuracy)는 93.7%로 나타났다. 의사결정나무의 경우 정밀도는 62.0%, 재현율은 35.8%, 정확도는 93.3%로 나타났다. 신경망의 경우 정상 데이터 및 부정거래 데이터의 불균형과 서비스 코드 데이터가 이상금융거래 탐지에 부정적인 영향을 준 것으로 판단되며, 재현율의 비율이 낮아 이상금융거

래 탐지모델로 이용하기에는 적합하지 않은 것으로 판단된다.

〈Table 5〉 Fraud Detection Result: Transaction-based Approach

			Actual	
			Fraud (Positive)	Normal (Negative)
SVM	Prediction	Fraud (Positive)	190	128
		Normal (Negative)	134	3738
Decision Tree	Prediction	Fraud (Positive)	116	71
		Normal (Negative)	208	3795
Neural Network	Prediction	Fraud (Positive)	0	0
		Normal (Negative)	324	3866

	SVM	Decision Tree	Neural Network
Precision	0.597	0.620	NA
Recall	0.586	0.358	NA
Accuracy	0.937	0.933	0.923

거래내역 기반 2차 분석에서는 현금인출, 환불, 쇼핑몰이용, 숙박 이용, 금융거래 이용 여부를 특성으로 추가하였다. 현금인출, 환불, 숙박 이용, 금융거래 이용은 부정거래에서 많은 비율을 차지하고 있으며, 쇼핑 거래내역은 정상거래에서 많은 비율을 차지하고 있는 특성을 보였기 때문에 이상금융거래 탐지를 정교화하기 위해 추가되었다. 2차 분석 결과는 <Table 6>과 같다. SVM의 정밀도는 67.5%, 재현율은 59.0%, 정확도는 94.6%로 나타나, 1차 분석보다 정밀도는 7.8%, 재현율은 0.4%, 정확도는 0.9%씩 각각 증가하였다. 의사결정나무의 경우 정밀도는 86.4%, 재현율은 27.5%, 정확도는 94.1%로 평가되었다. 신경망의 경우 1차 분석과 마찬가지로 재현율이 낮아 이상금융거래 탐지에 적합하지 않은 것으로 나타났다.

〈Table 6〉 Fraud Detection Result: Transaction-based Approach with Additional Features

			Actual	
			Fraud (Positive)	Normal (Negative)
SVM	Prediction	Fraud (Positive)	191	92
		Normal (Negative)	133	3774
Decision Tree	Prediction	Fraud (Positive)	89	14
		Normal (Negative)	235	3852
Neural Network	Prediction	Fraud (Positive)	0	0
		Normal (Negative)	324	3866

	SVM	Decision Tree	Neural Network
Precision	0.675	0.864	NA
Recall	0.590	0.275	NA
Accuracy	0.946	0.941	0.923

4.2 이용자 ID 기반 이상금융거래 탐지결과

이용자 ID 기반 모델에서 의사결정나무, 신경망 및 SVM을 이용해 이상금융거래를 예측한 결과는 <Table 7>과 같다. 모델 성능은 전반적으로 거래내역기반 모델보다 우수한 것으

로 나타났다. 머신러닝 알고리즘 가운데, 신경망이 가장 우수한 성능을 나타냈으며, 의사결정나무, SVM 순으로 우수한 성능을 나타내었으나 알고리즘 성능 차이는 크지 않았다.

〈Table 7〉 Fraud Detection Result : User ID-based Approach

			Actual	
			Fraud (Positive)	Normal (Negative)
SVM	Prediction	Fraud (Positive)	49	0
		Normal (Negative)	10	117
Decision Tree	Prediction	Fraud (Positive)	59	6
		Normal (Negative)	0	111
Neural Network	Prediction	Fraud (Positive)	59	1
		Normal (Negative)	0	116

	SVM	Decision Tree	Neural Network
Precision	1.0	0.908	0.983
Recall	0.831	1.0	1.0
Accuracy	0.943	0.966	0.994

거래내역 기반과 이용자 ID 기반 모델에서 가장 우수한 성능을 보인 결과를 <Table 8>에 요약하였다. 정상데이터와 이상금융거래 데이터의 불균형으로 인해 정밀도와 재현율을 비교하는 것이 중요하다. 1차 거래내역 기반에서는 SVM이 정밀도 59.7%, 재현율 58.6%를 나타내었고 2차 거래내역 기반분석에서는 정밀도, 재현율이 각각 67.5%, 59.0%로 나타났다. 이용자 ID 기반에서는 정밀도, 재현율이 각각 98.3%, 100%로 나타남에 따라, 이용자 ID 기반의 접근법이 거래내역 기반의 접근법보다 더 효과적인 것으로 나타났다.

〈Table 8〉 Comparison of Fraud Detection Result

Model/ Algorithm	Transaction 1	Transaction 2	User ID
	SVM	SVM	Neural Network
Precision	59.7%	67.5%	98.3%
Recall	58.6%	59.0%	100%
Accuracy	93.7%	94.6%	99.4%

5. 결 론

본 연구에서는 SVM, 의사결정나무, 신경망 등 머신러닝 알고리즘을 통해 금융 거래내역과 이용자 ID 기반의 이상금융거래 탐지 예측모델을 비교 분석하였다. 거래내역 기반 모델에서는 예측정확도 향상을 위해 5개의 특성(현금인출, 환불, 쇼핑몰이용, 숙박 이용, 금융거래)을 추가한 2차 분석을 수행하였다.

거래내역 기반 모델의 실험결과 1차 분석과 비교하면 특성을 추가한 2차 분석 결과가 향상됨을 확인하였으나, 이용자 ID 기반 모델의 성능에 비해서는 저조한 것을 확인하였다.

종합하면 거래내역 기반의 접근법보다 이용자 ID 기반의 접근법이 더 효과적인 것으로 나타났다. 이용자 ID 기반 모델에 적용된 머신러닝 알고리즘 가운데 신경망이 상대적으로 우수한 성능을 보였으나 다른 알고리즘과 차이는 크지 않았다.

본 연구는 실제 선불전자지급수단의 데이터를 기반으로 머신러닝 방법론을 적용하여 이상금융거래를 효과적으로 탐지할 수 있는 기법을 제시하였다는 데 연구의 의의가 있다. 본 연구를 통해 제시된 방법론이 이상금융거래 탐지시스템에 활용됨으로써 이상금융거래를 차단하거나 부정 이용자 ID의 거래 한도를 제한하여 전자금융사고 피해를 줄일 수 있을 것으로 기대된다.

본 연구의 의의에도 불구하고 본 연구는 다음과 같은 한계를 가지고 있다. 첫째, 분석에 사용된 데이터 수가 정상거래와 이상금융거래의 차이가 크고, 이용자 ID 분석에 사용된 계정과 거래데이터 수가 적어 분석에 한계가 있었다. 둘째, 선불전자지급수단의 거래내역을 기반으로 분석하였기 때문에 다른 금융서비스의 데이터 분석에 동일한 결과가 도출되지 않을 수 있다. 따라서 이용자의 정보(성별, 연령층 등) 및 다른 금융서비스 정보를 연계한 이상금융거래 탐지모델의 개발을 추후 연구과제로 진행할 예정이다.

References

[1] Bank of Korea, “Economic Statistics System - Search in Statistical Classification,” https://ecos.bok.or.kr/flex/EasySearch_e.jsp, 2022.01.29.

[2] Breiman, L., Stone, C. J., Feieman, J. H., and Olshen, L. A., “Classification and regression trees,” Chapman & Hall/CRC, London, 1984.

[3] Choi, B. H. and Cho, N. W., “A study on the fraud detection through sequential pattern analysis,” The Journal of Society for e-Business Studies, Vol. 26, No. 3, pp. 21-32, 2021.

[4] Chung, Y. M. and Lim, H. Y., “An experimental study on text categorization using an SVM classifier,” Journal of the Korean Society for information Management, Vol. 17, No. 4, pp. 229-248, 2001.

[5] Cortes, C. and Vapnik, V., “Support-vector networks,” Machine Learning, Vol. 20, No. 3, pp. 273-297, 1995.

[6] Han, H. C., Kim, H. N., and Kim, H. K., “Fraud detection system in mobile payment service using data mining,” The Journal of Korea Institute of Information Security & Cryptology, Vol. 26, No. 6, pp. 1527-1537, 2016.

[7] Hwang, S. W., “A study on distinction of deterioration of high speed railway track using an SVM,” Kangwon National University, 2013.

[8] Jan, S. U., Lee, Y. D., Shin, J. P., and Koo, I. S., “Sensor fault classification based on support vector machine and statistical time-domain features,” IEEE Access, Vol. 5, pp. 8682-8690, 2017.

[9] Jun, C. H., “Data Mining Techniques,” Hannarae Publishing Co, Seoul, 2012.

[10] Korean National Police Agency, Cyber Investigation - Status for cyber crime arrest, https://www.police.go.kr/eng/statistics/statisticsSm/statistics04.jsp, 2022.01.29.

[11] Lantz, B., “machine learning with R -

Second Edition," (Yoon, S. J., Trans), acornpub.co, Seoul, 2017 (Original work published 2015).

[12] Lee, G. H., Shin, B. C., and Hur, J. W., "Fault classification of gear pumps using SVM," Journal of Applied Reliability, Vol. 20, No. 2, pp. 187-196, 2020.

[13] Lee, T. H. and Kook, K. H., "A study on detection of small size malicious code using data mining method," Journal of Information and Security, Vol. 19, No. 1, pp. 11-17, 2019.

[14] McCulloch, W. S. and Pitts, W., "A logical calculus of the ideas immanent in nervous activity," The Bulletin of Mathematical Biophysics, Vol. 5, No. 4, pp. 115-133, 1943.

[15] Park, J. H., Kim, H. K., and Kim, E. J., "Effective normalization method for fraud detection using a decision tree," The Journal of Korea Institute of Information Security & Cryptology, Vol. 25, No. 1, pp. 133-146, 2015.

[16] Park, K. R., Kim, J. H., and Lee, S. H., "facial Feature Verification System based on SVM Classifier," KIPS Transactions on Software and Data Engineering, Vol. 11, No. 6, pp. 675-682, 2004.

[17] Seo, J. H., "A Study on the Performance Evaluation of Unbalanced Intrusion Detection Dataset Classification based on Machine Learning," Journal of Korean Institute of Intelligent Systems, Vol. 27, No. 5, pp. 466-474, 2017.

[18] Seo, M. K., "Practical data processing and analysis using R," Gilbut, Seoul, 2019.

[19] Seoulshinmun, "Customer lost his phone and all his assets were stolen with Kakao Pay, but NaverPay was different," https://www.seoul.co.kr/news/newsView.php?id=20220109500066, 2022.01.09.

[20] Vapnik, V., "An overview of statistical learning theory," IEEE Transactions on Neural Networks, Vol. 10, No. 5, pp. 988-999, 1999.

[21] Vapnik, V., "The Nature of Statistical Learning Theory," Springer, New York, NY, 1995.

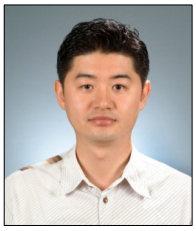
[22] Yang, E. M. and Seo, C. H., "A study on intrusion detection in network intrusion detection system using SVM," The Society of Digital Policy & Management, Vol. 16, No. 5, pp. 399-406, 2018.

[23] Yang, J. W., Lee, Y. D., and Koo, I. S., "Sensor fault detection scheme based on deep learning and support vector machine," The Journal of The Institute of Internet Broadcasting and Communication (IIBC), Vol. 18, No. 2, pp. 185-195, 2018.

[24] Yeo, W. K., Seo, Y. M., Lee, S. Y., and Jee, H. K., "Study on water stage prediction using hybrid model of artificial neural network and genetic algorithm," Journal of Korea Water Resources Association, Vol. 43, No. 8, pp. 721-731, 2010.

[25] Zhou, Z. H., "Machine Learning," (Kim, K. H., Trans), Jeipub, Paju, Gyeonggi-do, 2020 (Original work published 2016).

저 자 소 개



최병호 (E-mail: dadao001@seoultech.ac.kr)
2001년 상명대학교 정보통신학 (학사)
2016년 동국대학교 국제정보대학원 사이버포렌식 (석사)
2020년 서울과학기술대교 IT정책전문대학원 산업정보시스템 박사수료
관심분야 Fraud Detection, Social Network Analysis, Data Mining, Financial Technology Security

조남욱 (E-mail: nwcho@seoultech.ac.kr)
1994년 서울대학교 산업공학과 (학사)
1996년 서울대학교 산업공학과 (석사)
2001년 퍼듀대학교 산업공학과 (박사)
2004년~현재 서울과학기술대학교 산업공학과 교수
관심분야 Social Network Analysis, Business Performance Analysis