머신러닝 기반의 이상거래 탐지시스템 동향

(보안기술연구팀, 2017.8.25.)

1 개 요

□ 전자금융거래의 거래량 증가와 간편 결제 수단의 다양화, 동시에 나날이 치밀해져가는 사이버 금융 사기(Fraud) 방법들은 금융회사의 사기 탐지를 어렵게 만듦

○ 이에 금융권에서는 전자금융거래를 노린 사기 행위를 사전에 탐지 및 차단하여 거래의 보안성을 향상시키는 이상거래 탐지시스템(Fraud Detection System, FDS)을 도입

□ 한편, 최근 대량의 정보를 학습하여 예측·분류의 정확도를 향상시키는 머신러닝 기술이 발전하면서, 금융회사에서는 FDS 성능 고도화 방안으로 머신러닝 기술에 관심

○ 금융회사는 머신러닝 기반 FDS 운영을 통해 시스템의 향상된 탐지율, 이상행위에 대한 신속한 대응, 자동화된 탐지 결과 반영 등을 기대[1)]

< FDS 기술 변천과정 >

○ 금융거래 기술의 발전에 따라 사기 탐지 방식이 점차 컴퓨터 기반의 자동화 학습 방식으로 변화

⑴ 전자금융거래의 사기 탐지를 위해 초기에는 색출샘플링(Discovery Sampling)[2)]과 같은 방법이 이용되었으나 거래량 및 거래과정의 복잡도 증가 등으로 인해 이상거래탐지가 어려워짐

⑵ 탐지의 효율성 증가를 위해 컴퓨터 기반으로 자동화된 FDS가 개발되었지만, 전문가가 사전에 정의한 룰(규칙)에 의존하는 동작 방식으로 한계에 부딪힘

1) The Role of Machine Learning in Fraud Management, CyberSource, 2016

(3) 룰 기반 FDS의 한계를 극복하고자 인간의 개입을 최소화하고 누적된 금융거래 정보의 활용을 극대화시키는 데이터마이닝 기반 FDS가 연구 개발
- 데이터마이닝 기반 FDS는 수학, 통계, 머신러닝 등의 알고리즘을 사용하여 룰 생성 및 반영, 새로운 사기 패턴 발견 등을 자동화함으로서 사기 패턴을 일반화하고 오탐률을 감소시킴

□ 이에 본 보고서에서는 FDS의 머신러닝 활용 목적과 이상거래탐지 과정상의 머신러닝 기술 활용에 대해 소개

2 FDS의 머신러닝 활용 목적

□ 인공지능 구현 기술로 알려진 머신러닝은 수학적 알고리즘의 반복을 통해 기계 스스로가 대량의 과거 정보를 학습하게 함으로서 인간이 발견하기 어려운 정보 안의 패턴을 식별하고 이를 기반으로 예측·분류 등을 수행[3]

○ 따라서, 금융회사는 머신러닝을 활용한 사기 탐지 방식이 전통적 방식(룰, 인간에 의한 수동적 탐지) 보다 정확성, 신규 패턴 발견 가능성, 대응속도, 편리성 등을 향상시킬 것으로 기대

- **(실시간 의사결정)** 머신러닝 기술과 컴퓨팅 파워(CPU, GPU 등)의 발전은 금융회사가 실시간으로 금융거래를 모니터링하고 탐지된 비정상 거래 행위에 대해 즉각적인 대응 기회를 제공

- **(시스템 자동화)** 인간의 직접적인 시스템 튜닝, 블랙/화이트 리스트 및 통계적 규칙의 등록·갱신·삭제 등의 과정을

2) 색출샘플링(Discovery Sampling): 모집단에서에서 표본을 추출한 후, 표본을 대상으로 사기 거래와 같은 이상 징후 탐지를 수행. 한 건의 오류(이상 징후)라도 탐지되지 않은 경우 모집단을 수용하지만, 오류가 탐지된 경우 샘플링 크기를 증가시키면서 수용가능 한 이상 징후 비율을 측정. 이에 따라 모집단의 수용 여부를 결정

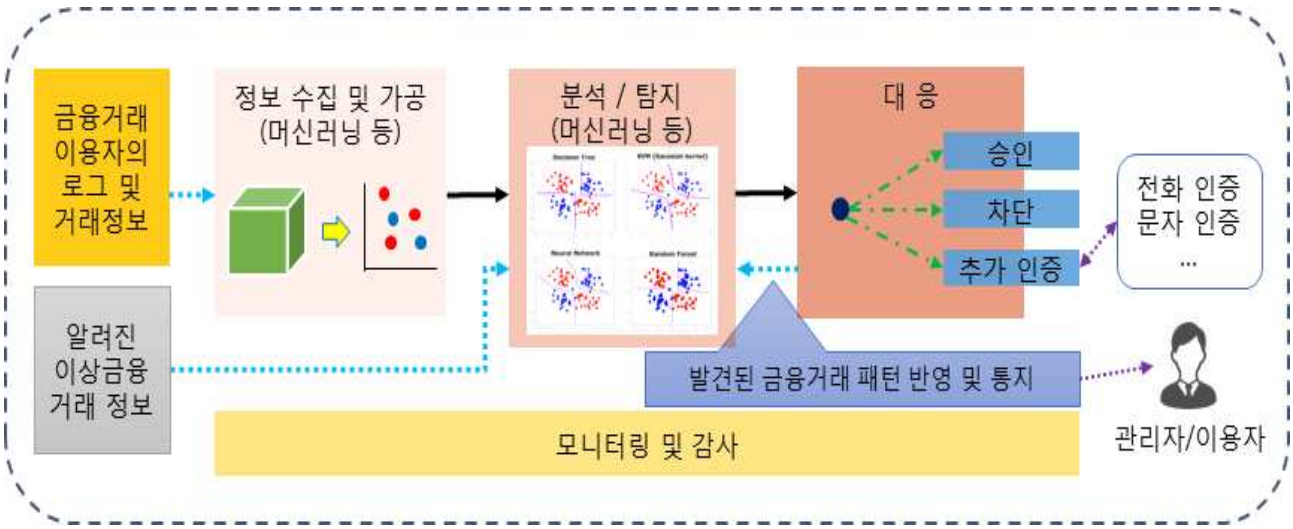
3) Andras Cser, Stop Billions In Fraud Losses With Machine Learning, Forrester, 2015.4.6.

머신러닝으로 자동화함으로써 시스템 유지 관리에 효율성 제고

- **(정확도 향상)** 기존 시스템에서 다루기 어려웠던 대량의 정보를 학습하여 시스템의 탐지 정확도를 향상 시키고, 지금까지 발견이 어려웠던 이상 징후를 탐지하며, 오탐은 인간으로부터 피드백 받음으로서 지속적인 성능 개선 가능

3 이상거래 탐지과정에서의 머신러닝 적용

□ **(FDS 구성요소)** 도입 권역(은행, 카드 등)에 따라 구성 방식에 차이가 있을 수 있으나, 크게 4가지 영역인 정보수집 및 가공, 분석/탐지, 대응, 모니터링 및 감사로 구성[4)]



[그림 1] 이상거래 탐지시스템(FDS) 구성 예시

○ **(정보 수집 및 가공)** 금융거래 이용자의 PC, 모바일 등에서 수집한 정보(금융거래 단말기, 로그인, 거래은행 등)를 축적하고, 시스템(분석/탐지 단계)에서 필요한 형태로 전처리

4) 금융보안연구원, 이상금융거래 탐지시스템 기술 가이드, 2014.8.

- 시스템에서 다양한 출처로부터 수집된 대량의 정보를 곧바로 사용하는 것은 어렵고, 시스템 복잡도를 증가시킬 수 있어 정보의 질적 향상 및 양적 감소 등을 위한 과정이 수행
- 정보가공을 위해 정보의 질적 손실은 최소화하면서 양을 축소하는 머신러닝 방법 중 하나인 차원축소(Dimensionality Reduction)[5] 등이 주로 연구되고,
- 차원축소 방법으로는 크게 특징선택(Feature Selection)[6], 특징추출(Feature Extraction)[7]이 존재

○ **(분석/탐지)** 전처리된 금융거래 정보와 이상금융거래 유형 정보를 머신러닝으로 분석하여 이상거래 탐지

- 분석방법으로 오용(Misuse)탐지, 이상(Anomaly)탐지 등이 존재하며, 각 방법에 대한 설명은 아래 "FDS의 주요 분석/탐지 방법" 표와 같음

<FDS의 주요 분석/탐지 방법>

분석방법	분석모델	설명
오용 탐지 (Misuse)	패턴탐지, 상태전이	- 금융거래정보들 중 '사기'에 해당하는 정보들을 통계, 휴리스틱 등의 방법을 사용하여 시그니처(=룰, 규칙)를 정의하고, 이를 기반으로 '사기'와 '비(非) 사기'를 판별 - 전문가 시스템(Expert System)으로 볼 수 있으며, 빠르고 단순한 구조

5) 차원축소(Dimensionality Reduction): 다양한 특징(속성)을 가지는 고차원(high-dimension)의 데이터를 머신러닝 등의 알고리즘에서 처리할 경우, 용량이 큰 전체 데이터와는 반대로, 데이터 내의 각 특징별 데이터 수는 적어지는 현상이 나타날 수 있음. 이로 인해 머신러닝이 적절히 이루어지지 않거나 과적합(Overfitting), 메모리 사용량 증가, 알고리즘 연산의 복잡성 증가 등의 현상이 발생 가능. 따라서 수집된 데이터를 가장 잘 대표할 수 있는 주요 특징들을 고르는 차원축소 과정이 필요

6) 특징선택(Feature Selection): 분석에 사용되어질 관련 있는 특징(속성)들을 직접 선택하는 방법. 대표적인 방법으로 Lasso, Information Gain, Laplacian Score 등이 존재

7) 특징추출(Feature Extraction): 고차원(high-dimension)의 특징을 갖는 원본 데이터를 저차원(low-dimension)으로 투영(projection)시킴으로써 새로운 특징 데이터를 추출. 새롭게 생성된 데이터는 대게 원본 데이터와 선형 또는 비선형 관계를 가짐. 대표적인 방법으로 PCA(Principle Component Analysis), LDA(Linear Discriminant Analysis), SVD(Singular Value Decomposition) 등이 존재

		- **(이슈)** 잘 알려지지 않은 '사기' 패턴의 경우 기존에 등록된 시그니처로 탐지되지 않아 발견이 어려움 - 이러한 이슈로 이상탐지 방법이 사용
이상 탐지 (Anomaly)	지도학습 (Supervised)	- 분석/탐지를 위해 수집되어진 금융거래정보들을 '사기', '비(非) 사기'로 태깅하고, 두 영역을 학습하여 각 경우에 대한 일반적인 패턴을 추출 - 추출된 금융거래패턴을 이용하여 새롭게 입력되는 금융거래가 '사기'인지 '비(非) 사기'인지 판별 - **(이슈)** 수집된 대용량 금융거래정보들 중 '사기'에 해당하는 정보가 많지 않고, 태깅된 정보들로 만드는 것이 어려움 - 이러한 이슈로 비지도학습 또는 하이브리드(지도학습+비지도학습) 방법이 사용
	비지도학습 (Unsupervised)	- 수집되어진 금융거래정보들을 태깅하지 않고, 시스템이 정보들을 분석하여 그룹화 - 각 그룹은 '사기', '비(非) 사기' 등으로 분류되고, 그룹별 특성과 새롭게 입력되는 금융거래의 특성을 비교하여 '사기'인지 '비(非) 사기'인지 판별 - **(이슈)** '사기' 거래정보에 대한 정확한 태깅 없이 학습함으로 지도학습 방법에 비해 오탐률이 높을 수 있음
	하이브리드 (지도+비지도)	- 금융거래정보들 중 적은양의 일부를 '사기', '비(非) 사기'로 태깅하고, 나머지는 태깅이 없는 형태로 학습
하이브리드 (오용+이상) 탐지	- 오용탐지와 이상탐지 방법이 가진 단점을 상호 보완하는 방식 - 알려지지 않은 '사기' 패턴은 이상탐지로 탐지하고, 상대적으로 높은 이상탐지의 오탐률을 오용탐지로 감소	

– 현재까지 룰 기반의 오용탐지 방법이 많이 사용되고 있지만 최근 딥러닝 기반의 이상탐지 또는 하이브리드(오용+이상) 탐지 방법이 도입 중

– 이상탐지 방법에서 사용되는 주요 머신러닝 알고리즘으로 규칙 유도(Rule Induction)[8], 랜덤포레스트(Random Forest)[9],

서포트벡터머신(SVM)[10], 자기조직화맵(SOM)[11], 은닉마코브모델(HMM)[12], 유전알고리즘(GA)[13], 딥러닝(Deep Learning)[14] 등이 존재

○ **(대응)** 이상거래로 판별된 거래정보에 대해 승인/차단/추가인증 등을 수행하며, FDS에서 재사용할 수 있도록 저장하고 관리자 및 이용자에게 통지

○ **(모니터링 및 감사)** FDS 전 과정에 대한 관리 및 모니터링을 수행하고, 경우에 따라 수집될 수 있는 개인정보 등에 대한 관리 방안 제공

4 국내·외 머신러닝 기반 FDS 활용 현황

□ 머신러닝의 FDS 적용은 국내보다 국외에서 활발히 이루어졌으며, 금융회사들은 주로 머신러닝 기술 전문 업체와 협력하여 시스템을 구축

---

8) 규칙 유도(Rule Induction): 데이터의 패턴을 찾아 IF-THEN 형태의 규칙으로 정의하는 방법. 데이터의 일부 또는 전체를 표현하는 규칙을 반복적으로 찾아나가면서 규칙 집합을 생성하고, 과적합(Overfitting)을 완화시키기 위해 프루닝(가지치기) 과정을 거침

9) 랜덤포레스트(Random Forest): 단일 학습 알고리즘의 성능보다 더 높은 성능을 얻기 위해 다중 학습 알고리즘을 사용하는 앙상블 학습 방법의 일종으로, 다수의 의사결정나무 알고리즘으로부터의 평균치를 이용하여 동작
※ 의사결정나무(Decision Tree): 다수의 변수로 표현되는 데이터 집합에서 정해진 규칙에 따라 변수들을 반복적으로 분할함으로써 전체 데이터 집합에 대한 분류나무를 생성. 대표적으로 ID3, C4.5, C5.0, CART 등의 알고리즘이 존재

10) 서포트벡터머신(SVM, Support Vector Machine): 딥러닝 활성화 이전까지 일반적으로 많이 사용되어진 분류 알고리즘으로 기본적으로는 데이터를 두 개의 그룹으로 분류하며, 이 때 2개의 그룹으로 데이터를 분류하는 최적의 기준선을 찾는 것이 알고리즘의 목적. 또한 N개의 그룹으로 데이터를 분류하기 위해 커널트릭을 사용

11) 자기조직화맵(SOM, Self-Organizing Map): 비지도학습 신경망 모델의 유형 중 하나로 정보 집합을 그래프로 표현하여 분석할 수 있으며, 유사한 패턴을 가진 정보들을 클러스터링

12) 은닉마코브모델(HMM, Hidden Markov Model): 음성·필기·동작 인식 등과 같이 시간에 따라 변화하는 것에서 패턴을 인식하는데 유용. 확률이론을 기반으로 하며 이전 상태와 현재 상태의 값을 이용해 미래의 값을 예측하는 방법. 고려하는 상태의 수에 따라 알고리즘의 복잡도가 증가

13) 유전알고리즘(GA, Genetic Algorithm): 유전학에서 다윈의 진화론 개념을 이용한 것으로 유전자가 세대를 반복하면서 자연환경에 적응할 수 있는 적합한 형태로 변이하고 살아남는 것처럼 해결하고자 하는 문제의 가능한 해들을 대상으로 선택, 교차, 변이 등을 수행함으로써 가능한 최적의 해를 찾아내는 방법

14) 딥러닝(Deep Learning): 인간의 신경망 구조에서 착안한 학습 알고리즘으로 입력층, 출력층, 다수의 은닉층을 구성하여 학습하는 방식. 대표적으로 심층 신경망, 컨볼루션 신경망, 재귀적신경망, 오토인코더 등이 존재

○ 사용하는 머신러닝 기술로 최근 우수한 성능을 보이는 딥러닝이 주로 채택되었으며, 그 외 기존에 알려진 자기조직화맵, 서포트벡터머신, 랜덤포레스트 기술 등이 활용

○ 한편, 대다수 기업이 **머신러닝 도입 여부와 도입 시 사용한 기술을 비공개**

□ 국외 금융회사의 머신러닝 기반 FDS 활용

○ (Paypal) 딥러닝 기반의 FDS가 금융거래 고객 약 1억 7천만명이 발생시킨 약 40억 건의 거래정보를 학습하여 사기 탐지를 수행

○ (BillGuard) 고객의 신용카드 사용과 은행계좌 이체를 딥러닝 기반 시스템으로 모니터링하고, 이상징후 발생 시 해당 고객의 사용자 앱으로 통지

○ (Sul America) 보험 클레임의 약 20%가 사기, 남용 등에서 비롯된 것을 파악하고, 보험금 지급 및 클레임 과정에서의 정확성, 유효성 등을 확인하고자 딥러닝 기반 시스템을 도입

○ (D'Oro) 사기로 인한 은행 손실을 감소시키기 위해 딥러닝 기반 FDS 도입

○ (BAE System) 금융거래 모니터링을 위해 자기조직화맵 알고리즘 기반의 NetReveal 시스템을 개발하였으며, 이를 통해 유사한 패턴을 보이는 금융거래자들의 행위를 그룹화하여 이상행위 식별

○ (US Credit Issuer) 랜덤포레스트, 서포트벡터머신 등 여러 머신러닝 알고리즘을 활용한 시스템을 도입하여 이상거래의 탐지율 향상

○ **(US Bank)** AML(Anti Money Laundering) 시스템의 오탐률을 낮추고자 비지도 및 지도학습 기반의 머신러닝 솔루션 도입

□ 국내 금융회사에서는 카드사와 은행을 시작으로 머신러닝 기반 FDS를 도입(예정 포함)하여 운영

○ **(SK증권)** 룰 방식(오용탐지)과 딥러닝 방식(이상탐지)이 혼합된 하이브리드(오용+이상 탐지) FDS 도입

○ **(신한은행)** 딥러닝 기반 FDS의 모형을 구축하고, 개발한 학습 모형 16개에 대해 기존 방식과의 정확도 비교 결과 딥러닝 기반 모형의 우수성 확인

○ **(한국스마트카드)** 딥러닝 기반 FDS를 구축하였고, 시스템 오류를 이상거래로 탐지하는 등의 오탐이 발견되었으나 실제 이상거래에 대해서는 우수한 탐지 성능을 보임

○ **(KB국민카드)** '17년 3분기 내 딥러닝 기반 FDS 도입 예정

5 결론

□ 금융 분야의 이상거래 탐지시스템(FDS) 활용은 이미 활성화된 상태로 현재는 머신러닝 기술을 적용하여 시스템의 성능 향상을 도모하거나 관심 수준

□ FDS를 도입한 회사가 직면하는 주요 이슈로 Concept Drift[15]의 어려움, 정상/비정상 정보의 불균형, 대용량 정보의 축소, 실시간 탐지의 어려움 등이 존재 할 수 있으며,

15) Concept Drift: 시간의 흐름에 따라 변화하는 인간 행위 등의 현상을 모델링하는 연구로 FDS에서의 Concept Drift는 시간에 따른 합법적인 이용자와 불법적인 이용자의 행위 모델링을 의미

○ 이는 금융 분야 등에서 사기 탐지를 연구해온 학계의 주요 연구 이슈[16]와 유사

○ 주요 이슈 중 Concept Drift를 제외한 실시간탐지, 정상/비정상 정보의 불균형, 대용량 정보의 축소는 머신러닝과 관련 있는 부분이며, 각 항목에 대한 설명은 아래 "FDS의 주요 이슈" 표와 같음

<FDS의 주요 이슈>

이슈 항목	설명
실시간 탐지	- FDS는 크게 이상징후 발견 시 즉각적인 대응을 하는 온라인 방식과 그렇지 않은 오프라인 방식이 존재 - 금융 분야와 같이 온라인 방식이 주로 요구되는 상황을 위해 제한된 자원(시간, 컴퓨팅 파워 등)을 기반으로 다양한 머신러닝 알고리즘들이 효과적으로 동작할 수 있도록 연구 중
정상/비정상 정보의 불균형	- 사기 탐지를 위해 수집된 정보를 정상 행위와 비정상 행위(사기 패턴 등)로 분류할 때 비정상 행위 정보의 양이 상대적으로 매우 부족 - 2009년 UCSD 데이터마이닝 대회에서 공개한 온라인 거래 데이터의 학습데이터를 살펴보면 97%가 정상적 행위이며 3%만이 비정상적 행위 - 이러한 정보 불균형은 머신러닝의 학습 성능을 감소시킬 수 있는 요소로 작용되며, 많은 연구에서는 정보의 균형을 맞추기 위해 Under Sampling[17] 등의 방법을 사용
대용량 정보의 축소	- 수집된 대량의 정보를 FDS에서 곧바로 사용하는 것은 어려운 일이며, 시스템 복잡도의 증가 가능성이 존재 - 따라서 분석/탐지를 위한 머신러닝 이전에, 정보의 질적 향상 및 양적 축소 등을 위한 과정이 수행되며, 머신러닝 기술(특징선택, 특징추출 등)이 적용 가능(상세 내용은 본문의 "FDS 구성요소" 참고)

16) Abdallah, Fraud Detection System: A survey, Journal of Network and Computer Application, 2016.4.
17) Under Sampling: 머신러닝에 사용되는 학습정보(training dataset)에서 정상/비정상 정보의 균형을 맞추고자 정상 정보의 일부를 삭제함으로써 정상 및 비정상 정보의 비율을 맞추는 것

○ 위 표와 같은 이슈들을 완화·해결함으로서 FDS의 성능이 고도화될 것으로 고려되지만 방안을 마련하는 것이 매우 어려움으로 산업계와 학계간의 지속적인 연구 협력 검토가 필요

□ 최근 머신러닝 기술 중 하나인 딥러닝이 세계적으로 확산됨에 따라 많은 금융회사에서 이에 대한 활용방안 모색

□ 하지만, 금융회사에서는 머신러닝 기술이 신기술임을 인지하고 시대 흐름에 따른 도입 보다 현 시스템과의 성능을 비교하면서 단계적인 도입 방안을 고려해보는 것이 필요

○ 또한, 전자금융거래 사기가 동일한 수법으로 여러 금융회사에 시도될 수 있는 만큼 금융 회사의 보안성 및 신뢰성 향상을 위해 **탐지된 사기 패턴, 탐지에 사용된 정보 등을 적극적으로 공유하는 것이 필요**