CZU: 343.37:336.71:004.89 **https://doi.org/10.59295/sum11(3)2024_06**

PARTICULARITĂȚILE UTILIZĂRII MACHINE LEARNING ÎN SCOPUL DETECTĂRII FRAUDEI BANCARE

Iurie CAPRIAN, Mihai GÎRLEA,
Universitatea de Stat din Moldova

Frauda rămâne o problemă clasică pentru industria bancară mondială, care are tendința generală de amplificare și modificare calitativă permanentă. De rând cu aceasta, activitatea bancară modernă este legată de folosirea unui volum tot mai mare de date legată de activitatea pieţelor financiare, a instituțiilor bancare și a clienților acestora. În aceste condiții, devine actuală implementarea unor tehnologii noi de inteligență artificială și, în mod special, a învățării automate, pentru detectarea oportună a anomaliilor existente legate de existența potențială a unei fraude. Învățarea automată este legată de constituirea sistemelor informatice capabile să învețe din date și să-și îmbunătățească performanța cu trecerea timpului. Prezentul articol prezintă esența, caracteristicile de bază și beneficiile învățării automate, precum și particularitățile aplicării în scopul combaterii fraudelor bancare.

Cuvinte-cheie: *machine learning, bancă, client, fraudă, luptă, protecţie.*

THE PARTICULARS OF USING MACHINE LEARNING TO DETECT BANKING FRAUD

Fraud remains a classic problem for the global banking industry, which has a general trend of permanent amplification and qualitative change. Along with this, modern banking is related to the use of an increasing volume of data related to the activity of financial markets, banking institutions and their customers. In these conditions, the implementation of new artificial intelligence technologies and, in particular, machine learning, for the timely detection of existing anomalies related to the potential existence of fraud, becomes relevant. Machine learning is about building computer systems capable of learning from data and improving their performance over time. This article presents the essence, basic features and benefits of machine learning, as well as the specifics of its application for the purpose of combating bank fraud.

Keywords: *machine learning, bank, customer, fraud, fighting, protection.*

Introducere

Potrivit unor experți, frauda bancară este definită ca „folosirea fraudei pentru a fura bani sau active de la o bancă, o instituție financiară sau deponenții unei bănci” [1].

Frauda bancară este o infracțiune efectuată prin folosirea unor mijloace potențial ilegale pentru a obține bani, active sau alte proprietăți deținute de o instituție bancară sau pentru a obține bani de la deponenți, pretinzându-se în mod fraudulos drept bancă sau altă instituție financiară. În multe cazuri, frauda bancară [2].

Răspândirea globală și transformarea permanentă a metodelor aplicate au făcut frauda bancară unul din pericolele importante pentru securitatea informațională, operațională și financiară a băncilor. Din acest considerent, aplicarea tehnologiilor informaționale avansate în cadrul băncilor pentru prevenirea și combaterea fraudelor bancare a devenit un imperativ al timpului.

Scopul cercetării efectuate constă în examinarea posibilităților de utilizare a tehnologiilor de învățare automată în scopul detectării fraudelor bancare.

Obiectivele cercetării au fost:

- examinarea esenței și tipologiei fraudei bancare;
- cercetarea importanței învățării automate;
- studierea posibilităților utilizării învățării automate în scopul detectării fraudelor bancare.

Cercetarea a fost realizată sub forma unei examinări a surselor bibliografice recente privind tendințele în dezvoltarea și utilizarea învățării automate în domeniul bancar la nivel mondial. Ca urmare, a fost conturat

un tablou de sinteză al conținutului domeniului dat, care a examinat esența și particularitățile tehnologice ale aplicării învățării automate în industria bancară în scopul detectării fraudelor bancare.

Metode și materiale aplicate

Studiul efectuat în scopul perfectării prezentului articol se bazează pe examinarea viziunilor și sinteza opiniilor de experți în domeniul fraudei bancare și aplicării **învățării automate în** scopul combaterii acesteia. Materialele acumulate au permis formularea unei imagini de sinteză, care este prezentată în acest articol.

Rezultate obținute și discuții

În opinia experților de la John Marshall Bank, o amploare tot mai mare au căpătat-o fraudele legate de utilizarea ilegală a informațiilor personale a altcuiva pentru a obține acces la o instituție bancară [3]:

- *Frauda cu împrumuturile*, în care informațiile personale și de cont ale clienților sunt folosite de criminali pentru a primi un împrumut pe numele acestora.
- *Preluarea de cont,* care are loc atunci când un infractor folosește contul existent al unei alte persoane pentru a face achiziții sau retrageri ilegale.
- *Frauda cu cecuri*. Un cec conține informații mai mult decât suficiente pentru un infractor, inclusiv numele, adresa, contul și numărul de rutare. Adesea, infractorul folosește substanțe chimice pentru a „spăla" informațiile dintr-un cec scris, pentru a crea cecuri contrafăcute sau pur și simplu pentru a falsifica un cec fără acordul victimei.
- *Fraudă prin transfer bancar*. Escrocii constrâng victima să trimită bani în contul lor din mai multe motive falsificate. Aceasta include o răscumpărare pentru o rudă „răpită", colectarea datoriilor, taxe de câștig la loterie, neprezentarea în instanță etc.
- *Escrocheria de tip phishing* apare atunci când un atacator, prefăcându-se ca o entitate de încredere, păcălește o victimă pentru a deschide un e-mail, un mesaj instantaneu sau un mesaj text. Destinatarul este apoi păcălit să facă clic pe un link rău intenționat, ceea ce poate duce la instalarea de malware, înghețarea sistemului ca parte a unui atac ransomware sau dezvăluirea de informații sensibile.

Experții de la Telus International au publicat unele statistici referitoare la unele categorii de fraude bancare, precum [4]:

- Valoarea tranzacțiilor frauduloase efectuate cu carduri de plată la nivel mondial în 2021 a fost estimată de Statistica la un nivel de peste 32 de miliarde USD, care ar putea crește la 38,5 miliarde USD până în 2027.
- În Raportul Crimei pe Internet din 2020, FBI a raportat că americanii au pierdut peste 54 milioane USD în escrocherii de phishing în acel an.
- Numai în 2020, pierderile financiare totale din furtul de identitate au fost de aproximativ 13 miliarde USD, conform rezultatelor Sondajului Javelin din 2021 privind frauda de identitate.

În mod separat, poate fi menționată frauda de *spălare a banilor*, care reprezintă procesul ilegal de ascundere a originilor banilor obținuți ilegal prin trecerea acestora printr-un sistem complex de transferuri bancare sau alte tranzacții [5].

Organizația Națiunilor Unite estimează că suma anuală aproximativă a spălării banilor oscilează între 800 milioane Dolari SUA și 2 trilioane Dolari SUA, din care aproximativ 90% rămân nedetectate [6].

În definiția lui James Bassey, ***machine learning (ML***) este „o tehnologie care permite computerelor să învețe fără a fi programate în mod explicit" [7].

Expertul Ed Burns prezintă următoarea definiție: „Machine learning este un tip de inteligență artificială, care permite aplicațiilor software să devină mai precise la prezicerea rezultatelor fără a fi programate în mod explicit pentru a face acest lucru. Algoritmii de învățare automată folosesc datele istorice ca intrare pentru a prezice noi valori de ieșire" [8].

Scopul principal al utilizării ML este dezvoltarea tehnologică a cunoștințelor umane.

ML are mai multe domenii de aplicare în cadrul băncilor, inclusiv: asigurarea conformării legale a activității instituției, efectuarea studiilor de piață, desfăşurarea analizelor predictive, formularea recomandărilor de produse, organizarea circuitului de documente, participarea în activitățile de fidelizare a clienților, fortificarea scorului de credit, perfecționarea activității investiționale și altele [9].

În anul 2022, experții de la Exadel au publicat unele date statistice referitoare la implementarea ML în domeniul bancar la nivel global [10]:

- 60% din toți profesioniștii angajați de companiile financiare au abilități de a crea sisteme de inteligență artificială.
- Potrivit unei prognoze formulate de Autonomous Next, până în anul 2030 băncile vor putea reduce costurile cu 22%, aplicând tehnologii de inteligență artificială, ceea ce înseamnă o economie de până la 1 trilion USD.
- În anul 2020 utilizarea tehnologiei de recunoaștere a feței urma să contribuie la o creștere a ratei anuale a veniturilor cu peste 20% și prevenirea fraudei cu cardurile de credit.
- Potrivit Insider Intelligence, în anul 2024 implementarea inteligenței artificiale și a ML în domeniul bancar va contribui la creșterea acceptării serviciilor bancare web, cât și a celor mobile în rândurile clienților din SUA, respectiv, până la 72,8% și 58,1%.
- Potrivit raportului AI în domeniul bancar al Insider Intelligence, economiile de costuri pentru bănci din aplicațiile cu inteligență artificială sunt estimate la nivel de 447 de miliarde USD până în anul 2023.

De asemenea, experții menționați indică asupra beneficiilor utilizării ML în cadrul băncilor [10]:

1. *Personalizarea ofertelor produselor bancare.* Volumul important și divers de informații despre comportamentul clienților permite băncilor să cunoască doleanțele lor în orice moment și pentru ce ei sunt dispuși să plătească.

2. *Reducerea costurilor și riscurilor operaționale*. Aplicarea ML reduce impactul factorului uman asupra activității băncilor, care poate conduce la pierderi grave. Chiar și angajații cu experiență pot lua decizii greșite, iar aplicarea ML în cadrul băncilor în operațiunile lor de rutină permite eliminarea acestui risc.

3. Îmbunătățirea deciziilor privind *creditarea clienților.* ML este capabilă să analizeze istoria de creditare, tranzacțiilor bancare și alte informații legate de clienți pentru determinarea solvabilității.

4. *Evaluarea îmbunătățită a investițiilor.* ML poate procesa cantități mari de date din alte surse în timp real și să ia în considerație preferințele privind toleranța la risc, investițiile și orizontul de timp.

5. *Verificarea conformității și detectarea fraudelor.* ML poate sprijini băncile în monitorizarea tranzacțiilor, urmărirea comportamentului clienților și înregistrarea informațiilor în sisteme suplimentare de conformitate și de reglementare, reducând riscul general. La fel, ML poate examina cantități mari de date prin aplicarea unor algoritmi diferiți și să identifice fraudele.

Experții de la Exadel afirmă: „Frauda în sectorul fintech devine o problemă comună pentru multe companii, indiferent de numărul de clienți și dimensiunea. Învățarea automată în finanțe poate evalua seturi substanțiale de date ale tranzacțiilor simultane în timp real. În același timp, ML poate minimiza aportul uman prin învățarea din rezultate și actualizarea modelelor. Cu ajutorul învățării automate, organizațiile financiare pot eticheta datele istorice ca fiind frauduloase sau nefrauduloase și pot continua să își îmbunătățească capacitatea de a detecta posibile fraude potențiale, învățând din modelele de comportament anterioare. ML poate ajuta băncile să identifice rapid activitatea utilizatorilor, să o verifice și să răspundă rapid și eficient la atacurile cibernetice” [10].

Zuzanna Pajorska indică asupra *formelor de utilizare a învățării automate* în scopul combaterii fraudei bancare [11]:

- analiza în timp real a datelor despre tranzacții;
- declanșarea automată a alertelor, dacă sunt detectate activități suspecte; sau
- blocarea tranzacțiilor suspecte.

Detectarea fraudelor prin utilizarea ML este legată de următoarele *activități* [10]:

- găsirea corelațiilor ascunse și implicite în date;
- detectarea automată a scenariilor de fraudă;
- număr redus de pași de verificare, rezultând o experiență mai bună pentru utilizator;
- prelucrarea datelor în timp real.

Utilizarea ML în scopul detectării fraudelor bancare se bazează pe următoarele [4], [9], [10], [12], [13]:

1. Învățarea automată este știința de a proiecta algoritmi care găsesc automat îmbunătățiri pe baza

experiențelor anterioare. Analizează seturi enorme de date folosind algoritmi complecși pentru a identifica modele. Acest tip de învățare profundă poate ajuta mașinile să prezică și să răspundă la situații, chiar dacă nu au fost programate în mod explicit în aceste moduri.

2. Algoritmii ML pot analiza sute de mii de tranzacții pe secundă folosind rețelele neuronale, luând decizii în timp real.

3. Tranzacțiile frauduloase arată anumite modele, care le diferențiază de cele autentice. Algoritmii ML recunosc aceste modele și sunt capabili să le diferențieze pe cele dintre fraudatori și clienții legitimi.

4. În timp ce oamenii și sistemele programate bazate pe reguli pot ignora sau trece cu vederea, fără să știe, frânturi de informații, algoritmii ML pot fi antrenați să analizeze chiar și cele mai aparent nelegate de informații pentru a găsi un model.

5. Sistemele de detectare și prevenire a fraudei bazate pe ML se bazează pe algoritmii, care pot fi antrenați cu date istorice despre exemplele anterioare de fraudă și înțeleg în mod autonom tiparele caracteristice ale acestor evenimente pentru a le recunoaște odată ce se repetă.

6. ML nu încetează niciodată să învețe și îmbunătățește abordarea de detectare a fraudelor în timp. Când sistemul admite o eroare, el învață din greșelile sale și își îmbunătățește acuratețea data viitoare.

7. ML este capabilă de detectarea anomaliilor în domeniul deservirii activelor instituțiilor bancare. Anomaliile pot apărea din cauza accidentelor, incompetenței sau erorilor de sistem în procesele de zi cu zi. Detectarea anomaliilor legate de activități ilegale precum preluarea contului, frauda, intruziunea în rețea sau spălarea banilor, care pot provoca rezultate neașteptate. Sistemele antifraudă de învățare automată pot găsi evenimente subtile și corelații în comportamentul utilizatorilor, compara multe variabile în timp real și pot procesa seturi mari de date pentru a identifica probabilitatea tranzacțiilor frauduloase.

8. ML are succes în eliminarea numărului necontrolat de tranzacții marcate, care au loc și în furnizarea unei liste concise a celor, care necesită investigații suplimentare de către un lucrător bancar împuternicit.

9. Algoritmii ML pot fi antrenați să detecteze și să analizeze tipare pe date aparent nesemnificative. Ei pot identifica modele subtile sau non-intuitive, care ar fi dificil sau poate chiar imposibil de perceput de către oameni. Acest lucru crește acuratețea detectării fraudelor, ceea ce înseamnă că vor exista mai puține fals pozitive și fraude care nu sunt detectate.

10. Algoritmii ML pot efectua sarcini repetitive și pot detecta modificări subtile ale tiparelor pe cantități mari de date. Acest lucru este esențial pentru detectarea fraudei într-un interval de timp mult mai scurt decât pot realiza oamenii. Algoritmii pot analiza sute de mii de plăți pe secundă, ceea ce reprezintă mai multă muncă decât o pot face mai mulți analiști umani în aceeași perioadă de timp. Acest lucru reduce costurile, precum și timpul necesar analizei tranzacțiilor, făcând, astfel, procesul mai eficient.

Detectarea fraudelor prin utilizarea ML este legată de următoarele activități [10]:

- găsirea corelațiilor ascunse și implicite în date;
- detectarea automată a scenariilor de fraudă;
- efectuarea unui număr redus de pași de verificare, rezultând o experiență mai bună pentru utilizator;
- prelucrarea datelor în timp real.

Realizarea programelor de prevenire a fraudei și de gestionare a riscurilor care utilizează ML începe prin colectarea și clasificarea cât mai multor date înregistrate anterior. Acestea includ informații despre tranzacțiile legitime și tranzacțiile frauduloase, adică cele care sunt etichetate drept bune (tranzacții legitime sau clienți) sau cele rele (tranzacții sau clienți frauduloase) [9].

Aceste date sunt apoi folosite pentru a „instrui" programul de ML cum să aprecieze dacă un anumit client sau tranzacție este frauduloasă sau nu. Pentru ca acest sistem de detectare a fraudei să aibă succes, este necesară dispunerea de un volum maximal de date cu modele de fraudă, astfel încât să ofere algoritmului o mulțime de exemple din care să învețe. Odată ce algoritmul de ML este antrenat, programul devine specific afacerii și poate fi considerat gata de utilizare în cadrul de management al fraudei al unei bănci [9].

În același timp, experții în domeniul abordat ne previn despre *riscul părtinirii (prejudecății)* în aplicarea tehnologiei ML. Este vorba de o eroare sistematică care apare în modelul de învățare automată în sine din cauza ipotezelor incorecte în procesul ML [14].

Astfel, Michelle Palomera afirmă: „Mașinile, ca și oamenii, pot fi părtinitoare. În sistemele AI, părtinirea apare atunci când sistemele produc rezultate care sunt prejudiciate din cauza ipotezelor neintenționate și eronate în procesul de învățare automată (ML). Pentru instituțiile financiare, algoritmii AI cu prejudecăți ar putea recompensa anumite grupuri în detrimentul altora, ducând la procese părtinitoare de creditare și de decizie care ar putea limita piața în timp și chiar ar putea schimba peisajul economiei.” [14].

Pentru a combate această problemă, băncile trebuie să investească în lucrători cu expertiza potrivită și să aplice o abordare multidisciplinară în cercetare, analiză, design de produs și dezvoltarea platformei cu utilizarea ML. Ei au nevoie de echipe și parteneri care sunt familiarizați cu părtinirile cognitive întâlnite în mod obișnuit în experiența utilizatorului, precum și cu factorii contributivi care provoacă părtinirea ML. Acestea includ procese care pot produce date lipsă, pot prezenta un potențial de comportament neașteptat sau implică parametri care influențează probabilitatea [14].

La momentul de față, universitățile pun o sarcină mai mare codării etice, care ar trebui să ajute băncile să recruteze talentul de care au nevoie. De exemplu, programul Embedded EthiCS reunește filozofi și informaticieni pentru a-i învăța pe studenți cum să ia decizii mai atent și mai etice atunci când construiesc tehnologii [14].

Concluzii

ML este o ramură specifică a inteligenței artificiale, al cărui obiectiv este de a dezvolta tehnici, care dau calculatoarelor posibilitatea de a învăța. ML a devenit un instrument modern al desfășurării unei activități bancare moderne, care este aplicat în forme diverse. Odată cu creșterea proporțiilor și diversității fraudelor bancare, ML are o importanță în creștere în detectarea acestora. Aplicarea ML în scopul combaterii fraudelor bancare are un șir de beneficii. În același timp, ML încă nu poate fi considerată drept soluție perfectă a problemelor bancare respective, fiind necesară dezvoltarea și perfecționarea continuă a acestor tehnologii.

Referinţe*:*

1. *Bank Fraud – Definitions & Penalties*. Disponibil: https://jsberrylaw.com/blog/bank-fraud-definition-penalties/. [Accesat la 09.08.2023].
2. *Bank fraud*. Disponibil: https://en.wikipedia.org/wiki/Bank_fraud. [Accesat: 09.08.2023]
3. *Common Types of Fraud*. Disponibil: https://www.johnmarshallbank.com/resources/security-center/types-of-fraud/. [Accesat la 11.08.2023].
4. *How is AI transforming fraud detection in banks?*. Disponibil: https://www.telusinternational.com/insights/trust-and-safety/article/ai-fraud-detection-in-banks. [Accesat la 11.08.2023].
5. *Money Laundering.* Disponibil: https://www.idnow.io/glossary/money-laundering/#:~:text=Money%20laundering%20is%20the%20illegal,has%20typically%20three%20main%20stages. [Accesat la 11.08.2023].
6. LAZIC, Marija. *27 Informative Money Laundering Statistics in 2022*. Disponibil: https://legaljobs.io/blog/money-laundering-statistics/. [Accesat la 11.08.2023].
7. BASSEY, James. *Ghidul complet pentru învățarea automată în domeniul bancar, al serviciilor financiare și al investițiilor*. Disponibil: https://stayinformedgroup.com/ro/machine-learning-in-banking/. [Accesat la 11.08.2023].
8. BURNS, Ed. *Machine learning*. Disponibil: https://www.ibm.com/topics/machine-learning. [Accesat la 11.08.2023].
9. *How does machine learning help with fraud detection in banks?*. Disponibil: https://www.miteksystems.com/blog/how-does-machine-learning-help-with-fraud-detection-in-banks. [Accesat la 12.08.2023].
10. *How Machine Learning is Used in Finance and Banking*. Disponibil: https://exadel.com/news/how-machine-learning-is-used-in-finance-and-banking/. [Accesat la 12.08.2023].
11. PAJORSKA, Zuzanna. *Banking Technology: Top 7 Trends for 2023*. Disponibil: https://stratoflow.com/banking-technology-trends/. [Accesat la 12.08.2023].
12. DI STEFANO, Andrea. *Machine learning for fraud detection: fighting crime with algorithms*. Disponibil: https://www.itransition.com/machine-learning/fraud-detection. [Accesat la 12.08.2023].
13. *Artificial Intelligence in Bank Fraud Detection and Prevention - SQN Banking Systems*. Disponibil: https://sqnbankingsystems.com/blog/artificial-intelligence-in-bank-fraud-detection-and-prevention/. [Accesat la 12.08.2023].

14. HARRISON, Polly Jean. *How to De-Bias Artificial Intelligence in Banking*. Disponibil: https://thefintechtimes.com/how-to-de-bias-artificial-intelligence-in-banking/. [Accesat la 12.08.2023].

Date despre autori:
Iurie CAPRIAN, doctorand, Universitatea de Stat din Moldova.
ORCID: 0000-0001-5484-3087
E-mail: iuriecaprian@gmail.com

Mihai GÎRLEA, doctor, conferențiar universitar, Universitatea de Stat din Moldova.
ORCID: 0009-0003-5395-5898

Prezentat la 24.01.2024