Detekcija prevara u kartičnom plaćanju koristeći tehnike strojnog učenja

---

1. Uvod

Industrija kartičnog plaćanja je ključni dio globalne ekonomije, omogućujući jednostavne i sigurne transakcije. Unatoč tome, kartične prevare predstavljaju značajan problem za banke, trgovce i korisnike. Prema podacima iz 2024. godine, globalni gubici zbog kartičnih prevara **premašuju 32 milijarde USD godišnje.** U Hrvatskoj, precizni podaci o gubicima nisu javno dostupni, no zna se da phishing i krađa identiteta često dominiraju među oblicima prevara.

Kartične prevare mogu se podijeliti na razne kategorije koje često evoluiraju s tehnološkim napretkom. Tradicionalni sustavi detekcije, koji se oslanjaju na pravila i heuristiku, često nisu dovoljno učinkoviti za identifikaciju složenih obrazaca prevara, što otvara prostor za primjenu tehnika strojnog učenja.

---

2. Vrste prevara u kartičnom plaćanju

Prevare u kartičnom plaćanju mogu se klasificirati u nekoliko glavnih kategorija:

- **Krađa identiteta**: Neovlašteno korištenje osobnih podataka za pristup financijskim računima.
- **Cloning/Skimming**: Kopiranje podataka s kartice pomoću neovlaštenih uređaja na bankomatima ili POS terminalima.
- **Phishing i socijalni inženjering**: Lažne poruke ili web stranice koje imitiraju legitimne institucije kako bi prikupile osjetljive informacije.
- **Account Takeover (ATO)**: Preuzimanje korisničkih računa uz pomoć ukradenih lozinki ili podataka.
- **Friendly Fraud**: Korisnici lažno prijavljuju neovlaštene transakcije kako bi ostvarili povrat sredstava.

Banke se bore protiv ovih oblika prevara kombinacijom tradicionalnih metoda i suvremenih tehnika strojnog učenja.

---

3. Razvoj tehnologije za detekciju prevara

Pristup prije strojnog učenja:

- Osnovan na pravilima i heuristici (npr. blokiranje transakcija iz određenih regija).
- Glavna ograničenja:
    - Visok broj lažno pozitivnih rezultata (legitimne transakcije označene kao prijevare).
    - Nemogućnost skaliranja za velike količine podataka.

Pristup uz strojno učenje:

- Algoritmi automatski prepoznaju složene obrasce prevara.
- Prednosti:
    - Povećana točnost i brzina.
    - Smanjenje broja lažno pozitivnih i negativnih rezultata.
    - Skalabilnost za velike količine transakcija u stvarnom vremenu.

Tablica usporedbe:

Aspekt	**Prije strojnog učenja**	**Uz strojno učenje**
Točnost	Niska	Visoka
Brzina detekcije	Spora	Brza
Prilagodljivost	Ograničena	Fleksibilna
Lažno pozitivni rezultati	Česti	Značajno smanjeni

---

4. Metode strojnog učenja u detekciji prevara

Nadzirano učenje:

- Koristi označene podatke za treniranje modela.
- Primjena: klasifikacija (npr. transakcija je "legitimna" ili "prevara").
- Algoritmi: Random Forest, XGBoost, Neuralne mreže.

Nenadzirano učenje:

- Koristi neoznačene podatke za otkrivanje anomalija.
- Primjena: detekcija neobičajenih obrazaca u podacima.
- Algoritmi: K-means, DBSCAN, PCA.

Potkripljeno učenje:

- Model uči kroz sustav nagrađivanja i kažnjavanja.
- Rijetko korišteno u detekciji prevara, ali ima potencijal za optimizaciju strategija detekcije.

---

5. Balansiranje podataka i undersampling metoda

- Prevare su rijetke u stvarnim podacima, što rezultira nebalansiranim datasetima.
- Metode balansiranja podataka:
  - **Undersampling**: Smanjenje broja instanci većinske klase.
  - **Oversampling**: Povećanje broja instanci manjinske klase (SMOTE).
- Priprema podataka:
  - Skaliranje i normalizacija podataka kako bi model bio učinkovitiji.

---

6. Detekcija anomalija

- Fokus na transakcije koje odstupaju od uobičajenog ponašanja.
- Algoritmi:
  - Isolation Forest.
  - Local Outlier Factor (LOF).
  - Autoencoders (neuronske mreže za kompresiju podataka).

---

7. Korištenje neuronskih mreža

- **Rekurentne neuronske mreže (RNN):** Analiza sekvencijalnih podataka za identifikaciju obrazaca u vremenskim serijama.
- **Konvolucijske neuronske mreže (CNN):** Primjena u prepoznavanju složenih obrazaca.
- **Primjeri iz industrije:**
  - Analiza velikih datasetova transakcija.
  - Detekcija u stvarnom vremenu.

---

8. Zaključak

Tehnike strojnog učenja značajno su poboljšale detekciju prevara u kartičnom plaćanju. Integracija suvremenih metoda poput neuronskih mreža i detekcije anomalija omogućava bankama brzu i točnu identifikaciju potencijalno sumnjivih transakcija. Budućnost ove industrije ovisi o daljnjem razvoju umjetne inteligencije i naprednih analitičkih tehnika.
