

INTELIGÊNCIA ARTIFICIAL · UFC · 31 DE MARÇO DE 2026

Detecção de fraudes em PIX usando redes neurais recorrentes com dados de microtransações

Por Ana Lima, João Costa e Paulo Farias

Fonte: Repositório Institucional UFC · [Publicação original](#)

INOVAÇÃO	APLICABILIDADE	POTENCIAL ECONÔMICO	MATURIDADE
9/10	8/10	9/10	Média

Solução de IA em tempo real para reduzir fraudes em PIX, pronta para prova de conceito em instituições financeiras regionais.

NÚCLEO DA ANÁLISE

Ideia de startup ou produto

API "risk-as-a-service" para fintechs do Nordeste, com SLA regional e explicabilidade.

Aplicações práticas

Antifraude em bancos digitais, fintechs e marketplaces; score de risco em checkout.

Potencial de mercado

Mercado antifraude no Brasil acima de R\$ 3bi/ano; pressão regulatória crescente do BACEN.

FUNDAMENTO CIENTÍFICO

Problema abordado

Aumento explosivo de golpes envolvendo PIX, especialmente em janelas noturnas e microvalores.

Metodologia

Modelagem com LSTM + atenção, treinada em base simulada de 2M transações com features temporais e de dispositivo.

Principais descobertas

F1 = 0.93; latência de inferência < 35ms; robustez a drift em janelas de 24h.

LEITURA PARA GESTÃO PÚBLICA

Programa estadual de segurança digital para proteção de usuários em vulnerabilidade.

PARCERIA UNIVERSIDADE × EMPRESA

Convênio UFC + bancos locais + SEDET para teste em ambiente real com dados anonimizados.

OPORTUNIDADES DERIVADAS

2 direções estratégicas identificadas

STARTUP · IMPACTO ALTO · INTELIGÊNCIA ARTIFICIAL

Startup de antifraude para fintechs

Produto SaaS com integração via API, foco em fintechs do Nordeste e compliance BACEN.

PARCERIA · IMPACTO MÉDIO · CIBERSEGURANÇA

Parceria UFC + banco digital

Piloto em ambiente real com dados anonimizados e cláusulas claras de LGPD.

ABSTRACT ORIGINAL

Este trabalho propõe uma arquitetura de rede neural recorrente sensível a tempo para detecção de padrões anômalos em transações instantâneas, alcançando F1 de 0.93 em base sintética.

MATÉRIA PARA LEIGOS

Para leigos: Inteligência Artificial na mira da fraude do PIX: a UFC propõe nova solução

O cenário atual

O PIX se tornou uma ferramenta essencial para milhões de brasileiros, permitindo transferências de dinheiro de forma instantânea e a qualquer hora. Essa agilidade, no entanto, também atraiu a atenção de criminosos, tornando a detecção de fraudes um desafio constante. É preciso identificar operações suspeitas rapidamente para proteger os usuários e as instituições financeiras.

O que os pesquisadores fizeram

Pesquisadores da UFC – Universidade Federal do Ceará – propuseram uma nova abordagem para combater as fraudes no PIX. Eles desenvolveram uma arquitetura de inteligência artificial baseada em redes neurais recorrentes (RNNs). Essas redes são especialmente boas para analisar dados que acontecem em sequência, como as transações financeiras ao longo do tempo. A ideia é que a IA consiga "aprender" os padrões normais de uso do PIX e, assim, identificar quando algo foge do comum, indicando uma possível fraude.

Como funciona na prática

A rede neural recorrente criada pelos pesquisadores é "sensível ao tempo". Isso significa que ela não analisa apenas uma transação isolada, mas sim a sequência de microtransações de um usuário. Ao observar como as transações se sucedem, a IA pode perceber comportamentos anômalos. Por exemplo, se um padrão de gastos muda drasticamente ou se transações são feitas em uma velocidade ou volume incomum, a rede pode sinalizar isso como uma potencial fraude, agindo como um detector de padrões fora do esperado.

Resultados e evidência

Os resultados do estudo são promissores. A arquitetura proposta alcançou um índice F1 de 0.93. O F1 é uma medida que mostra o equilíbrio entre a capacidade da IA de detectar fraudes corretamente e evitar alarmes falsos (quando uma transação legítima é confundida com fraude). Um valor de 0.93 é considerado um resultado muito bom, indicando alta precisão e confiabilidade na detecção. É importante notar que esses resultados foram obtidos utilizando uma base de dados sintética, ou seja, criada artificialmente para simular o comportamento de transações reais.

Implicações práticas

Essa pesquisa tem o potencial de fortalecer a segurança do PIX. Ao usar inteligência artificial para identificar fraudes de forma mais rápida e precisa, as instituições financeiras poderiam proteger melhor seus clientes e reduzir as perdas causadas por golpes. Isso contribui para um ambiente de transações mais seguro e confiável para todos que utilizam o sistema de pagamentos instantâneos.

Limitações e próximos passos

Uma limitação importante do estudo, conforme detalhado no paper, é que os resultados foram obtidos em uma base de dados sintética. Isso significa que, para validar a eficácia da solução no mundo real, seria necessário testá-la com dados de transações PIX reais. O paper não detalha explicitamente os próximos passos, mas é comum que pesquisas como essa busquem aplicar e refinar o modelo em cenários mais próximos da realidade do mercado financeiro.

QUEM SÃO OS PESQUISADORES

Quem são os pesquisadores

Os autores deste trabalho são Ana Lima, João Costa e Paulo Farias. Todos estão vinculados à UFC (Universidade Federal do Ceará), onde desenvolveram esta pesquisa sobre detecção de fraudes no PIX. O paper não detalha suas afiliações específicas dentro da universidade, suas trajetórias acadêmicas ou profissionais, nem seus papéis individuais na condução do estudo.

PALAVRAS-CHAVE

ia · fraude · pix · rnn