**ACM**

**QP-1. Quais características das transações financeiras são mais relevantes para a detecção de fraudes em pagamentos instantâneos via Pix?**

**QP-2. Quais algoritmos de Machine Learning apresentam melhor desempenho na detecção de fraudes de transações Pix em ambientes de Big Data?**

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | A DQN-based Internet Financial Fraud Transaction Detection Method |
| **Ano** | 2021 |
| **Veículo publicado** | In The 5th International Conference on Computer Science and Application Engineering. |
| **Autores** | Wang, Xiaoguo and Wan, Zeguo and Zhang, Yin |
| **QP1** | Propõe um método de detecção de transações fraudulentas em finanças online baseado em Deep Q Learning |
| **QP2** | Propõe e avalia um método de detecção de transações fraudulentas baseado em Deep Q Learning (DQN) |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | AI versus AI in Financial Crimes & Detection: GenAI Crime Waves to Co-Evolutionary AI |
| **Ano** | 2024 |
| **Veículo publicado** | In 5th ACM International Conference on AI in Finance |
| **Autores** | Kurshan, Eren and Mehta, Dhagash and Balch, Tucker |
| **QP1** | Discute tendências recentes de crimes financeiros impulsionados por IA e ressalta que a velocidade e o volume dos pagamentos digitais aumentaram os desafios na detecção de fraudes |
| **QP2** | Discute o uso crescente de sistemas de detecção de crimes baseados em machine learning e como os grupos criminosos rapidamente adaptaram a IA para seus propósitos. |

**SCOPUS**

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection |
| **Ano** | 2021 |
| **Veículo publicado** | Expert Systems With Applications |
| **Autores** | Li, Zhenchuan and Huang, Mian and Liu, Guanjun and Jiang, Changjun |
| **QP1** | O artigo não aborda especificamente as características de transações Pix. Ele se concentra em transações com cartão de crédito, mencionando características como tempo, valores (Amount), e outras 28 features transformadas numericamente por um método PCA para proteção de privacidade. |
| **QP2** | O artigo demonstra a eficácia do uso de algoritmos de Machine Learning na detecção de fraudes financeiras em um contexto de grandes volumes de dados (Big Data), como evidenciado pelos experimentos com o conjunto de dados privado que continha até 3,5 milhões de transações. Os experimentos foram realizados em conjuntos de dados com um alto grau de desequilíbrio de classes, simulando cenários de fraude reais onde transações legítimas são muito mais numerosas que as fraudulentas. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | A Machine Learning Method with Hybrid Feature Selection for  Improved Credit Card Fraud Detection |
| **Ano** | 2023 |
| **Veículo publicado** | Applied Sciences |
| **Autores** | Mienye, Ibomoiye Domor and Sun, Yanxia |
| **QP1** | O artigo avalia características que incluem atributos anonimizados (V1-V28), Time (tempo decorrido desde a primeira transação) e Amount (valor da transação). Isso pode ser uma relevância para identificar padrões no pix. |
| **QP2** | Ele aborda desafios como alta dimensionalidade e classes desbalanceadas, que são típicos em cenários de fraude em grandes volumes de dados (Big Data).A proposta do artigo é um método híbrido de seleção de features (IG-GAW) que visa melhorar o desempenho dos classificadores de ML, como o Extreme Learning Machine (ELM), na detecção de fraude. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | A Multi-perspective Fraud Detection Method for Multi-Participant E-commerce Transactions |
| **Ano** | 2024 |
| **Veículo publicado** | IEEE Transactions on Computational Social Systems |
| **Autores** | Yu, Wangyang and Wang, Yadi and Liu, Lu and An, Yisheng and Yuan, Bo and Panneerselvam, John |
| **QP1** | Inconsistências nos dados da transação (como valor ou recebedor), horários e dispositivos atípicos, além de desvios no comportamento do usuário. Essas características, embora analisadas em e-commerce, podem ser adaptadas para o contexto do Pix. |
| **QP2** | O uso de Machine Learning, como o SVM, mostrou-se eficaz na detecção de fraudes em e-commerce, mas o artigo não avalia diretamente sua aplicação em transações Pix ou em ambiente de Big Data. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | A Credit Card Fraud Detection Algorithm Based on SDT and Federated Learning |
| **Ano** | 2024 |
| **Veículo publicado** | IEEE Access |
| **Autores** | Tang, Yuxuan and Liu, Zhanjun |
| **QP1** | Embora focado em cartões de crédito, o artigo aponta características úteis para detectar fraudes que podem ser adaptadas ao Pix, como valor e tempo da transação, histórico do usuário e localização. Além disso, dados específicos do Pix, como chave utilizada e tipo de conta, também podem ajudar a identificar padrões suspeitos. |
| **QP2** | O uso de aprendizado profundo com Transformers e aprendizado federado mostrou alta eficácia na detecção de fraudes em cartões de crédito, mas o artigo não testa essas técnicas em transações Pix ou em ambiente de Big Data. Ainda assim, os resultados indicam potencial promissor, exigindo estudos específicos com dados do Pix. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | A rule based approach to minimize false-positive declines in Electronic Card Not Present financial transactions using feature engineering techniques |
| **Ano** | 2021 |
| **Veículo publicado** | 21st International Conference on Advances in ICT for Emerging Regions |
| **Autores** | Delgolla, Madhushika and Halloluwa, Thilina and Rathnayake, Anuradha |
| **QP1** | O artigo identifica diversas características úteis para detectar fraudes em transações CNP, como ID do usuário, valor, IP, tipo de navegador, resposta do banco, horário da transação e falhas na autenticação. Também destaca padrões suspeitos, como várias tentativas em curto tempo, transações em horários incomuns e uso do mesmo cartão por múltiplos usuários. |
| **QP2** | Algoritmos como Random Forest e XgBoost mostraram alta eficácia na detecção de fraudes CNP, especialmente quando combinados com engenharia de atributos comportamentais. O XgBoost se destacou com baixa taxa de falsos positivos. Apesar de não caracterizar explicitamente um ambiente Big Data, o volume e a complexidade dos dados analisados indicam boa aplicabilidade em contextos de grande escala. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | An Ensemble Machine Learning Model For Classification Of Credit Card Fradulent |
| **Ano** | 2023 |
| **Veículo publicado** | Journal of Theoretical and Applied Information Technology |
| **Autores** | Mathew, Tina Elizabeth |
| **QP1** | O artigo utiliza transações com 28 features transformadas por PCA, além das variáveis 'Amount' e 'Time', para detectar fraudes em cartões de crédito. Destaca-se a relevância de padrões de valor, tempo e correlação com a variável alvo (fraude). |
| **QP2** | Algoritmos de Machine Learning, especialmente modelos de ensemble como o soft voting, mostraram alta eficácia na detecção de fraudes, alcançando acurácia de até 99,92%. O uso de técnicas como SMOTE e RUS ajudou a lidar com o desbalanceamento dos dados, e algoritmos como Random Forest e XGBoost também tiveram bom desempenho, mesmo em ambiente com grande volume de dados. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Automatic Machine Learning Algorithms For Fraud Detection In Digital Payment Systems |
| **Ano** | 2020 |
| **Veículo publicado** | Journal of Theoretical and Applied Information Technology (JATIT) |
| **Autores** | Kolodiziev, O. and Mints, A. and Sidelov, P. and Pleskun, I. and Lozynska, O. |
| **QP1** | O artigo destaca características como data, hora, valor da transação, moeda, identificação do cliente e do terminal, além de informações adicionais como risco do comerciante e dados históricos do cliente. Embora o estudo não aborda o Pix diretamente, essas características podem ser adaptadas para detectar padrões suspeitos nesse sistema, considerando suas particularidades. |
| **QP2** | Algoritmos de Machine Learning, como XGBoost e LightGBM, mostraram alta eficácia na detecção de fraudes em sistemas de pagamento digital, alcançando AUCs superiores a 0.97. Mesmo sem foco específico no Pix, os resultados indicam que ML automatizado é promissor em ambientes de Big Data, com boa acurácia, interpretabilidade e menor custo de desenvolvimento. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Digital Payment Fraud Detection Methods in digital ages and Industry 4.0 |
| **Ano** | 2022 |
| **Veículo publicado** | Computers and Electrical Engineering |
| **Autores** | Chang, Victor and Doan, Le Minh Thao and Di Stefano, Alessandro and Sun, Zhili and Fortino, Giancarlo |
| **QP1** | As características que podem ser usadas para identificar fraudes no Pix incluem tempo da transação (*Time*), valor (*Amount*) e outras variáveis derivadas (via PCA). O estudo mostra que transações fraudulentas apresentam padrões distintos nessas features, o que pode ser aplicado à detecção de fraudes no Pix. |
| **QP2** | O uso de algoritmos de Machine Learning demonstrou alta eficácia na detecção de fraudes em transações digitais. Modelos como Random Forest e Regressão Logística alcançaram ótimo desempenho com técnicas como PCA e balanceamento dos dados, o que indica que essas abordagens também podem ser eficazes em transações Pix em ambiente de Big Data. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Credit Card Fraud Detection Using Machine Learning Techniques |
| **Ano** | 2022 |
| **Veículo publicado** | Future Computing and Informatics Journal |
| **Autores** | Nermin Samy, shimaa mohamed, Amira M. Idrees AMI |
| **QP1** | O artigo menciona características como tempo, valor, classe da transação e features transformadas por PCA, aplicadas a transações com cartão de crédito. Não se trata do Pix, mas algumas dessas características podem ser úteis para detectar fraudes nesse sistema. |
| **QP2** | O artigo mostra que algoritmos de ML são eficazes na detecção de fraudes em grandes volumes de transações de cartão de crédito, com bons resultados em métricas como precisão e F1-score. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Hybrid machine learning system for solving fraud detection tasks |
| **Ano** | 2020 |
| **Veículo publicado** | IEEE Third International Conference on Data Stream Mining & Processing |
| **Autores** | Vynokurova, Olena and Peleshko, Dmytro and Bondarenko, Oleksandr and Ilyasov, Vadim and Serzhantov, Vladislav and Peleshko, Marta |
| **QP1** | O artigo descreve a detecção de anomalias em transações eletrônicas com base em 41 features, incluindo IDs de usuário/dispositivo, geolocalização, tipo de conexão e histórico de transações. Embora não trate do Pix, essas características podem ser úteis para identificar padrões suspeitos nesse sistema. |
| **QP2** | O uso de Machine Learning demonstrou alta eficácia na detecção de anomalias em transações eletrônicas em tempo real. O sistema híbrido com Isolation Forest e Random Forest alcançou até 96% de precisão. Apesar de não mencionar o Pix, os resultados indicam que ML pode ser eficaz em cenários com grande volume de dados, como o Pix. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Enhancing Trust and Safety in Digital Payments: An LLM-Powered Approach |
| **Ano** | 2024 |
| **Veículo publicado** | Plataforma **arXiv** |
| **Autores** | Dahiphale, Devendra and Madiraju, Naveen and Lin, Justin and Karve, Rutvik and Agrawal, Monu and Modwal, Anant and Balakrishnan, Ramanan and Shah, Shanay and Kaushal, Govind and Mandawat, Priya and Hariramani, Prakash and Merchant, Arif |
| **QP1** | O artigo identifica características como valor, tipo e texto da transação, histórico de usuários e relatórios de spam, aplicadas a UPI/GPay. Apesar da semelhança com o Pix, não trata diretamente desse sistema. |
| **QP2** | O uso de LLMs mostrou eficácia na detecção de fraudes em UPI/GPay, com alta acurácia (93,33%) em grandes volumes de dados (até 4 milhões de transações). O estudo não aborda o Pix, mas sugere potencial similar nesse contexto. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Evaluating the Computational Advantages of the Variational Quantum Circuit Model in Financial Fraud Detection |
| **Ano** | 2024 |
| **Veículo publicado** | Revista IEEE Access |
| **Autores** | Tudisco, Antonio and Volpe, Deborah and Ranieri, Giacomo and Curato, Gianbiagio and Ricossa, Davide and Graziano, Mariagrazia and Corbelletto, Davide |
| **QP1** | O artigo usa dados da Intesa Sanpaolo e menciona features como timestamp, valor, data e variáveis categóricas, com análise via PCA. Não trata do Pix, mas mostra quais tipos de características podem ser úteis. |
| **QP2** | Mostra eficácia de algoritmos clássicos e quânticos em detectar fraudes em grandes volumes de dados financeiros. Embora relevante ao contexto do Pix, os testes foram com dados da Intesa Sanpaolo, não Pix. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Financial Crime Fraud Detection Using Graph Computing: Application Considerations Outlook |
| **Ano** | 2020 |
| **Veículo publicado** | Segunda Conferência Internacional sobre Inteligência Artificial Transdisciplinar (TransAI 2020), organizada pelo IEEE. |
| **Autores** | Kurshan, Eren and Shen, Hongda and Yu, Haojie |
| **QP1** | O artigo não trata do Pix, mas discute características relevantes para detectar fraudes em pagamentos P2P, como tipo, valor e tempo da transação, dispositivos, canais, histórico entre as partes, perfis de risco e padrões em grafos. Aponta o uso de ML com análise de grafos como eficaz para sistemas como o Pix. |
| **QP2** | O artigo não avalia ML no Pix, mas mostra eficácia de algoritmos baseados em grafos (como GNNs) em ambientes com grandes volumes de dados financeiros. Aponta desafios reais (tempo real, dados ruidosos, ataques) que afetam a eficácia prática. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Graph Computing for Financial Crime and Fraud Detection: Trends, Challenges and Outlook |
| **Ano** | 2020 |
| **Veículo publicado** | **International Journal of Semantic Computing**, volume 14, número 4 |
| **Autores** | Kurshan, Eren and Shen, Hongda |
| **QP1** | Embora não mencione o Pix, o artigo descreve características relevantes para detectar fraudes em sistemas de pagamento P2P e digitais, como tipo e valor da transação, conectividade entre entidades, padrões comportamentais e uso de grafos. Essas características são aplicáveis ao contexto do Pix. |
| **QP2** | O artigo não trata do Pix diretamente, mas demonstra que ML, especialmente com grafos, é eficaz na detecção de fraudes em sistemas financeiros de grande escala. Aponta vantagens técnicas e desafios práticos, o que é relevante para o ambiente de Big Data do Pix. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Impact of Deep Feature Synthesis on Deep Learning in Electronic Transaction Fraud Detection |
| **Ano** | 2023 |
| **Veículo publicado** | IEEE 3rd International Conference on Software Engineering and Artificial Intelligence (SEAI) |
| **Autores** | Uddin, Mohammed Najim and Azad, Salahuddin and Hossain, Md Rahat and Chugh, Ritesh |
| **QP1** | O artigo, embora não cite o Pix, utiliza dados transacionais semelhantes (cartão de crédito) e aborda técnicas relevantes como engenharia de atributos (DFS) para enriquecer as características da transação. Isso permite identificar padrões suspeitos com base em atributos derivados, como relações entre entidades, frequência de uso e valores. Essas características são aplicáveis ao contexto de transações Pix. |
| **QP2** | O artigo demonstra que o uso de Deep Learning (CNN), combinado com engenharia de atributos (DFS), melhora significativamente o desempenho da detecção de fraudes. Trabalha com grandes volumes de dados e aborda desafios como desbalanceamento de classes, o que reforça a aplicabilidade e eficácia de ML em ambientes similares ao Pix, mesmo sem citar diretamente Big Data ou Pix. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Leveraging ensemble learning for enhanced security in credit card transaction fraudulent within smart cities for cybersecurity challenges |
| **Ano** | 2024 |
| **Veículo publicado** | Journal of Discrete Mathematical Sciences & Cryptography |
| **Autores** | Padhi, Bharat Kumar and Chakravarty, Sujata and Naik, Bighnaraj and Nayak, Soumya Ranjan and Poonia, Ramesh Chandra |
| **QP1** | O artigo trata de características comuns em fraudes, como o desbalanceamento das classes, variação nos padrões e atributos transacionais (valor, frequência, etc.), que são relevantes para detectar anomalias. Embora não cite o Pix, essas propriedades são diretamente aplicáveis a sistemas de pagamento digital como o Pix. |
| **QP2** | O artigo propõe e valida um modelo híbrido (SMOTE-LightGBM) eficaz em grandes volumes de dados desbalanceados, com alto desempenho (recall 0.889, AUC 0.990). Isso demonstra a aplicabilidade e eficácia de ML em cenários similares ao do Pix, mesmo com desafios típicos de Big Data e fraude dinâmica. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Optimizing fraud detection in financial transactions with machine learning and imbalance mitigation |
| **Ano** | 2025 |
| **Veículo publicado** | **Expert Systems**, da editora Wiley |
| **Autores** | Al-dahasi, Ezaz Mohammed and Alsheikh, Rama Khaled and Khan, Fakhri Alam and Jeon, Gwanggil |
| **QP1** | O artigo identifica atributos-chave como “transaction amount”, “transaction type” e “account balances” como relevantes para detecção de fraude, utilizando técnicas de interpretabilidade (SHAP) para destacar a importância de cada feature. Essas características são compatíveis com os dados transacionais do Pix. |
| **QP2** | O estudo aplica ML em um dataset com mais de 1 milhão de registros, altamente desbalanceado, e demonstra que modelos como XGBoost e Random Forest atingem alto desempenho (F1-score 0.99). O uso de técnicas como undersampling, validação cruzada e explicabilidade com SHAP reforça sua eficácia em cenários complexos como o do Pix. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Advancements in Credit Card Fraud Detection: A Comprehensive Evaluation of Current Approaches |
| **Ano** | 2024 |
| **Veículo publicado** | Advances in Science and Engineering Technology (ASET) |
| **Autores** | Panthakkan, Alavikunhu and Prajapati, Dharmistha and Chaubey, Nirbhay and Joshi, Ritesh and Mansoor, Wathiq and Al-Ahmad, Hussain |
| **QP1** | O artigo aborda diferentes tipos de fraudes (como phishing, skimming, transações card-not-present) e usa dados históricos de transações para treinar modelos de ML, reforçando a importância de atributos transacionais para distinguir fraudes — uma abordagem aplicável ao contexto do Pix. |
| **QP2** | O estudo testa diversos algoritmos supervisionados de ML (DT, KNN, SVM, RF, XGBoost, ANN) em um dataset desbalanceado com mais de 283 mil transações. Demonstra conhecimento dos desafios típicos de ambientes de Big Data e fraudes, como desbalanceamento severo (0,17% de fraudes) e apresenta métricas relevantes (F1-score, Cohen’s Kappa), validando a eficácia dos modelos. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Cost-Sensitive Model Evaluation Approach for Financial Fraud Detection System |
| **Ano** | 2021 |
| **Veículo publicado** | **Second International Conference on Electronics and Sustainable Communication Systems (ICESC 2021)**, organizada pelo IEEE |
| **Autores** | Pant, Pooja and Srivastava, Prakash |
| **QP1** | O artigo discute o ciclo completo de uma transação financeira e os mecanismos de detecção de fraude (FDS), apresentando atributos relevantes e técnicas de redução e seleção de atributos (como forward/backward selection, embedded/wrapper methods), o que é diretamente aplicável à identificação de padrões suspeitos em transações Pix. |
| **QP2** | O estudo apresenta uma análise de múltiplos algoritmos de ML (como DT, ANN, Logistic Models, Ensemble Learner) e discute explicitamente os desafios de aplicar essas técnicas em grandes volumes de dados desbalanceados. Também enfatiza a importância de avaliação custo-sensível e técnicas como SMOTE, reforçando a relevância e eficácia dessas abordagens para ambientes como o Pix. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Detection of Fraudulent Activities in Unified Payments Interface using Machine Learning - LSTM Networks |
| **Ano** | 2024 |
| **Veículo publicado** | International Conference on Communication, Power and Computing Technologies (ICCPCT), organizada pelo IEEE. |
| **Autores** | Raju, M. Naga and Chandrasena Reddy, Yarramreddy and Babu, Polavarapu Nagendra and Pavan Ravipati, Venkata Sai and Chaitanya, Velpula |
| **QP1** | O artigo detalha o pré-processamento de dados e a engenharia de atributos relevantes como valor da transação, frequência, timestamp e tipo de comerciante, além da utilização de dados reais e sintéticos (via GANs). Esses atributos são fundamentais para identificar padrões anômalos em transações financeiras e se alinham diretamente ao contexto do Pix. |
| **QP2** | O artigo detalha o pré-processamento de dados e a engenharia de atributos relevantes como valor da transação, frequência, timestamp e tipo de comerciante, além da utilização de dados reais e sintéticos (via GANs). Esses atributos são fundamentais para identificar padrões anômalos em transações financeiras e se alinham diretamente ao contexto do Pix. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Ensemble Approach for Credit Card Fraud Detection Using Champion-Challenger Analysis |
| **Ano** | 2022 |
| **Veículo publicado** | **International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)**. |
| **Autores** | Muhal, Harshit and Khatri, Gaurav and Dhama, Gaurav Kumar and Bansal, Deepika |
| **QP1** | Embora o artigo não detalhe explicitamente os atributos transacionais utilizados (devido ao uso de PCA para anonimização dos dados), ele explora a combinação de múltiplos algoritmos que analisam características temporais, comportamentais e estatísticas extraídas dos dados. A arquitetura de modelos como LSTM e CNN presume a existência de padrões sequenciais e espaciais nos dados, indicando que atributos como valor, tempo, frequência e padrões de uso foram considerados de forma implícita. Isso fornece base suficiente para inferência de padrões aplicáveis ao Pix. |
| **QP2** | O artigo demonstra, por meio de um framework de ensemble Champion-Challenger, que a combinação de modelos de ML e DL, especialmente LSTM, Random Forest e Adaboost, atinge altíssimos níveis de acurácia, precisão e recall na detecção de fraudes. Apesar do dataset não ser de escala bilionária, o uso de técnicas robustas para lidar com desbalanceamento (como SMOTE) e o desempenho elevado indicam forte aplicabilidade em ambientes de grande volume de dados, como o Pix. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Fraud Detection on Bank Payments Using Machine Learning |
| **Ano** | 2022 |
| **Veículo publicado** | International Conference for Advancement in Technology (ICONAT) |
| **Autores** | Ranjan, Pinku and Santhosh, Kammari and Kumar, Arun and Kumar, Somesh |
| **QP1** | O artigo não fornece uma descrição aprofundada das features utilizadas, mas menciona o uso de variáveis categóricas transformadas em numéricas, remoção de variáveis irrelevantes e uso de técnicas de pré-processamento que implicam na análise de atributos transacionais. Isso indica que o modelo considerou variáveis relacionadas ao comportamento da transação, mesmo que de forma genérica. Isso contribui para a compreensão das características úteis na detecção de fraude, ainda que sem o detalhamento técnico de atributos como tempo, frequência ou valor. |
| **QP2** | Apesar de o dataset utilizado (Banksim) ser de menor escala e sintético, o artigo demonstra que algoritmos clássicos de Machine Learning, como Random Forest, podem atingir altos níveis de acurácia (96.64%) na detecção de fraudes. Além disso, o estudo discute explicitamente o impacto do desbalanceamento de classes e a escolha de técnicas apropriadas (undersampling). Esses elementos tornam o estudo relevante como evidência da eficácia do ML em contextos similares ao Pix, mesmo não sendo ambientado em Big Data. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Monitoring and detection of NEFT fraudulent requests: A comparative analysis of machine learning models |
| **Ano** | 2024 |
| **Veículo publicado** | 15th International Conference on Computing and Communication Networks (ICCCNT 2024) |
| **Autores** | Bhowmik, Somnath and Howlader, Jaydeep |
| **QP1** | O artigo identifica explicitamente diversas **features relevantes** para detecção de fraude, como SenderAccountType, BeneficiaryAccountNumber, Amount, SenderAccountNumber, BeneficiaryIFSC, além de padrões como **grandes valores de transações**, **alta frequência de transações** e **inconsistência entre datas**. Essas características comportamentais são diretamente aplicáveis ao contexto do Pix, que compartilha a mesma natureza de transações digitais em tempo real. Portanto, o artigo contribui significativamente para a identificação de padrões suspeitos. |
| **QP2** | Embora o volume de dados utilizado seja relativamente pequeno, o estudo simula **diferentes cenários de desbalanceamento** e compara a eficácia de **cinco algoritmos de ML** em métricas relevantes como Precision, Recall e AUC. A Decision Tree apresentou desempenho superior em todos os cenários. Essa comparação oferece evidência empírica da eficácia de ML na detecção de fraude em pagamentos digitais, o que é aplicável ao Pix. A menção ao uso futuro de Big Data reforça o alinhamento com o ambiente proposto. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Optimizing Logistic Regression for Flawless Fraud Detection in Digital Payments |
| **Ano** | 2024 |
| **Veículo publicado** | Second International Conference on Intelligent Cyber Physical Systems (ICICPS) |
| **Autores** | Kant, Vishnu |
| **QP1** | O artigo destaca características como ID da transação, timestamp, valor, contas de cliente/comerciante, e localização, que são úteis na detecção de fraudes e aplicáveis ao Pix, especialmente ao analisar padrões de tempo, frequência e localização. |
| **QP2** | A Regressão Logística (LR) mostrou boa performance com 99.9% de acurácia em transações não fraudulentas, mas com recall de 0.67% para fraudes, sugerindo que, embora eficaz, ajustes são necessários para lidar com falsos negativos. A LR é promissora em ambientes de Big Data, com bons resultados no volume de transações. |

**Wiley**

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Artificial Intelligence Applications in the Indian Financial Ecosystem |
| **Ano** | 2024 |
| **Veículo publicado** | Scrivener Publishing LLC |
| **Autores** | Manda, Vijaya Kittu and Nihar, Khaliq Lubza |
| **QP1** | O artigo apresenta como algoritmos de IA podem identificar fluxos anormais de fundos e detectar atividades financeiras incomuns, o que é aplicável ao Pix. Embora não trate especificamente de atributos da transação, o foco em anomalias e padrões comportamentais é relevante para o contexto. |
| **QP2** | O artigo aborda o uso de IA para analisar grandes volumes de dados financeiros, detectar padrões e anomalias e identificar atividades suspeitas, o que é relevante para a detecção de fraude em ambientes como o Pix. Apesar de não trazer métricas específicas, apresenta fundamentos aplicáveis ao contexto investigado. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Big Data, AI and Machine Learning |
| **Ano** | 2020 |
| **Veículo publicado** | Scrivener Publishing LLC |
| **Autores** | Dubovi, Omri |
| **QP1** | O artigo descreve múltiplas características usadas em transações online, como localização, ID do dispositivo, valor gasto e impressões digitais móveis. Essas informações ajudam tanto em sistemas baseados em regras quanto em IA/ML a identificar comportamentos anômalos aplicável à detecção de fraudes no Pix. |
| **QP2** | O artigo destaca que sistemas de IA/ML em pagamentos online analisam grandes volumes de dados transacionais, identificando padrões e anomalias em tempo real. Isso é aplicável ao contexto do Pix, onde o uso de IA pode ajudar a reconhecer fraudes com rapidez e precisão. A ênfase na importância de dados de alta qualidade também reforça a relevância do pré-processamento e da curadoria de dados no combate a fraudes. |

| **Campo** | **Informação a ser preenchida** |
| --- | --- |
| **Título da publicação** | Financial Fraud Detection Approach Based on Firefly Optimization Algorithm and Support Vector Machine |
| **Ano** | 2022 |
| **Veículo publicado** | Applied Computational Intelligence and Soft Computing |
| **Autores** | Singh, Ajeet and Jain, Anurag and Biable, Seblewongel Esseynew |
| **QP1** | O estudo usa atributos como ID do cartão, data, destinatário e valor da transação. Também destaca a importância da seleção de características (Feature Selection) para melhorar a detecção de fraudes em conjuntos de dados grandes e desbalanceados, algo altamente relevante para o contexto do Pix. |
| **QP2** | O estudo apresenta um modelo híbrido (FFSVM) que utiliza seleção de características (CFS) para lidar com dados de alta dimensionalidade. Embora o foco seja em cartões de crédito, a estratégia de selecionar atributos relevantes para detecção de fraudes é diretamente aplicável ao Pix. |