Contemporânea
Contemporary Journal
Vol. 4 N°. 11: p. 01-20, 2024
ISSN: 2447-0961

Artigo

IDEALIZAÇÃO DE MONITOR DE FRAUDES BANCÁRIAS A PARTIR DA INTELIGÊNCIA ARTIFICIAL GENERATIVA

DESIGNATION OF A BANK FRAUD MONITOR USING GENERATIVE ARTIFICIAL INTELLIGENCE

DESIGNACIÓN DE UN MONITOR DE FRAUDE BANCARIO MEDIANTE INTELIGENCIA ARTIFICIAL GENERATIVA

DOI: 10.56083/RCV4N11-169
Receipt of originals: 10/25/2024
Acceptance for publication: 11/15/2024

Leonardo do Carmo Venturini
Graduando em Engenharia da Computação
Instituição: Universidade São Judas Tadeu (USJT)
Endereço: Osasco, São Paulo, Brasil
E-mail: venturini1997@gmail.com

Otávio Brandão da Silva
Graduando em Engenharia da Computação
Instituição: Universidade São Judas Tadeu
Endereço: Osasco, São Paulo, Brasil
E-mail: otaviobrandao11@gmail.com

Thiago Necolau de Oliveira
Graduando em Engenharia da Computação
Instituição: Universidade São Judas Tadeu
Endereço: Osasco, São Paulo, Brasil
E-mail: thiagonecola@gmail.com

Roberto Marcos Kalili
Graduado em Engenharia Civil
Instituição: Universidade Presbiteriana Mackenzie
Endereço: São Paulo, São Paulo, Brasil
E-mail: roberto.kalili@saojudas.br

RESUMO: É notável o quanto as evoluções tecnológicas estão presentes no nosso dia-a-dia, nas mais diversas áreas de atuação da sociedade, como por exemplo nas áreas da saúde, bancária e comercial, porém como tudo,

existem seus prós e contras. Um dos contras dessa evolução, são como criminosos utilizam esses mesmos artifícios para realização de engenharia social e/ou phishing com o intuito de cometer fraudes bancarias. Através de pesquisas/estudos conseguimos visualizar a quantidade de pessoas que são afetadas por fraudes em geral. Com demonstração dos institutos do meio bancário, entendemos o quão é necessário o avanço das tecnologias para que essas situações sejam amenizadas. Utilizando de ferramentas tecnológicas disponíveis no mercado, conceitos e funcionalidades da Inteligência Artificial Generativa, padrões de dados, geolocalização, entendendo sobre a maneira que os órgãos reguladores atuam no meio bancário, o artigo tende a idealizar uma ferramenta de monitoramento para mitigar fraudes e garantir que ambientes bancários sejam mais seguros.

PALAVRAS-CHAVE: inteligência artificial, inteligência artificial generativa, fraudes, tecnologia, geolocalização.

ABSTRACT: It is remarkable how much technological developments are present in our daily lives, in the most diverse areas of activity in society, such as in the areas of health, banking and commerce, but like everything, there are their pros and cons. One of the drawbacks of this evolution is how criminals use these same devices to carry out social engineering and/or phishing with the aim of committing bank fraud. Through research/studies we were able to visualize the number of people who are affected by fraud in general. With demonstrations from banking institutes, we understand how necessary the advancement of technologies is for these situations to be alleviated. Using technological tools available on the market, concepts and functionalities of Generative Artificial Intelligence, data standards, geolocation, understanding the way regulatory bodies act in the banking environment, the article tends to devise a monitoring tool to mitigate fraud and ensure that banking environments are safer.

KEYWORDS: artificial intelligence, generative artificial intelligence, fraud, technology, geolocation.

RESUMEN: Es notable la presencia de los avances tecnológicos en nuestra vida cotidiana, en los más diversos ámbitos de actividad de la sociedad, como en las áreas de la salud, la banca y el comercio, pero como todo, tienen sus pros y sus contras. Uno de los inconvenientes de esta evolución es cómo los delincuentes utilizan estos mismos dispositivos para realizar ingeniería social y/o phishing con el objetivo de cometer fraude bancario. A través de investigaciones/estudios pudimos visualizar la cantidad de personas afectadas por el fraude en general. Con manifestaciones de institutos bancarios entendemos lo necesario que es el avance de las tecnologías para paliar estas situaciones. Utilizando herramientas tecnológicas disponibles en

el mercado, conceptos y funcionalidades de Inteligencia Artificial Generativa, estándares de datos, geolocalización, entendiendo la forma en que actúan los organismos reguladores en el entorno bancario, el artículo tiende a idear una herramienta de seguimiento para mitigar el fraude y garantizar que los entornos bancarios sean más seguros.

PALABRAS CLAVE: inteligencia artificial, inteligencia artificial generativo, fraude, tecnologia, geolocalización.

1. Introdução

Nos tempos atuais, sabe-se o quanto a tecnologia vem evoluindo em diversas áreas de atuação da sociedade e como tudo que é novo, pode ser utilizado para aplicações benéficas, segundo Del Claro(2009), onde na Era Digital trouxe mudanças nas áreas econômicas e sociais da nossa sociedade, como por exemplo o uso de um cartão para realizar movimentações bancárias ou o uso de dispositivos eletrônicos para a comunicação, como da mesma forma também pode ser utilizada para aplicações nocivas, segundo Klettenberg(2016), como o uso da Engenharia Social para receber informações sigilosas bancárias.

Conforme Instituto de Pesquisa DataSenado (2024), em uma pesquisa realizada com 21.808 pessoas, cerca de 24% já perderam dinheiro por algum crime digital como clonagem de cartão, fraude na internet ou invasão de contas bancárias, o que demonstra à necessidade de medidas mais eficazes no combate a esse tipo de prática.

Tabela 1 – "Nos últimos 12 meses, você perdeu dinheiro por algum crime digital como clonagem de cartão, fraude na internet ou invasão de contas bancárias?" – Brasil – 2024

Respostas	Estimativa	Margem de erro	Amostra Observada	Amostra Ponderada	População Estimada
Sim	24%	±1,4%	5.641	5.338	41.570.297
Não	75%	±1,4%	16.116	16.417	127.852.535
Não sei/prefiro não responder	0%	±0,1%	51	54	417.352
Total	100%	-	21.808	21.809	169.840.184

Fonte: Instituto de pesquisa DataSenado – coleta de 5 a 28.6.2024

Com o contexto atual, o intuito é entender como utilizar novas tecnologias para o monitoramento de fraudes, detalhando sobre cada etapa de sua idealização.

2. Referencial Teórico

Estamos vivendo o ápice da evolução tecnológica no mundo atual, onde em muitos aspectos, diversas coisas que demoravam semanas, meses e anos são feitas em poucos instantes. Conforme DEL CLARO(2009), a Era Digital a partir de 1980 proporcionou grandes avanços para a produtividade para a sociedade como um todo, influenciando diretamente no mundo econômico e como consequência auxiliando em facilidades para a população, como na saúde, com aparelhos mais precisos e eficientes para diagnósticos e tratamentos; no comercio, com o avanço da internet e atividades econômicas, possibilitando transações virtuais, pagamento online, comercio eletrônico sendo muitos mais acessíveis para os demais.

Mas da mesma forma que apresenta diversas características positivas, pessoas com má índole utilizam esses mesmos artifícios dos avanços tecnológicos, com o intuito de aplicar golpes e enganar pessoas, para obter vantagens. Como por exemplo, os desafios como a engenharia social, conforme dito por KLETTENBERG (2016), utilizar da boa-fé, desconhecimento da vítima e sensação de segurança, para conseguir informações confidenciais e realizar fraudes; a prática de "Phishing", citado

por REZENDE (2010) a prática de "pescar senhas", ou seja, a partir de e-mails, SMS, ou sites fraudulentos se passando pela instituição bancária. conseguir dados sigilosos das vítimas, utilizando a falta de conhecimento, além de possíveis vulnerabilidades que o próprio serviço bancário está exposto, conclui REZENDE (2010).

Para combater atitudes citadas, é necessário utilizar todos os artifícios que estão ao nosso alcance no momento, entre elas a Inteligência Artificial.

2.1 Inteligência Artificial

Conforme GOMES (2010) a Inteligência Artificial desde do início de seu surgimento, tem como base 4 linhas de pensamentos: Sistemas que pensam como Seres Humanos, Sistemas que atuam como Seres Humanos, Sistemas que pensam racionalmente e Sistema que atuam racionalmente. A partir desses pontos entendemos a maneira se inicia as discussões sobre o assunto.

Mas não existe ao certo uma definição concreta do que seria Inteligência Artificial, mas de forma breve trata-se de sistemas computacionais que resolvem problemas, diz SICHMAN (2021). Utilizando de base o conceito teórico do Machine Learning, a Inteligência Artificial aprende a partir de entrada de dados e com o contato com mais cenários e situações diversas, ela tende a melhorar ao longo do tempo, conforme SPADINI (2023). Sendo mais especifico a Inteligência se baseia em algoritmos de Machine Learning supervisionada, que tem como objetivo criar um modelo que realize uma conexão entre os dados de entrada e sua saída, diz SPADINI (2023).

Claramente por ser algo sistêmico, a agilidade do processamento é muito maior do que a de um humano em si. Como por exemplo, um artigo de 100 páginas, onde um humano irá ler isso por volta de 6 horas, uma inteligência artificial irá realizar isso em segundos, demonstrando um resumo pronto e até mesmo possíveis questões e discussões sobre o documento. No

entanto, conforme reforça SICHMAN (2021), dependendo do tipo de problema ela não terá uma única solução para determinado assunto, sendo necessário a determinação para que a IA consiga realizar decisões ou a melhor escolha que ela possa seguir em cenários específicos, chegando ao tópico da Inteligência Artificial Generativa.

2.2 Modelo de Linguagem

Mas antes de seguir para o tópico de inteligência artificial generativa, é necessário o entendimento de modelo de linguagem. CARLEN (2023) informa que o modelo de linguagem se trata de entender qual a melhor sequência lógica se encaixa em determinado conceito. Como por exemplo "Roberto comeu um...", utilizando um modelo bem treinado, ele pode prever a próxima palavra como "Roberto comeu um hamburguer". Utilizando o mesmo modelo, porém com um treinamento insuficiente, ele iria prever o Hamburguer como "Pão com carne". Reforçando com base nos conhecimentos compartilhados por CARLEN (2023), conforme a quantidade de conteúdo que é consumido, a compreensão do que virá a seguir nas frases será facilitada, a partir de insights gerados pela IA.

2.3 Inteligência Artificial Generativo

Com os conceitos de Inteligência Artificial e Modelo de Linguagem claros, a Inteligência Artificial Generativa entra como um subproduto desses dois tópicos. Ela tem o poder de criar, gerar novas informações a partir de conceitos já ensinados, utilizando o raciocino da IA e soar natural utilizando o modelo de linguagem diz CARLEN (2023). Então, o céu é o limite para a aplicação desse modelo, sendo possível determinar que realize tarefas mais simples como classificação e geração de imagens até tarefas mais complexas, conclui CARLEN (2023). Entre os demais tipos de tarefas

complexas, um monitor de fraudes.

2.4 Fraude e Orgãos Reguladores

Mas o que é fraude? "[...] artigo 171 do Código Penal consiste basicamente na prática de golpes, nos quais o criminoso enganar a vítima para obter algum tipo de vantagem, na maioria das vezes em dinheiro" (ACS, 2021, p.1). Entendendo esse conceito e reutilizando conceitos citados de KLETTENBERG (2016) e REZENDE (2010), os avanços tecnológicos contribuem para que cada vez mais aumente esses tipos de crimes nos meios digitais. Nada mais justo do que utilizar os avanços tecnológicos, especificamente a inteligência artificial generativa, para produzir uma ferramenta para que esse tipo de situação seja mitigado. Mas quais métodos pode-se utilizar para constituir um monitor de fraude?

Um dos métodos seria a geolocalização. Ela surge como uma solução eficaz, pois conforme CVM (Comissão de Valores Mobiliários), para auditoria, os institutos bancários devem armazenar dados dos clientes por 5 anos, entre eles registro de login e IP de clientes.

No Brasil existem alguns órgãos reguladores que atuam ativamente no combate à fraude. Conforme (GOV.BR,2022a), o Coaf (Conselho de Controle de Atividades Financeiras) exige que instituições financeiras enviem relatórios de operações suspeitas, incluindo transações de alto valor, transações internacionais, uso de paraísos fiscais e dificuldades na identificação de beneficiários finais. Em casos de irregularidades ou suspeitas, as instituições devem reportar as transações ao Coaf em um prazo de até 24 horas.

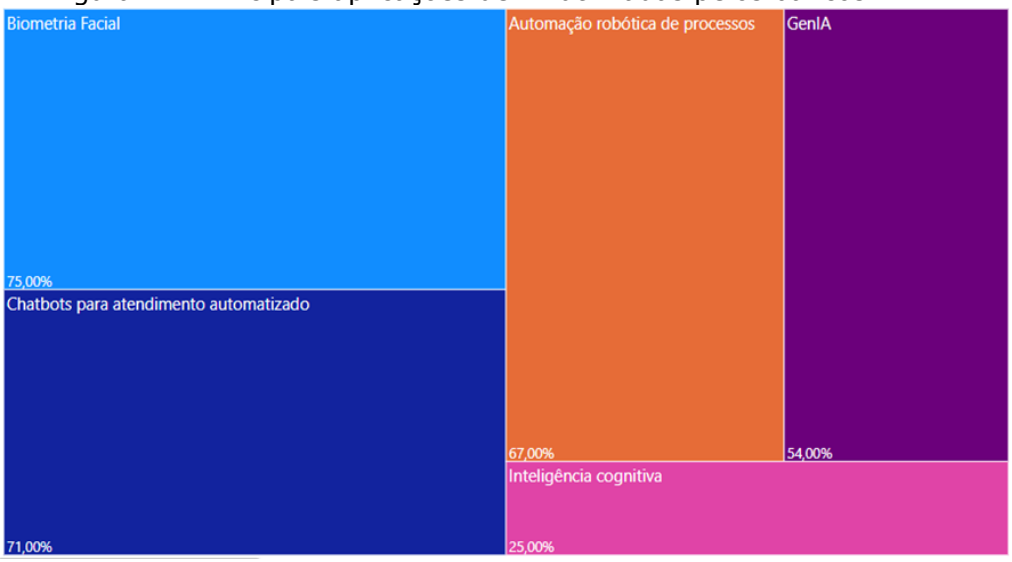
Em 2021, foi realizada a primeira ANR (Avaliação Nacional de Risco do Brasil), com o objetivo de identificar as principais ameaças e vulnerabilidades do sistema financeiro em setores estratégicos. A ANR (2022) analisa mais de 60 tipos de riscos, considerando, por exemplo, a abrangência geográfica.

Essas avaliações permitem o aprimoramento de políticas de prevenção a fraudes financeiras (GOV.BR, 2022b).

O BCB (Banco Central do Brasil) é um dos principais reguladores de práticas de monitoramento e exige que bancos e instituições financeiras implementem sistemas para a detecção de transações incomuns (BANCO CENTRAL DO BRASIL, 2024).

Conforme RODRIGUES (2024), apesar das normas preventivas utilizadas pelo Banco Central do Brasil, ainda é necessário o uso de novas tecnologias para evitar possíveis fraudes. Para isso, os bancos estão cada vez mais adotando a inteligência artificial (IA), uma ferramenta crucial para identificar possíveis fraudes. De acordo com a pesquisa FEBRABAN (2024), as principais aplicações de IA utilizadas pelos bancos incluem biometria facial (75%), chatbots para atendimento automatizado (71%), automação robótica de processos (67%), inteligência artificial generativa (GenIA) (54%) e inteligência cognitiva (25%), conforme Figura 1. Essas tecnologias permitem a análise de padrões de comportamento e transações em tempo real, aumentando a eficiência na identificação de possíveis atividades fraudulentas.

Figura 1 – Principais aplicações de IA utilizadas pelos bancos



Fonte: Febraban (2024)

Segundo dados da CNDL (Confederação Nacional de Dirigentes Lojistas) e do SPC (Serviço de Proteção ao Crédito) Brasil, 20% dos entrevistados já sofreram algum tipo de fraude financeira nos últimos 12 meses, o que representa 7,2 milhões de consumidores. O principal tipo de golpe foi a clonagem de cartões de crédito e/ou débito (6%), seguido pela compra de produtos em anúncios falsos em redes sociais (4%), transações financeiras na conta bancária sem autorização (3%), emissão de cartões de crédito sem autorização usando documentos falsos, perdidos ou roubados (3%) e empréstimos feitos em nome de outras pessoas sem autorização (3%), conclui CNDL BRASIL(2024).

De acordo com FEBRABAN TECH (2022), no Brasil, os principais bancos, como Bradesco, Itaú, Banco do Brasil e Santander, utilizam IA para identificar e prevenir fraudes de maneira cada vez mais precisa e eficiente. Essa tecnologia desempenha um papel fundamental no combate a atividades fraudulentas, permitindo que as instituições detectem padrões incomuns de comportamento que indicam possíveis ameaças.

2.5 Geolocalização

Voltando ao tópico de geolocalização, o que seria um IP? Mais conhecido como protocolo de internet (IP) é um registro único para cada computador conectado à rede, permite rastrear a localização dos dispositivos, conforme mencionado por ROHR (2021) em reportagem ao site Globo. A partir desse registro, existe uma identificação estimada dos endereços de todo o globo terrestre. Conforme Fernando Amatte, diretor de Red Team para América Latina da empresa de segurança digital Cipher, o mesmo explica que os endereços IP são distribuídos mundialmente pela IANA (sigla em inglês para "autoridade para atribuição de números de internet"). Segundo ROHR (2021), A IANA reserva faixas de número, ou "blocos de endereços", para determinados países e cada país possui sua própria

autoridade para realizar essa distribuição. Sendo mais especifico para o Brasil, o órgão responsável é o Núcleo de Informação e Coordenação do Ponto BR (NIC.br).

Com as informações da IANA e a compreensão das regras de distribuição de endereços cibernéticos, é possível padronizar e conseguir uma localização estimada através do IP. Com essa informação, é possível concluir que cada usuário tem seu padrão de acesso e a partir do método de treinamento da IA generativa é possível identificar possíveis desvios dos padrões mapeados.

3. Metodologia

Conforme informações anteriores, entendendo que existem órgãos que realizam essas fiscalizações e obrigam que as instituições bancárias tenham esses dados armazenados, o uso de IA fica cada vez mais comum, o que demonstra que padronizar informações para diferentes tipos de aplicações com o intuito de ensinar a IA generativa se torna totalmente viável.

3.1 Vertex IA – AutoML

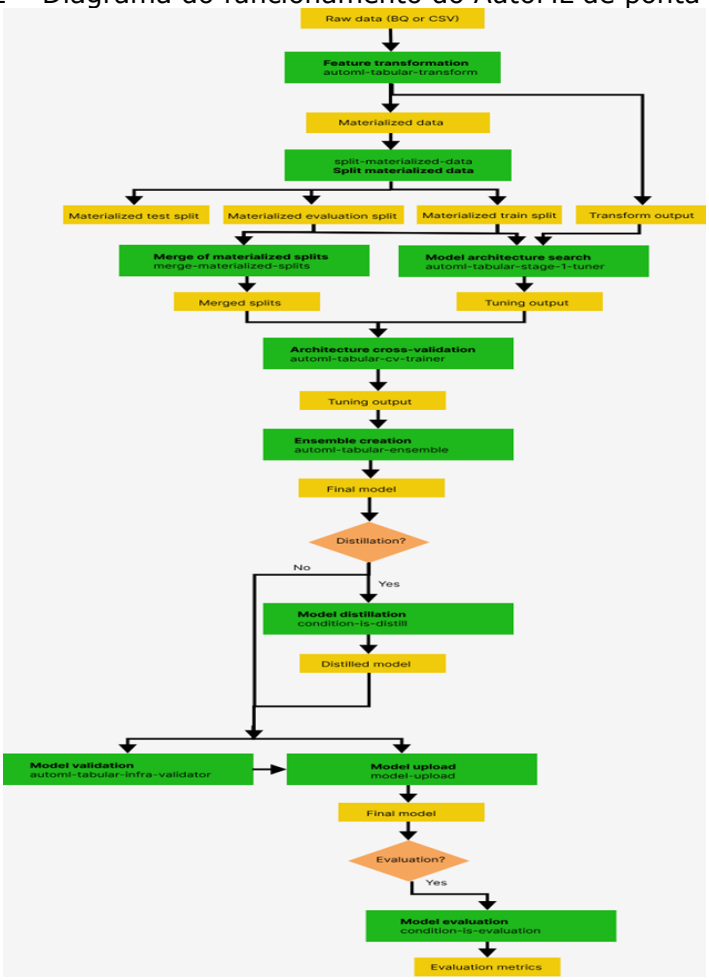
Entendendo as informações anteriores, conseguimos agora entrar no tópico de como a tecnologia funciona. Utilizaremos uma das ferramentas disponibilizadas no mercado, que será a Vertex IA, da Google Cloud. Explicaremos o funcionamento geral da ferramenta, como vai ser definido a atuação para um monitor de fraudes e alguns exemplos práticos.

Conforme a GOOGLE GLOUD (2024a), a Vertex IA é uma plataforma da Google Cloud baseada em nuvem que facilita o treinamento e aplicação de modelos de Machine Learning e ferramentas de Inteligência Artificial. Entre as diversas funcionalidades que essa plataforma possui, utilizaremos a funcionalidade do AutoML tabular (Automated Machine Learning) para

desenvolver o método e a atuação para o monitor de fraudes.

Como o próprio nome diz, o AutoML seria a automatização do aprendizado de máquina, sem a necessidade de código ou divisão de dados, diz a GOOGLE CLOUD (2024b). Conforme Figura 2, o AutoML de ponta a ponta tem várias etapas e executa diversas atividades como transformação e adequação dos tipos de dados, divisão dos dados em conjunto de treinamento, avaliação e teste, mescla da avaliação e treinamentos materializados, validação cruzada e escolha entre diferentes arquiteturas para produzir o melhor resultado final.

Figura 2 – Diagrama do funcionamento do AutoML de ponta a ponta

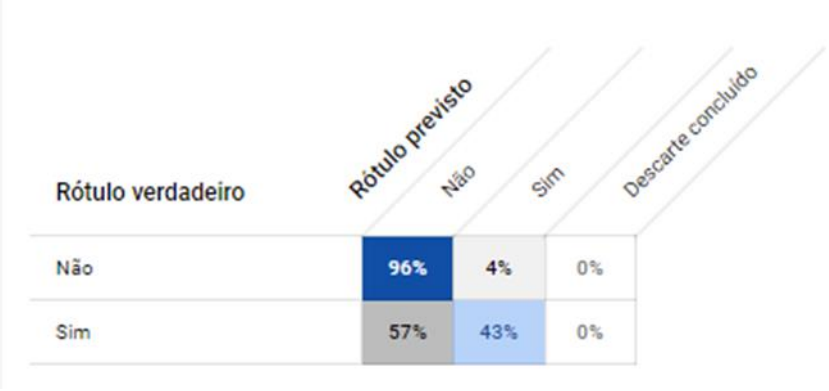


Fonte: Google Cloud, 2024b

Com a plataforma e o código em mãos, é fundamental que os dados necessários sejam alimentados, como por exemplo os dados de padronização de IP, padronização de comportamentos, boas práticas da instituição financeira e por meio de uma API, os dados em tempo real das ações dos clientes, logs de horário e IP de acesso de todos os usuários da instituição, para integrar a solução.

A partir do que foi definido acima, serão realizados treinamentos de aprendizados supervisionados, com intuito de ensinar a determinar situações que se assemelham a uma fraude ou não, com base em atributos definidos na alimentação dos dados, ou seja, a partir da anormalidade de acesso (IP) e/ou nos comportamentos habituais dos clientes, será definido como fraude e serão aplicadas ações de contorno e bloqueios, com intuito de mitigar o golpe.

Figura 3 – Resultados do modelo AutoML tabular executado com dados fictícios



Fonte: Autores

Ao longo do treinamento, é esperado que o monitor de fraudes consiga identificar com precisão o que é uma fraude para aplicar uma ação, porém entendendo que nem tudo é perfeito, também existem cenários de resultados falsos positivos, ou seja, quando um caso não é uma fraude, mas são realizadas ações de bloqueio e cenários de falsos negativos, quando não são identificadas as fraudes, conforme Figura 3. Entendendo que esses tipos

de cenários são possíveis, os testes e validações da solução é um passo fundamento para o produto final. O mesmo tem que ser realizado de forma detalhada e estruturada, para corrigir e mitigar cenários negativos antes que a solução seja aplicada de fato.

Com o racional definido, iremos demonstrar alguns exemplos de aplicações práticas da ferramenta.

3.2 Exemplos Práticos

Tabela 2 – Exemplo de histórico de acesso do cliente

Nome	Data/hora	Ip de acesso	Região
Cliente X	01/08/2024 - 15:03	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	03/08/2024 - 12:30	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	04/08/2024 - 13:25	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	07/08/2024 - 17:43	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	11/08/2024 - 11:00	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	14/08/2024 - 12:32	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	16/08/2024 - 14:31	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	22/08/2024 - 18:02	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	25/08/2024 - 21:31	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	03/09/2024 - 22:22	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	11/09/2024 - 10:43	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	12/09/2024 - 11:54	xxx.xxx.xxx	São Paulo - São Paulo
Cliente X	15/09/2024 - 03:25	xxx.yyy.xxx	Pará - Belém
Cliente X	15/09/2024 - 11:30	xxx.xxx.xxx	São Paulo - São Paulo

Fonte: Autores

Conforme exemplo da tabela 2, o décimo terceiro acesso realizado, dia 15/09/2024 às 03:25, foi identificado como uma anormalidade, de acordo com os padrões de IP que o cliente vinha realizando os acessos. A Inteligência Artificial Generativa utilizando de base, seus treinamentos e metodologia, realizou um bloqueio no mesmo instante que houve esse acesso. O cliente foi notificado por e-mail do bloqueio e recebeu as instruções necessárias para se resguardar, entre elas a mudança de senha. No mesmo dia 15/09/2024 às 11:30, o cliente realizou o acesso e em contato com seu gerente, seguiu as instruções repassadas para se precaver de possíveis ameaças futuras

Diante do exemplo, foi possível observar o funcionamento de uma das funcionalidades do monitor de fraudes e como ele evitou que ocorresse uma invasão a conta bancária de um cliente.

Tabela 3 - Exemplo de histórico de acessos no mês

Nome	Data/hora	Região de acesso	Atividades Realizadas
Cliente X	25/07/2024 13:54	São Paulo - São Paulo	Pagamento de Boletos
Cliente X	30/07/2024 16:23	São Paulo - Osasco	Verificação do Saldo
Cliente X	30/07/2024 16:35	São Paulo - Osasco	Investimento
Cliente Z	30/07/2024 17:35	Rio de Janeiro - Rio de Janeiro	Pagamento de Boletos
Cliente Y	30/07/2024 19:37	São Paulo - Osasco	Verificação do Extrato
Cliente X	01/08/2024 13:54	São Paulo - São Paulo	Pagamento de Boletos
Cliente X	07/08/2024 13:02	São Paulo - São Paulo	Pagamento de Boletos
Cliente X	09/08/2024 17:23	São Paulo - Osasco	Verificação do Extrato
Cliente X	12/08/2024 13:23	São Paulo - Osasco	Verificação do Extrato
Cliente X	14/08/2024 13:07	São Paulo - São Paulo	Pagamento de Boletos
Cliente Z	14/08/2024 16:07	Rio de Janeiro - Rio de Janeiro	Pagamento de Boletos
Cliente Y	14/08/2024 19:23	São Paulo - Osasco	Verificação do Extrato
Cliente Z	14/08/2024 20:07	Rio de Janeiro - Rio de Janeiro	Pagamento de Boletos
Cliente Z	14/08/2024 20:12	Rio de Janeiro - Rio de Janeiro	Transferência Bancaria
Cliente X	15/08/2024 13:02	São Paulo - São Paulo	Transferência Bancaria
Cliente Z	20/08/2024 22:18	Rio de Janeiro - Rio de Janeiro	Pagamento de Boletos
Cliente X	21/08/2024 13:19	São Paulo - São Paulo	Pagamento de Boletos
Cliente X	23/08/2024 17:23	São Paulo - Osasco	Verificação do Extrato
Cliente Y	23/08/2024 14:23	São Paulo - Osasco	Verificação do Extrato
Cliente Y	24/08/2024 19:23	São Paulo - Osasco	Verificação do Extrato
Cliente X	27/08/2024 13:18	São Paulo - São Paulo	Pagamento de Boletos
Cliente X	30/08/2024 16:45	São Paulo - Osasco	Verificação do Saldo
Cliente X	30/08/2024 16:58	São Paulo - Osasco	Investimento
Cliente X	31/08/2024 04:18	São Paulo - Osasco	Verificação do Saldo
Cliente X	31/08/2024 04:20	São Paulo - Osasco	Solicitação de Empréstimo
Cliente X	31/08/2024 04:23	São Paulo - Osasco	Transferência Bancaria

Fonte: Autores

(MOHANTY; AASHIMA; MISHRA 2023) comentam que ao deixar o trabalho monótono com a Inteligência artificial a carga de trabalho nos humanos se torna mais leve e as decisões tomadas se tornam melhores, o que pode levar a um melhor atendimento e serviço prestado, ao observar a tabela 3 é possível identificar que uma pessoa teria um intenso trabalho para identificar e registrar os padrões de comportamento de vários clientes diferentes. A Inteligência Artificial Generativa tem a capacidade de

identificar, por exemplo que na tabela 3 as últimas movimentações foram anormais rapidamente, pois o padrão comportamental do cliente demonstrava que ele não faria esse tipo de ação no horário em que ela foi realizada, e assim pode impedi-las em tempo real, algo que um funcionário comum nunca seria capaz de fazer em tempo real.

4. Resultados e Discussões

Com o entendimento do momento atual vivido na sociedade, do que é Inteligência Artificial, Inteligência Artificial Generativa, IPs de acesso, comportamentos de usuários e como os dados são padronizados a solução do uso de IA generativa para monitorar desvios no acesso trata-se de algo viável e eficiente para mitigar possíveis fraudes. Clientes que tiveram seus dados vazados ou concebidos através de engenharia social, phishing e/ou qualquer outro tipo de fraude estarão resguardados através desse monitoramento.

Mas como toda ideia e projeto, melhorias são cabíveis a todo momento. Entendendo que a ideia descrita no artigo é um MVP (Minimum Viable Product), a mesma traz resultados satisfatórios.

Conforme dito por (VEDAPRADHA.R; HARIHARAN RAVI, 2018), o uso de IA em soluções bancárias estão e serão mais utilizadas com o passar do tempo. Com ênfase no uso de dados e uso da Inteligência Artificial, a capacidade de análise de informações em grandes quantidades em prol dos clientes permite que os bancos operem em um bom ritmo e entreguem a melhor solução final aos clientes.

Porém como toda solução tecnológica, é necessário entender possíveis riscos, entre elas a questão de alucinação da ferramenta. Conforme a própria GOOGLE (2024), as alucinações seriam resultados incorretos ou enganosos geradas pela ferramenta, seja por questão de treinamento insuficiente ou previsões incorretas sobre o assunto decorrente. Para esse tipo de situação,

em seguida do mapeamento de uma possível alucinação, o monitor seria tirado dos ambientes de produção por um tempo e seria treinada e homologada até que seus resultados sejam satisfatórios.

Considerando todas soluções de Inteligência Artificial Generativa, ao conhecer e estar em contato com mais situações ao longo de tempo do uso, a tendência é que a ferramenta se torne cada vez mais eficiente, ou seja, não se pode esperar que de primeiro momento ela realize e identifique todos os cenários existente, mas sendo definidos de base dados com objetivos claros sobre seu escopo de atual, a ferramenta irá suprir de forma eficiente.

5. Conclusão

Em vista dos fatos apresentados, podemos concluir que a utilização de novas tecnologias como a Inteligência Artificial e Inteligência Artificial Generativa na prevenção de fraudes bancárias representa um avanço significativo e de extrema importância na melhoria da segurança e mitigação de riscos tanto paro o banco como para o usuário. Ao analisar dados com base na geolocalização e padrões comportamentais dos usuários, a ideia do monitoramento utilizando com base a IA generativa consegue prevenir possíveis prejuízos, aumentar a segurança, evitar que erros humanos ocorram, aumento na produtividade devido ao funcionamento 24/7. Porém os resultados serão positivos, a partir do entendimento que os treinamentos com alimentação de dados coerentes e coesos serão realizados de forma correta e constante pela equipe responsável. Diante de um cenário cada vez mais tecnológico, é essencial o constante investimento em pesquisas e desenvolvimento de novas tecnologias para aprimorar a proteção de dados dos usuários, é possível vislumbrar um futuro em que os danos causados pelas fraudes financeiras sejam significativamente reduzidos, reforçando assim a confiança dos usuários nos bancos e sistemas financeiros.

Agradecimentos

A Deus por nos dar saúde e garantir nossa segurança durante nossa jornada acadêmica.

Os autores agradecem o apoio incondicional de suas respectivas famílias desde o início da graduação.

Os mesmos agradecem ao professor Roberto Marcos Kalili pelo apoio imensurável para o desenvolvimento do artigo e à instituição Universidade São Judas Tadeu por todo o suporte ao longo dos anos.

Aos demais que participaram de nossa jornada na Universidade São Judas Tadeu.

Muito Obrigado!

Referências

ACS. Estelionato. *In*: ACS. **Estelionato**. Website, 2021. Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/estelionato-1#:~:text=O%20famoso%20crime%20do%20artigo,maioria%20da%20vezes%20em%20dinheiro. Acesso em: 11 nov. 2024.

BANCO CENTRAL DO BRASIL. **Monitoramento do Sistema Financeiro**. Brasil, 2024. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/monitoramento. Acesso em: 11 nov. 2024.

CARLE, Eben. Ask a Techspert: What is generative AI?. *In*: CARLE, Eben. **Ask a Techspert: What is generative AI?**. Website, 11 mar. 2023. Disponível em: https://blog.google/inside-google/googlers/ask-a-techspert/what-is-generative-ai/. Acesso em: 11 nov. 2024.

CNDL BRASIL. **7,2 milhões de consumidores sofreram golpes financeiros nos últimos 12 meses, aponta CNDL / SPC Brasil**. Brasil, 2024. Disponível em: https://site.cndl.org.br/72-milhoes-de-consumidores-sofreram-golpes-financeiros-nos-ultimos-12-meses-aponta-cndl-spc-brasil/. Acesso em: 11 nov. 2024.

DEL CLARO, Fernanda. **O avanço tecnológico no mundo econômico.** Revista FAE, Vitrine da Conjuntura, v. 2, n. 8, p.1-4, 2009.
FEBRABAN TECH. **Como os bancos estão usando a inteligência artificial e o big data para evitar a exposição a crimes financeiros**. Brasil, 20 set. 2022. Disponível em: https://febrabantech.febraban.org.br/temas/inteligencia-artificial/como-os-bancos-estao-usando-a-inteligencia-artificial-e-o-big-data-para-evitar-a-exposicao-a-crimes-financeiros. Acesso em: 11 nov. 2024.

GOMES, DENNIS DOS SANTOS. **Inteligência Artificial: Conceitos e Aplicações**. [*S. l.*], dezembro 2010. Disponível em: https://www.professores.uff.br/screspo/wp-content/uploads/sites/127/2017/09/ia_intro.pdf. Acesso em: 11 nov. 2024.

GOOGLE CLOUD. Fluxo de trabalho tabular para o AutoML de ponta a ponta. Website, 15 mar. 2024. Disponível em: https://cloud.google.com/vertex-ai/docs/tabular-data/tabular-workflows/e2e-automl?hl=pt-br. Acesso em: 17 nov. 2024.

GOOGLE CLOUD. Introdução à Vertex AI. [S. l.], 26 jul. 2024. Disponível em: https://cloud.google.com/vertex-ai/docs/start/introduction-unified-

platform?hl=pt-br#:~:text=A%20Vertex%20AI%20%C3%A9%20uma,aplicativos%20com%20tecnologia%20de%20IA. Acesso em: 17 nov. 2024.

GOOGLE. O que são alucinações de IA?. *In*: **O que são alucinações de IA?**. Website, 2024. Disponível em: https://cloud.google.com/discover/what-are-ai-hallucinations?hl=pt-BR. Acesso em: 11 nov. 2024.

GOV.BR. **Avaliação Nacional de Risco (ANR)**. Brasil, 2022. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagem-de-dinheiro/avaliacao-nacional-de-riscos-anr. Acesso em: 11 nov. 2024.

GOV.BR. **Conselho de Controle de Atividades Financeiras (Coaf)**. Brasil, 26 jan. 2022. Disponível em: https://www.gov.br/pt-br/orgaos/conselho-de-controle-de-atividades-financeiras. Acesso em: 11 nov. 2024.

INSTITUTO de Pesquisa DataSenado Panorama Político 2024: **Apostas esportivas, golpes digitais e endividamento**. Secretaria de Transparencia, Setembro 2024. Disponível em: https://www12.senado.leg.br/institucional/datasenado/materias/relatorios-de-pesquisa/golpes-digitais-atingem-24-dos-brasileiros-aponta-21a-edicao-da-pesquisa-panorama-politico. Acesso em: 31 out. 2024.

KLETTENBERG, Josiane. **Segurança da informação: Um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de Instituições Bancárias**, 2016. p.181. Pós-Graduação em Ciência da Informação - Centro de Ciências da Educação da Universidade Federal de Santa Catarina, Florianópolis, ano da defesa.

MOHANTY, Birajit; AASHIMA; MISHRA, Shweta. ROLE OF ARTIFICIAL INTELLIGENCE IN FINANCIAL FRAUD DETECTION. **RMAM**, [*s. l.*], ano 2023, p. 0-22, Abril 2023. Disponível em: https://www.abacademies.org/articles/role-of-artificial-intelligence-in-financial-fraud-detection.pdf. Acesso em: 11 nov. 2024.

REGISTRO DE AUDITOR INDEPENDENTE. In: **REGISTRO DE AUDITOR INDEPENDENTE**. CVM, 9 out. 2024. Disponível em: https://sistemas.cvm.gov.br/port/snc/ResumoNormas.asp#:~:text=Para%20obter%20registro%20como%20auditor,da%20data%20do%20registro%20na. Acesso em: 9 out. 2024.

REZENDE, Frederico Antonio Oliveira de. **RESPONSABILIDADE CIVIL DOS BANCOS EM RELAÇÃO ÀS FRAUDES ELETRÔNICAS**. FMU DIREITO

- Revista Eletrônica, 18 out. 2012. Disponível em: https://revistaseletronicas.fmu.br/index.php/FMUD/article/view/78. Acesso em: 11 nov. 2024.

RODRIGUES, Luiz Victor. IA no setor bancário: como pode ser aplicada? A IA pode ser usada pelos bancos para agilizar burocracias, acelerar o processo de vendas de serviços e, ainda, melhorar o atendimento ao cliente.. Website, 21 abr. 2024. Disponível em: https://www.salesforce.com/br/blog/ia-setor-bancario/. Acesso em: 12 nov. 2024.

ROHR, Altieres. **Localização de endereço de IP: entenda como pode ser feito o rastreamento e o que é mito. Localização de endereço de IP: entenda como pode ser feito o rastreamento e o que é mito**, G1, p. 0-100, 2 mar. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2021/03/02/localizacao-de-endereco-de-ip-entenda-como-pode-ser-feito-o-rastreamento-e-o-que-e-mito.ghtml. Acesso em: 1 out. 2024.

SICHMAN, Jaime Simão. **Inteligência Artificial e sociedade: avanços e riscos**. Scielo, 12 mar. 2021. Disponível em: https://doi.org/10.1590/s0103-4014.2021.35101.004. Acesso em: 11 nov. 2024.

SPADINI, Allan Segovia. O que é Inteligência Artificial? Como funciona uma IA, quais os tipos e exemplos. [S. l.], 4 dez. 2023. Disponível em: https://www.alura.com.br/artigos/inteligencia-artificial-ia?srsltid=AfmBOoq9e2AAW1v6aOzRWbXWaqpNhniH3p7RMyHFSDd7pwUsdR8ZZzAa. Acesso em: 14 nov. 2024.

VEDAPRADHA.r; HARIHARAN Ravi, 2018. **"Application Of Artificial Intelligence In Investment Banks,"** Review of Economic and Business Studies, Alexandru Ioan Cuza University, Faculty of Economics and Business Administration, issue 22, pages 131-136, December.