IDENTIFICAÇÃO DE PROBLEMAS E FALHAS DE SEGURANÇA EM CÓDIGO DE PROGRAMAÇÃO: UMA ABORDAGEM UTILIZANDO INTELIGÊNCIA ARTIFICIAL GENERATIVA

Pedro Vinícius da Rocha Fraga, Franciele Carla Petry

Resumo

A detecção de falhas de segurança em códigos de programação é essencial para garantir a qualidade e a segurança de softwares modernos. Com o aumento da complexidade e do volume de códigos, a análise manual de vulnerabilidades tornou-se desafiadora, destacando o potencial das técnicas de Inteligência Artificial (IA) na análise estática de código, que identifica problemas diretamente no código-fonte antes de sua execução. Apesar de ferramentas como GitHub Copilot e ChatGPT oferecerem suporte durante o desenvolvimento, limitações como respostas incorretas e falhas lógicas representam desafios significativos. Este artigo apresenta uma análise da eficácia de ferramentas de IA na identificação e resolução de vulnerabilidades, como Cross-Site Scripting (XSS), SQL Injection, utilizando as linguagens TypeScript e JavaScript. A pesquisa envolve testes e comparações entre diferentes ferramentas de IA, considerando seus modelos, versões e configurações, com o objetivo de avaliar seu impacto no processo de desenvolvimento de software.

Palavras-chave: Inteligência Artificial, análise de código, segurança em software, vulnerabilidades, TypeScript, JavaScript.

1 INTRODUÇÃO

A detecção eficiente de problemas e falhas de segurança em códigos de programação é fundamental para garantir a qualidade e segurança dos softwares e seus ambientes. O aumento de complexidade e volume de códigos em sistemas modernos tornam desafiador a identificação manual de possíveis vulnerabilidades. Nesse contexto, a aplicação de técnicas de Inteligência Artificial (IA) para análise de código tem se mostrado uma alternativa promissora.

Quando a detecção de problemas de programação é feita utilizando estratégias estáticas, ou seja diretamente pelo código fonte, problemas são identificados antes mesmo de serem percebidos ou destacados de maneira dinâmica em ambientes reais. Apesar das limitações atuais, o futuro aponta para a Inteligência Artificial participando ativamente em projetos de desenvolvimento, algo que já é realidade com ferramentas como "GitHub Copilot" que sugere códigos automaticamente enquanto o programador digita e "Chat GPT" que ajuda na redação de textos e respostas.

No entanto, respostas incorretas contendo falhas ou erros lógicos também são uma grande limitação e preocupação durante o uso das ferramentas. Plataformas de código como StackOverflow bloqueiam respostas geradas por Inteligência Artificial como medida de cautela, considerando que o amplo uso é relativamente novo e suas implicações ainda não são amplamente compreendidas (Alecrim, 2022).

A abordagem do presente projeto foi o desenvolvimento de um conjunto diversificado de testes e análise de eficácia de ferramentas de IA na identificação e resolução de problemas em diferentes contextos dentro de códigos de programação. Para atingir esse objetivo, o projeto utiliza as linguagens de programação TypeScript e JavaScript, devido à sua relevância e ampla utilização no desenvolvimento web. Serão realizados

testes específicos para identificar vulnerabilidades conhecidas, como Cross-Site Scripting (XSS), SQL Injection.

Para atingir o objetivo do projeto foram gerados dados de comparação entre ferramentas de IA para análise, levando em consideração os seus modelos, versões e configurações. A parte comunicativa com a IA é de grande importância, bem como a exposição de contextos e comunicação clara com as ferramentas e de maneira a não influenciar respostas.

2 **DESENVOLVIMENTO**

Para o desenvolvimento adequado do projeto é necessário uma base conceitual sobre o funcionamento das tecnologias utilizadas, sobre o entendimento dos problemas e desafios enfrentados em códigos de programação e como afetam pessoas e empresas, bem como soluções já adotadas atualmente.

2.1 FERRAMENTAS DE INTELIGÊNCIA ARTIFICIAL

O conceito de Inteligência Artificial pode ser definido como: utilização de computadores para imitar a capacidade de inteligência humana. Considerando as capacidades de resolução de problemas e tomadas de decisão da mente humana. Atualmente já existem diversas aplicações reais do conceito como por exemplo em ferramentas de atendimento ao cliente, geralmente treinadas com um banco de dados que contém perguntas frequentes, dispensando ou reduzindo a necessidade de um humano realizar atendimentos totalmente manuais. Mecanismos de recomendação utilizando dados de comportamento passado também auxiliam na descoberta de tendências e estratégias relevantes (IBM).

No final de novembro de 2022, a ferramenta ChatGPT, desenvolvida pela OpenAi revolucionou o mercado ao atingir a marca de 100 milhões de usuários após 2 meses de ser exposta para o público, se tornando o aplicativo com crescimento mais rápido da história (Exame, 2023). A principal funcionalidade da ferramenta é responder a perguntas sobre variados assuntos, resolver problemas lógicos e fornecer soluções aos inputs que recebe por meio de mensagens em uma interface com formato de chat, simulando uma conversa, consegue ter diálogos baseados em informações obtidas em bancos de dados, publicações na internet e outras fontes do mundo digital (Curvelo, 2023).

O grande sucesso do ChatGPT fez com que outras grandes empresas começassem a analisar, desenvolver e implementar soluções como esta em seus respectivos serviços e produtos, inclusive surgindo diversos concorrentes diretos da ferramenta com interface de chat, como por exemplo o Gemini do Google.

De acordo com o relatório do Fórum Econômico Mundial, a IA pode contribuir com até US$15,7 trilhões para a economia global até 2030. A Precedence Research conhecida por fazer análise de mercado, projeta um crescimento de 869% em oito anos, indo de US$165 bilhões em 2023 para US$1,6 trilhões em 2030. Aliás, o mercado de inteligência artificial tem crescido rapidamente há algum tempo. Segundo a MarketsandMarkets, o mercado global de IA deve atingir US$190,61 bilhões em 2025, com uma taxa de crescimento anual composta (CAGR) de 36,62% entre 2019 e 2025 (Run Talent, 2023).

2.2 PROBLEMAS E VULNERABILIDADES EM CÓDIGOS DE PROGRAMAÇÃO

Problemas e vulnerabilidades nos códigos de programação podem ter impactos significativos tanto nos indivíduos como nas organizações. Estas vulnerabilidades, conforme Mahyari, 2022 podem levar a consequências sociais e financeiras desastrosas. Para os indivíduos, tais vulnerabilidades podem resultar em roubo de identidade, perda de privacidade e roubo de propriedade intelectual (TARAFDAR; GUPTA; TUREL, 2015). Por outro lado, para as organizações, as repercussões podem ser ainda mais graves, incluindo perdas financeiras, danos à reputação e responsabilidades legais. A exploração de vulnerabilidades em sistemas de software pode levar a violações de dados, interrupções de serviços e acesso não autorizado a informações confidenciais, representando uma ameaça à segurança e estabilidade geral dos sistemas.

Além disso, o impacto das vulnerabilidades nos códigos de programação vão além das perdas financeiras imediatas. As vulnerabilidades também podem afetar sistemas de infraestruturas críticas, como redes de transporte, redes de energia e sistemas de saúde (Smit et al., 2014). As perturbações nestes sistemas devido à exploração de vulnerabilidades podem ter consequências de longo alcance, afetando a segurança pública, a estabilidade econômica e a segurança nacional. Portanto, abordar e mitigar as vulnerabilidades nos códigos de programação é essencial não só para preservar os interesses individuais e organizacionais, mas também para garantir a resiliência e a segurança de funções sociais vitais que dependem de sistemas de software.

2.3 MÉTODOS COMUNS PARA IDENTIFICAÇÃO DE VULNERABILIDADES E ERROS EM CÓDIGO DE PROGRAMAÇÃO

Os erros e falhas em códigos podem acontecer por diversos motivos, falhas humanas, má configurações, uso incorreto de ferramentas e erros de digitação. Editores de texto conseguem identificar erros de digitação de sintaxe de acordo com a linguagem de programação. Revisões e análise de código são comumente feitas manualmente por humanos que analisam as informações alteradas, incluídas e excluídas, custando tempo ao humano que muitas vezes tem que entender todo o contexto de um código para analisar com sabedoria e eficiência, mesmo assim devido a complexidade do sistema, ou desatenção detalhes cruciais podem passar despercebidos.

2.4 DESAFIOS E LIMITAÇÕES DAS FERRAMENTAS DE IA PARA IDENTIFICAÇÃO DE VULNERABILIDADES

Apesar dos avanços significativos, as ferramentas de inteligência artificial para identificação de vulnerabilidades em códigos de programação ainda enfrentam diversos desafios e limitações. Uma das principais dificuldades é a alta taxa de falsos positivos, onde ocorre uma identificação errônea de um trecho de código como vulnerável (Bertucci et al., 2021).

Além disso, a complexidade e a sofisticação dos ataques de segurança estão em constante evolução, o que exige uma atualização contínua dos modelos de IA para garantir que eles possam identificar novas formas de vulnerabilidades. Isso requer um esforço significativo em termos de coleta de novos dados e re-treinamento dos modelos, podendo ser custoso e demorado (Goodfellow et al., 2016).

2.5 IMPACTO DA IA GENERATIVA NA SEGURANÇA DE SISTEMAS

A implementação de IA generativa na segurança de sistemas tem potencial para transformar significativamente a maneira como as vulnerabilidades são detectadas e mitigadas. Um dos principais impactos é a capacidade de automatizar a análise de grandes volumes de código, permitindo que as organizações identifiquem e corrijam vulnerabilidades de forma mais rápida e eficiente. Ferramentas baseadas em IA generativa podem escanear repositórios de código em busca de padrões de vulnerabilidade conhecidos, reduzindo a necessidade de revisões manuais extensivas (Lipo et al., 2021).

Além disso, a IA generativa pode ajudar a identificar vulnerabilidades emergentes que ainda não foram documentadas. Isso é possível devido à sua capacidade de aprender continuamente a partir de novos dados e ajustar seus modelos de detecção conforme surgem novos tipos de ameaças. Por exemplo, ao analisar os commits mais recentes em repositórios de código aberto, uma IA generativa pode detectar alterações suspeitas que possam introduzir novas vulnerabilidades (Stoica et al., 2017).

No entanto, a utilização de IA generativa na segurança de sistemas não está isenta de desafios. Um dos principais problemas é garantir que os modelos de IA sejam treinados com dados representativos e de alta qualidade. Dados inadequados ou enviesados podem levar a modelos de detecção ineficazes que não conseguem identificar todas as vulnerabilidades relevantes. Além disso, a confiança excessiva em ferramentas automatizadas pode resultar na negligência de revisões manuais essenciais, potencialmente deixando passar vulnerabilidades críticas (Buendgen et al., 2022).

2.6 IMPACTO DA IA GENERATIVA NA DETECÇÃO DE ERROS DE SEGURANÇA

A IA generativa está evoluindo para não apenas detectar vulnerabilidades, mas também sugerir correções. Essa função se destaca no contexto da cibersegurança, onde a rapidez para identificar e mitigar ameaças pode fazer a diferença entre um sistema seguro e um vulnerável. Estudos mostram que, ao utilizar IA para monitorar o código em tempo real, empresas conseguiram reduzir incidentes de segurança em até 30% (Lima; Carvalho, 2022). Contudo, ainda existem desafios a serem enfrentados, especialmente no que se refere à geração de falsos positivos. A IA, muitas vezes, pode apontar potenciais vulnerabilidades que, após uma análise humana, revelam-se inofensivas. Isso pode levar à sobrecarga de trabalho para os desenvolvedores, que precisam verificar manualmente cada alerta (Silva et al., 2021).

Outro desafio significativo está relacionado à confiabilidade das IAs em detectar vulnerabilidades em contextos desconhecidos ou pouco documentados. Embora a IA seja excelente em identificar padrões já conhecidos, novas formas de ataque ou exploits sofisticados podem não ser detectados, o que evidencia a necessidade de uma integração entre a inteligência humana e as ferramentas de IA (Garcia et al., 2021).

2.7 CONSIDERAÇÕES ÉTICAS NO USO DE IA NO DESENVOLVIMENTO DE SOFTWARE

A transparência e responsabilidade são questões éticas chave. A natureza de "caixa preta" de muitos algoritmos de IA dificulta a explicação sobre como eles chegam a determinadas conclusões, o que pode ser problemático quando essas decisões afetam pessoas diretamente. Essa falta de clareza questiona quem deve ser responsabilizado em casos de erros,

como no uso de veículos autônomos ou diagnósticos médicos errados (Binns, 2023).

Privacidade de dados é outra área de grande preocupação. A coleta massiva de dados pessoais para o treinamento de IAs levanta questões sobre o uso adequado e seguro dessas informações. Em alguns casos, a IA foi usada para vigilância e controle social, como em sistemas de reconhecimento facial empregados por governos para monitorar populações, exacerbando questões de privacidade e direitos humanos (Whittaker et al., 2022).

2.8 IMPLICAÇÕES PARA O MERCADO DE TRABALHO

As Implicações para o Mercado de Trabalho derivadas do avanço da IA generativa são amplas e impactam diversas indústrias. A automação de tarefas antes exclusivas de humanos, como análise de dados, criação de conteúdo e até mesmo desenvolvimento de software, está transformando profundamente a forma como as organizações operam. Esse cenário traz tanto oportunidades quanto desafios para trabalhadores e empregadores. Por um lado, a IA generativa pode aumentar a produtividade e permitir a realização de tarefas de maneira mais rápida e eficiente, liberando trabalhadores para colocar foco em atividades mais estratégicas e criativas. No setor de tecnologia, por exemplo, engenheiros de software podem utilizar a IA para automatizar partes do processo de codificação, reduzindo o tempo necessário para desenvolver soluções complexas e melhorando a qualidade do código final (Whittaker et al., 2022).

Por outro lado, há preocupações em torno da substituição de empregos. Profissões que envolvem tarefas repetitivas ou baseadas em padrões, como análise financeira, suporte ao cliente e criação de conteúdo

básico, estão entre as mais vulneráveis à automação. Segundo estudos, estima-se que até 30% das atividades em setores como o financeiro e o administrativo podem ser realizadas por IA nos próximos anos, o que pode resultar em um deslocamento significativo de trabalhadores (Arntz et al., 2020).

Essa transformação também cria uma demanda crescente por novas habilidades. Profissionais capacitados em áreas como ciência de dados, machine learning e segurança cibernética tendem a se tornar cada vez mais valiosos, à medida que a IA se integra em processos empresariais. Nesse sentido, a adaptação a essas mudanças será um dos fatores-chave para a empregabilidade futura.

Além disso, o impacto sobre o mercado de trabalho está levando governos e empresas a discutir questões éticas e regulamentações para proteger trabalhadores e garantir uma transição justa. O debate sobre a renda básica universal também está ganhando força, com algumas organizações argumentando que, em um mundo com menos empregos tradicionais, será necessário repensar os modelos econômicos e sociais (Brynjolfsson & McAfee, 2021).

2.9 IMPLICAÇÕES NA SEGURANÇA DE DADOS

A capacidade dessas ferramentas de criar conteúdo em massa pode ser explorada para ataques cibernéticos mais sofisticados, como phishing e engenharia social, com maior personalização e verossimilhança nas mensagens geradas. Essas técnicas, apoiadas pela IA, tornam mais difícil a identificação de fraudes por parte das vítimas e sistemas de defesa (Brundage et al., 2020).

A segurança dos dados utilizados para treinar esses modelos também é uma questão central. O uso de grandes volumes de dados sensíveis durante o processo de treinamento de modelos pode expor informações confidenciais, como dados pessoais, a riscos de vazamento. Além disso, ataques adversariais, onde invasores manipulam os inputs de IA para gerar resultados maliciosos, representam uma ameaça crescente. Esses ataques exploram vulnerabilidades nos modelos e podem impactar diretamente a confiabilidade dos sistemas de IA (Papernot et al., 2018).

Em resposta a essas ameaças, é necessário uma regulamentação mais rígida e o desenvolvimento de protocolos de segurança cibernética robustos, focados em práticas como a anonimização de dados, auditorias de segurança frequentes e a criação de defesas contra IA adversária. A implementação dessas medidas visa garantir que o progresso nas tecnologias de IA generativa seja acompanhado de uma proteção eficaz dos dados pessoais (Brundage et al., 2020).

2.10 MATERIAIS E MÉTODOS

Para garantir uma análise detalhada e justa das ferramentas de inteligência artificial generativa utilizadas neste projeto, foram estabelecidos critérios específicos que permitirão avaliar o desempenho de cada IA na identificação e resolução de vulnerabilidades em códigos de programação. Esses critérios foram selecionados com base em suas relevâncias práticas para o desenvolvimento de software seguro.

1. Precisão na Detecção Este critério se refere à capacidade da IA de identificar corretamente os erros e vulnerabilidades no código. A precisão é crucial, pois um erro não identificado pode comprometer a segurança do sistema. A ferramenta será

avaliada pela sua taxa de acertos, comparando o número de vulnerabilidades encontradas com o número total de vulnerabilidades presentes no código.

2. Abrangência

   A abrangência está relacionada à capacidade da IA de detectar uma ampla gama de vulnerabilidades, desde problemas de segurança críticos até erros menores de lógica e sintaxe. Quanto mais variada for a gama de problemas que a ferramenta consegue identificar, maior será sua utilidade em diferentes contextos de desenvolvimento.

3. Qualidade das Sugestões

   Além de detectar os problemas, a qualidade das soluções propostas é fundamental. Esse critério avalia se as sugestões fornecidas pela IA são precisas, eficazes e seguem as melhores práticas de desenvolvimento de software seguro. Soluções inadequadas ou incompletas podem gerar novos problemas no código.

4. Facilidade de Integração

   A facilidade de integração avalia como a ferramenta de IA pode ser incorporada aos fluxos de trabalho existentes de desenvolvimento. Ferramentas que oferecem APIs claras, boas documentações e compatibilidade com outras tecnologias serão vistas como mais vantajosas para uso contínuo em ambientes de desenvolvimento reais.

5. Taxa de Falsos Positivos

   Esse critério mede quantas vezes a IA identifica um problema inexistente no código. Uma alta taxa de falsos positivos pode

reduzir a confiança dos desenvolvedores na ferramenta e aumentar o tempo gasto revisando alertas incorretos. Por isso, é essencial que a IA mantenha uma baixa taxa de falsos positivos para ser considerada confiável.

Para avaliar o desempenho das IAs generativas na identificação de vulnerabilidades em códigos de programação, utilizamos um cálculo de porcentagem de sucesso. Esse cálculo considera a quantidade de critérios atendidos pela IA em relação ao total de critérios avaliados.

A porcentagem de sucesso serve como uma métrica objetiva para comparar diferentes IAs. Ela permite avaliar, de forma quantitativa, a eficácia de cada ferramenta em atender aos requisitos estabelecidos, como a detecção de vulnerabilidades, abrangência de tipos de falhas, qualidade das sugestões e integração com ferramentas de desenvolvimento. Dessa forma, facilita a identificação da eficácia das IAs para o contexto de desenvolvimento seguro de software.

2.11 TECNOLOGIAS UTILIZADAS

Para a condução dos testes e análise de resultados deste trabalho, foram utilizadas tecnologias amplamente reconhecidas no desenvolvimento de software seguro, sendo elas: TypeScript, HTML, CSS e SQL. Essas tecnologias foram escolhidas por sua versatilidade e relevância na criação de cenários que simulam vulnerabilidades comuns no ambiente de desenvolvimento real.

O TypeScript foi selecionado por oferecer suporte a tipagem estática, o que contribui para a detecção precoce de erros durante a etapa de desenvolvimento. O HTML e o CSS foram utilizados para criar interfaces web simples, permitindo a inserção de vulnerabilidades como o Cross-Site

Scripting (XSS). O SQL foi aplicado para simular cenários de injeção de comandos, como o SQL Injection, enquanto o uso combinado dessas tecnologias possibilitou a reprodução de vulnerabilidades do tipo buffer overflow em estruturas controladas.

As ferramentas de inteligência artificial analisadas foram o ChatGPT (modelo GPT-4o mini), da OpenAI, e o Gemini (modelo Gemini 1.5), da Google. A escolha dessas ferramentas se justifica por sua ampla adoção no mercado, capacidades avançadas de processamento de linguagem natural e compreensão de código. Ambas as ferramentas foram testadas em situações controladas para verificar sua eficácia na identificação de falhas de segurança e na sugestão de correções.

2.12 METODOLOGIA DOS TESTES

As vulnerabilidades foram propositalmente implementadas em código controlado para avaliar a eficácia das IAs generativas na identificação de falhas de segurança e no oferecimento de sugestões de correção. Não foram deixadas pistas no código e no contexto dos testes que o código havia erros propositais, com o objetivo de não influenciar nas respostas da IA, assim como em um ambiente real. A coleta de métricas levou em consideração a precisão na detecção das vulnerabilidades, a relevância das sugestões de correção, e a capacidade das IAs em lidar com diferentes linguagens e estruturas de código, possibilitando uma análise aprofundada da aplicabilidade dessas ferramentas na segurança de software.

2.12.1 Preparação do ambiente

Para cada teste, foram criados cenários específicos contendo vulnerabilidades intencionais, como XSS, SQL Injection e buffer overflow, de

forma que os códigos apresentados às IAs não tivessem indicações explícitas de erros, simulando um ambiente real de desenvolvimento. Todos os testes seguiram padrões controlados para garantir comparabilidade dos resultados.

2.12.2 Execução dos testes

As vulnerabilidades foram apresentadas às ferramentas de IA por meio de mensagens cuidadosamente elaboradas. As instruções foram enviadas às ferramentas requisitando por uma revisão de código, em seguida foi enviado o código contendo as vulnerabilidades, e as respostas das ferramentas foram analisadas quanto à precisão, abrangência, qualidade das sugestões e taxa de falsos positivos.

3 **CONCLUSÃO**

A análise realizada demonstrou o potencial das IAs generativas como ferramentas de apoio na identificação de problemas em códigos de programação. Apesar das variações de desempenho, a aplicação dessas tecnologias pode contribuir significativamente para o desenvolvimento de software mais seguro e eficiente. Contudo, ainda existem lacunas importantes a serem abordadas, especialmente em relação à abrangência de tipos de vulnerabilidades detectadas, precisão das sugestões de correção e as constantes atualizações de software.

Esses resultados reforçam a necessidade de melhorias contínuas nessas ferramentas para que possam atender plenamente às demandas do mercado e dos desenvolvedores.

REFERÊNCIAS

ALECRIM, E. Stack Overflow proíbe respostas dadas por inteligência artificial do ChatGPT. Disponível em: <https://tecnoblog.net/noticias/stack-overflow-proibe-respostas-dadas-por-inteligencia-artificial-do-chatgpt/>. Acesso em: 16 jun. 2024.

ARNTZ, M., GREGORY, T., ZIERAHN, U. The Risk of Automation for Jobs in OECD Countries: A Comparative Analysis. OECD Social, Employment and Migration Working Papers, 2016. Disponível em: https://www.oecd-ilibrary.org/employment/the-risk-of-automation-for-jobs-in-oecd-countries_5jlz9h56dvq7-en. Acesso em: 20 set. 2024.

BERTUCCI, O.; MARTINEZ, J.; LAFARGE, P.; JULLIEN, J. An Analysis of Machine Learning Vulnerability Detection Models and Training Strategies. Journal of Systems and Software, v. 174, p. 110891, 2021. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0164121220302493>. Acesso em: 23 mai. 2024.

BINNS, R. Fairness in Machine Learning: Lessons from Political Philosophy. 2023. Disponível em: https://www.researchgate.net/publication/356704520_Fairness_in_Machine_Learning. Acesso em: 20 set. 2024.

BRUNDAGE, M., et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. 2020. Disponível em: https://maliciousaireport.com. Acesso em: 24 set. 2024.

BRYNJOLFSSON, E., McAFEE, A. The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company, 2021.
BUENDGEN, R.; SCHNEIDER, M.; TEUBER, L.; STARK, R.; KUPPER, A. Trustworthy AI for Automated Vulnerability Detection. Proceedings of the 2022 IEEE/ACM 44th International Conference on Software Engineering: New Ideas and Emerging Results, p. 21-25, 2022. Disponível em: <https://ieeexplore.ieee.org/document/9783293>. Acesso em: 18 jun. 2024.

CURVELO, R. ChatGPT: tudo o que você precisa saber! Disponível em: <https://br.hubspot.com/blog/marketing/chatgpt>. Acesso em 17 mar. 2024.

EXAME. ChatGPT experimenta queda em tráfego mensal, mas mantém base de usuários. Disponível em:

<https://exame.com/inteligencia-artificial/chatgpt-experimenta-queda-em-trafego-mensal-mas-mantem-base-de-usuarios/>. Acesso em: 24 mar. 2024.

FERNANDES, J., CARVALHO, L., OLIVEIRA, D., OLIVEIRA, E., PEREIRA, F., & LAUSCHNER, T. (2023). Correlação entre complexidade e dificuldade de questões de programação em juízes online. https://sol.sbc.org.br/index.php/educomp/article/view/23879

FERREIRA, R. L. D. M.; DOS SANTOS, A. F. P.; CHOREN, R. Uma Uma Técnica Prognóstica para Desenvolvimento Seguro de Aplicativo Android. Journal on Advances in Theoretical and Applied Informatics, v. 3, n. 1, p. 39, 30 ago. 2017.

GARCIA, M.; SILVEIRA, P.; ROCHA, T. Cybersecurity and AI: A new frontier in software protection. International Journal of Software Security, v. 10, n. 1, p. 45-63, 2021.

GOMES, M., BECKER, L., GESTARO, L., AMARAL, É., & TAROUCO, L. (2015). Um estudo sobre erros em programação - registrando as dificuldades de programadores iniciantes. https://tophotels.com/tecnologia-da-informacao-no-sistema-educacional-do-brasil.pt-br

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. Deep Learning. Cambridge: MIT Press, 2016. Disponível em: <https://www.deeplearningbook.org/>.Acesso em: 22 mai. 2024.

LIMA, C.; CARVALHO, P. AI-Powered Vulnerability Detection: Efficiency and Challenges. Computers & Security, v. 45, p. 90-105, 2022. LIPO, B.; JIN, Y.; YU, F. Deep Learning-Based Vulnerability Detection Using Graph Neural Networks. Proceedings of the 30th USENIX Security Symposium, p. 375-391, 2021. Disponível em: <https://www.usenix.org/conference/usenixsecurity21/presentation/lipo>. Acesso em: 18 jun. 2024.

MAHYARI, A. A Hierarchical Deep Neural Network for Detecting Lines of Codes with Vulnerabilities. Disponível em: <https://arxiv.org/abs/2211.08517>. Acesso em: 23 mar. 2024.

MAHYARI, M. Security Vulnerabilities in Software Systems: Implications for Development Practices. Cybersecurity Journal, v. 6, n. 1, p. 95-108, 2022. Network-based risk assessment of the US crude pipeline infrastructure. Disponível em: <https://www.inderscience.com/info/inarticle.php?artid=59550>. Acesso em: 23 mar. 2024.

PAPERNOT, N., MCDANIEL, P., GOODFELLOW, I. Practical Black-Box Attacks against Machine Learning. Proceedings of the 2018 ACM Conference on Computer and Communications Security. Disponível em: https://dl.acm.org/doi/10.1145/2976749.2978313. Acesso em: 24 set. 2024.

RUNTALENT. ChatGPT: o impacto da Inteligência Artificial no mercado de trabalho. Disponível em: <https://runtalent.it/chatgpt-o-impacto-da-inteligencia-artificial/>. Acesso em: 23 mar. 2024.

SILVA, F.; MARTINS, A.; GOMES, D. Falsos Positivos em Ferramentas de Detecção de Vulnerabilidades Baseadas em IA. Revista de Engenharia de Software, v. 12, n. 4, p. 110-125, 2021. STOICA, I.; SONG, D.; POPA, R. A.; PATTINSON, R.; SHENKER, S.; KOHLER, E. A Berkeley View of Systems Challenges for AI. Technical Report No. UCB/EECS-2017-11, 2017. Disponível em: <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2017/EECS-2017-11.html>. Acesso em: 18 jun. 2024.

TARAFDAR, M.; GUPTA, A.; TUREL, O. Editorial. Information Systems Journal, v. 25, n. 3, p. 161–170, 18 mar. 2015. WHITAKER, M., et al. The Role of AI in Surveillance: Ethical and Societal Considerations. 2022. Disponível em: https://www.apa.org/monitor/2024/04/addressing-equity-ethics-artificial-intelligence. Acesso em: 20 set. 2024.

Sobre o(s) autor(es)
Acadêmico do curso de Ciência da Computação, campus de São Miguel do Oeste. E-mail: pedrovini2002@gmail.com
Professora do Curso de Ciência da Computação, Mestre em Informática pela Universidade Federal do Paraná - UFPR. E-mail: franciele.petry@unoesc.edu.br