XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

MACHINE LEARNING E INTELIGÊNCIA ARTIFICIAL PARA ANÁLISE COMPORTAMENTAL NO ACESSO A SISTEMAS FINANCEIROS: FOCO NA SEGURANÇA DE BANCO DE DADOS

Gustavo de Carvalho Vieira[1]; Matheus Andrade Danno[2]; Leonardo Neto da Cunha[3]; Elaine Cristina Gomes de Moraes[4]; Marco Aurelio Migliorini Antunes[5]
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – gustavovieira0512@gmail.com;
[2]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – matheusdanno@gmail.com;
[3]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – leonardo.cunha@alunos.fibbauru.br;
[4]Professora do Curso de Ciência da Computação – Faculdades Integradas de Bauru – FIB – moraes.e@gmail.com;
[5]Professor Me. do Curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB - mamantunes@gmail.com

Grupo de trabalho: Ciência da Computação

Palavras-chave: Inteligência artificial, machine learning, análise comportamental, segurança de dados, sistemas financeiros.

Introdução: Com a digitalização dos serviços financeiros, proteger informações sensíveis tornou-se fundamental. A análise comportamental baseada em IA e machine learning permite identificar padrões suspeitos e fraudes em tempo real. Sistemas modernos minimizam falsos positivos e otimizam a experiência do usuário, enquanto a adaptabilidade dos modelos melhora a eficiência ao longo do tempo. Essas ferramentas são essenciais para garantir a confiança nas instituições financeiras, protegendo ativos e reduzindo custos operacionais (Cataldo, 2024).

Objetivos: Este estudo explora o uso de IA e aprendizado de máquina na segurança de bancos de dados financeiros, com foco na detecção de fraudes e mitigação de ameaças. Através da implementação de algoritmos avançados, é possível identificar padrões de comportamento que indicam atividades fraudulentas, permitindo uma resposta rápida e eficaz. O trabalho também analisa como a análise comportamental consegue diferenciar atividades legítimas de suspeitas, sem comprometer a experiência do cliente. Essa abordagem não só melhora a segurança, mas também promove a confiança do usuário nas instituições financeiras, que cada vez mais dependem de tecnologias inovadoras para proteger dados sensíveis. Além disso, a evolução contínua dessas tecnologias sugere que o futuro da segurança financeira será marcado por soluções cada vez mais sofisticadas e adaptativa (Leite; Ribeiro, 2024).

Relevância do Estudo: A IA é essencial para combater ataques sofisticados e proteger dados sensíveis. Sistemas de detecção de anomalias monitoram comportamentos normais e alertam sobre atividades fora do padrão, enquanto sistemas de prevenção bloqueiam transações suspeitas no momento da ocorrência, utilizando análises preditivas e listas negras. Esses mecanismos garantem segurança contínua e preservam a reputação das instituições financeiras, que dependem cada vez mais da confiança dos clientes. Além disso, a integração de IA em processos de segurança cibernética permite uma adaptação constante às novas ameaças, melhorando a eficácia das defesas ao longo do tempo. Dessa forma, a aplicação de tecnologias avançadas de IA não só fortalece a proteção dos dados, mas também contribui para um ambiente financeiro mais seguro e confiável (Segurança [...], 2024a).

Materiais e métodos: Este estudo realiza uma revisão da literatura sobre abordagens de IA e aprendizado de máquina aplicadas à segurança de dados, com foco em algoritmos de detecção de anomalias e redes neurais. Esses modelos são treinados para reconhecer padrões e identificar atividades fraudulentas de forma automatizada e precisa. De acordo com Costa (2024), a utilização de técnicas avançadas de aprendizado de máquina não só melhora a eficiência na detecção de fraudes, mas também minimiza os falsos positivos, proporcionando uma resposta mais ágil e eficaz às ameaças.

Resultados e discussões: Os modelos preditivos analisados aprimoram a segurança, reduzindo falsos positivos e melhorando a experiência do usuário. A capacidade dos algoritmos de se adaptarem a novos padrões fortalece a prevenção contra fraudes, tornando os sistemas mais responsivos às ameaças emergentes. Contudo, é essencial monitorar vieses (biases) nos modelos, pois esses podem comprometer a precisão e a equidade das decisões, exigindo ajustes contínuos. A manutenção de um processo de revisão regular é fundamental para garantir que os modelos permaneçam justos e eficazes ao longo do tempo. Além disso, a implementação de práticas de transparência e responsabilidade no desenvolvimento dos modelos contribui para a confiança dos usuários e a aceitação das soluções tecnológicas. Ao abordar esses aspectos, as instituições podem maximizar o potencial dos modelos preditivos, assegurando que suas operações não apenas protejam os dados, mas também respeitem os princípios éticos (Segurança [...], 2024).

Conclusão: O uso de IA e aprendizado de máquina na análise comportamental é essencial para fortalecer a segurança dos bancos de dados financeiros. Essas tecnologias permitem a detecção de fraudes em tempo real, a redução de custos e a garantia de uma experiência segura para os clientes. Além disso, o futuro aponta para uma maior integração entre essas soluções e regulamentações cada vez mais rigorosas, o que exigirá das instituições financeiras a adoção de práticas mais robustas de segurança e conformidade. À medida que as ameaças cibernéticas evoluem, a capacidade de adaptar e aprimorar continuamente os algoritmos será fundamental para proteger dados sensíveis. Portanto, investir em inovação tecnológica e treinamento de pessoal se torna imprescindível para enfrentar os desafios do cenário financeiro atual.

Referências

CATALDO, B. Inteligência artificial no combate a fraudes impacta o setor de pagamentos**.** **Instituto Propague**, 2024. Disponível em: https://institutopropague.org/tecnologia-e-dados/o-papel-da-inteligencia-artificial-no-combate-de-fraudes-ameaca-ou-solucao-para-os-pagamentos/. Acesso em: 16 out. 2024.

COSTA, V. **Aplicação de machine learning na identificação de fraudes financeiras.** Disponível em: https://www.dio.me/articles/aplicacao-de-machine-learning-na-identificacao-de-fraudes-financeiras. Acesso em: 13 out. 2024.

LEITE, E.H.; RIBEIRO, D.F. O papel transformador da inteligência artificial na segurança. **Interface tecnológica**, v. 20, n. 1, 2023. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/1669. Acesso em: 13 out. 2024.

SEGURANÇA financeira na era digital e o avanço da tecnologia. **Cesar**, 2024a. Disponível em: https://www.cesar.org.br/w/seguranca-financeira-na-era-digital-e-o-avanco-da-tecnologia. Acesso em: 14 out. 2024.

SEGURANÇA de dados na era da IA: protegendo informações sensíveis de bancos e fintechs. **O2obots**, 2024. Disponível em: https://www.o2obots.com/blog/seguranca-de-dados-na-era-da-ia-protegendo-informacoes-sensiveis-de-bancos-e-fintechs. Acesso em: 15 out. 2024.

XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

PROJETO INTEGRADOR ENQUANTO ESTRATÉGIA DE ENSINO-APRENDIZAGEM EM CURSOS DE T.I.: ESTUDO DE CASO CURSO DE TECNOLOGIA EM JOGOS DIGITAIS PRIMEIRO SEMESTRE

Fernando Hideki Iga[1]; João Pedro Bicudo Gasperoto[2]; Leonardo Marques Quirino da Silva[3]; Ryan Dias de Oliveira[4]; Marcos Danilo Graciano[5]
[1]Aluno de Jogos Digitais – Faculdade de Tecnologia de Ourinhos – Fatec Ourinhos
fernando.iga@fatec.sp.gov.br;
[2]Aluno de Jogos Digitais – Faculdade de Tecnologia de Ourinhos – Fatec Ourinhos
joao.gasperoto@fatec.sp.gov.br;
[3]Aluno de Jogos Digitais – Faculdade de Tecnologia de Ourinhos – Fatec Ourinhos
leonardo.silva473@fatec.sp.gov.br;
[4]Aluno de Jogos Digitais – Faculdade de Tecnologia de Ourinhos – Fatec Ourinhos
ryan.oliveira5@fatec.sp.gov.br;
[5]Professor do curso de Jogos Digitais – Faculdade de Tecnologia de Ourinhos – Fatec Ourinhos
marcos.graciano@fatec.sp.gov.br.

Grupo de trabalho: Tecnologia em Jogos Digitais

Palavras-chave: projeto integrador, jogos digitais, tecnologia da informação

Introdução: O sistema de Projeto Integrador tem se tornado uma estratégia de grande interesse em diversos cursos superiores das mais diferentes áreas. Segundo o Ministério da Educação (2017), o projeto integrador objetiva que os estudantes desenvolvam, de maneira prática, os conhecimentos adquiridos durante o processo de aprendizagem nas disciplinas do curso. Além disso, estabelece um preparo para aplicação de ideias e resolução de problemas em sua área levando experiência para o mercado de trabalho. Mas, para um primeiro semestre de um curso de tecnologia, como deve ser o desenvolvimento deste projeto? Para alunos recém-chegados ao ambiente acadêmico, alguma adaptação deve ser feita para que os mesmos obtenham sucesso na execução de seus trabalhos? Mais especificamente, no caso dos alunos do curso de Tecnologia em Jogos Digitais, necessitando de múltiplos talentos (desenho, programação, desenvolvimento de áudio, dentre outros), como proceder?

Objetivos: O objetivo principal desta pesquisa é apresentar como funciona o desenvolvimento de um Projeto Integrador no contexto do curso de Tecnologia em Jogos Digitais para alunos do primeiro semestre.

Relevância do Estudo: O projeto integrador é de extrema valia tanto para a instituição de ensino quanto para os alunos. Enquanto instituição de ensino, os coordenadores e direção podem apresentar para a comunidade interna e externa os resultados das pesquisas desenvolvidas, ou seja, soluções reais para problemas da vida cotidiana, demonstrando o quanto se produz dentro do seu espaço. Já para os alunos, a possibilidade de ver os conteúdos estudados sendo aplicados e gerando soluções reais também os cativam e os faz repensar algum pensamento de abandono do curso ou falta de visão de aplicabilidade prática das disciplinas. Na visão de Santos e Barra (2012) e Salvador e Toassi (2013), o PI aprimora o currículo e trabalho em equipe dos estudantes, aperfeiçoando suas habilidades sociais e planejamento sobre situações problemas das suas áreas de estudos. Também, com benefício na área, não só profissional, mas científica e para docentes e servidores envolvidos nessa dinâmica. De acordo com o Projeto Pedagógico do curso de Jogos Digitais, Fatec (2019) as matérias que devem ser contempladas são: Princípios de Jogos Digitais, Arte Digital I, Engine de Jogos I, Programação, Português I, Inglês I, Matemática Discreta e Metodologia da Pesquisa Científico-Tecnológica.

Materiais e métodos: O Projeto Integrador, no caso do primeiro semestre do curso de Jogos Digitais da Fatec Ourinhos, exige que os alunos produzam um jogo utilizando o *software* Piskel (para a produção de cenários, itens e personagens em pixel art), a engine Construct 3 (para a programação do game) e permite o uso de áudios gratuitos ou produzidos, tudo acompanhado por um professor orientador não deixando que nenhuma questão ética ou legal seja comprometida. Cada grupo deve conter, no máximo, 5 alunos. Um tema é repassado aos alunos que devem desenvolver o produto em volta desse contexto. No caso da pesquisa apresentada, o tema era *Contexto Empresarial*.

Resultados e discussões: Com base em Fernandes et. al. (2009), o *brainstorming* é uma parte do projeto de um jogo que agrupa as metas do jogo, objetivo, estilos e tudo com que esse produto estará relacionado. Dentre as ideias apresentadas, decidiu-se que o jogo se passaria ao redor de um alienígena estagiário que precisaria cumprir as tarefas designadas pelo chefe. No roteiro produzido pelos alunos, tudo que deveria constar no jogo foi registrado detalhadamente, desde cada posição de cenários até quais sonorização e diálogos. Para a parte visual do produto, primeiramente, todos os elementos foram planejados em papel quadriculado para melhor visualização do ambiente e suas proporções. Após, foram feitas *pixels arts* na ferramenta *Piskel*. Já a programação aconteceu na *engine Construct 3.* Na parte de sonorização, a ferramenta utilizada foi o *Linux MultiMedia Studio (*LMMS). Após todas as etapas do jogo finalizadas foram realizados testes em busca de erros e *bugs*. Por fim, o jogo foi publicado no site *itch.io* com o nome "*Trainee´s Life*".

Conclusão: Sendo assim, constata-se o quanto o projeto integrador amplifica, fortalece e favorece o aprendizado dos discentes da área tecnológica, principalmente, em Jogos Digitais. Dessa maneira, os alunos, ao saírem da faculdade terão experiências de aplicação das disciplinas aprendidas ao longo de todo curso e habilidades fortalecidas de como agrupar diferentes conteúdos em um único projeto. Além disso, questões como trabalho em equipe, comunicação e a busca por conhecimento autônomo foram cruciais para cumprir as demandas. Com isso, o estudante chegará ao mundo do trabalho muito mais preparado e qualificado.

Referências

BRASIL. Ministério da Educação. **Projeto integrador:** orientações complementares. Bahia, 2017. Disponível em: https://www.ifbaiano.edu.br/unidades/lapa/files/2015/11/projeto-integrador.pdf. Acesso em: 17 de mar. de 2024.

FATEC, Faculdade de Tecnologia de Ourinhos, **Projeto pedagógico do curso superior de tecnologia em jogos digitais**. 2019. Disponível em: https://www.fatecourinhos.edu.br/cursos/jogos/PP_JOGOS.PDF. Acesso em: 17 de mar. de 2024.

FERNANDES, Anita Maria da Rocha; et. al. **Jogos Eletrônicos**: mapeando novas perspectivas. Florianópolis: Visual Books, 2009.

SALVADOR, Antonio Ricardo; TOASSI, Andresa Jaqueline. Projeto integrador: uma ferramenta de ensino-aprendizagem em cursos técnicos. **Revista E-Tech: Tecnologias para Competitividade Industrial - ISSN - 1983-1838**, p. 69–102, 25 abr. 2013.

SANTOS, Maria Célia Calmon; BARRA, Sérgio Rodrigues. O projeto integrador como ferramenta de construção de habilidades e competências no ensino de engenharia e tecnologia. In: CONGRESSO BRASILEIRO DE EDUCAÇÃO EM ENGENHARIA, 40, 2012, Belém: Abenge. *Artigos…* Belém: Abenge, 2012, p. 1 - 10. Disponível em: https://www.abenge.org.br/cobenge/legado/arquivos/7/artigos/104305.pdf. Acesso em: 6 de maio de 2024.

XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

INTEGRANDO CHAOS ENGINEERING À SEGURANÇA DA INFORMAÇÃO: UM NOVO PARADIGMA PARA MITIGAÇÃO DE RISCOS

Murilo Storti Irani[1]; Pedro Augusto de Oliveira[2]; Ronaldo César Dametto[3];
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – muriloirani@gmail.com;
[2]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – pedro.oliveira.cc01@gmail.com;
[3]Professor Coordenador do Curso de Ciência da Computação – Faculdades Integradas de Bauru – FIB – ronaldo.dametto@fibbauru.br.

Grupo de trabalho: Ciência da Computação

Palavras-chave: Proteção de Dados, Engenharia do Caos, OWASP, Pequenos Negócios.

Introdução: O paradigma da segurança cibernética evolui com a ascensão da interconectividade global, que transforma redes e sistemas em pontos críticos de vulnerabilidade (NAKAMURA, 2003). Para pequenas empresas, cujas infraestruturas frequentemente carecem da robustez e dos recursos de grandes corporações, o impacto de falhas de segurança é desproporcional. A Engenharia do Caos, um conceito derivado da análise de falhas em sistemas complexos, emerge como uma abordagem revolucionária na proteção cibernética (BASIRI, A. et al, 2016). Não apenas prevendo eventos adversos, mas intencionalmente criando-os, ela desafia o estado da arte da segurança digital ao submeter sistemas à turbulência controlada. Este estudo propõe a aplicação dessa técnica em conjunto com as diretrizes Open Web Application Security Project (OWASP Foundation), redefinindo as práticas de segurança em pequenos negócios ao transformar fragilidades em oportunidades de fortalecimento estrutural. Nossa abordagem oferece uma solução disruptiva ao capacitar pequenos empreendedores com uma metodologia sofisticada e acessível para enfrentar a crescente sofisticação das ameaças cibernéticas.

Objetivos: Este estudo visa integrar as diretrizes de análise da Engenharia do Caos como ferramenta de resiliência digital, desafiando a visão tradicional da segurança da informação (SIMONSSON et al., 2019). O objetivo é criar um relatório das inserções e respectivas falhas encontradas em sistemas, somada às diretrizes de OWASP, proporcionando não apenas detecção de vulnerabilidades, mas a construção ativa de um ecossistema digital mais robusto, desenvolvendo uma infraestrutura de software web que possa ser acessada por qualquer usuário, que não necessariamente tenha conhecimento técnico na área de segurança, e possa replicar em infraestruturas menores, testando aplicações on-line, rastreando os domínios e subdomínios, identificando falhas e levando resiliência às empresas que, muitas vezes, estão à margem das tecnologias de ponta, sem que isso implique em custos proibitivos ou em complexidade operacional insustentável.

Relevância do Estudo: Em um cenário de hiperconectividade, a segurança cibernética deixa de ser uma simples camada de proteção, e sim um agente fundamental para a continuidade e inovação de negócios. Pequenas empresas, que historicamente sofrem com ataques cibernéticos devido à falta de investimentos robustos em segurança, encontram na Engenharia do Caos um ponto de inflexão (COMPTON, 2019). Ao contrário de abordagens que dependem de respostas reativas a ataques, a Engenharia do Caos antecipa o inesperado, promovendo a evolução dos sistemas através da simulação de falhas reais. Esta proposta é inovadora por não depender de uma infraestrutura robusta, podendo ser aplicada em ambientes leves, comuns às pequenas empresas. A relevância, portanto, vai além da mitigação de riscos: ela reside na transformação de vulnerabilidades em motores de crescimento resiliente.

ISSN 2358-6044
2024

Materiais e métodos: O estudo foi baseado no desenvolvimento de uma plataforma que integra os conceitos de Engenharia do Caos e OWASP em um ambiente de simulação de ataques. A implementação foi realizada utilizando a linguagem Python para automatização. O sistema foi desenhado para realizar inserções controladas de varreduras em domínios e subdomínios de sistemas web, prevendo interrupções de rede e simulações de falhas de serviço. As falhas identificadas, foram estudas de acordo com o ciclo de Chaos Engineering, que envolve a formulação de hipóteses sobre o estado estável dos sistemas, seguido da alternância entre cenários controlados e de produção. Paralelamente, a ferramenta realizou varreduras de vulnerabilidades baseadas no OWASP, identificando fraquezas como Injeção SQL (SQL Injection), Controle de Acesso Quebrado (Broken Access Control) e Configurações Incorretas de Segurança (COSTA, 2017). Cada teste foi monitorado em tempo real, com métricas de resiliência como tempo de recuperação e manutenção de integridade dos dados. A plataforma gerou relatórios com as vulnerabilidades detectadas e a resposta dos sistemas às falhas simuladas, priorizando insights que guiam pequenas empresas na implementação de soluções práticas de defesa.

Resultados e discussões: Os testes realizados demonstraram uma nova capacidade de identificação de vulnerabilidades em sistemas de pequeno porte. Utilizamos a duração de cada requisição como métrica para medir a resiliência dos sites, identificando vulnerabilidades como XSS (Cross-Site Scripting), SQL Injection (Injeção de SQL) e Open Redirect (Redirecionamento Aberto) (OWASP Foundation). Ao aplicar essa metodologia em sites com vulnerabilidades conhecidas, como os testados no Acunetix, observamos que a ferramenta detectou as falhas corretamente. Esses resultados foram validados manualmente, confirmando a eficácia da abordagem automatizada. Esse modelo de segurança preditiva permite uma resiliência que, em vez de responder a incidentes passados, antecipa cenários futuros, criando sistemas proativos.

Conclusão: A integração da Engenharia do Caos com os padrões OWASP em pequenos negócios representa uma transformação na segurança da informação. Oferecendo uma ferramenta estratégica poderosa, convertendo vulnerabilidades em vantagens competitivas, assegurando a continuidade e a evolução segura no ambiente digital. Este estudo propõe uma solução escalável e acessível que redefine a resiliência cibernética.

Referências:

BASIRI, A. et al. **Chaos engineering**. IEEE Software, IEEE, v. 33, n. 3, p. 35–41, 2016.

COMPTON, R. A**. Distributed denial-of-service attack mitigation with reduced latency**. [S.l.]: Google Patents, 2019. US Patent App. 15/880,522.

COSTA, J. V. **Análise de vulnerabilidades de segurança em portais de governos eletrônicos**. 2017. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) Universidade Federal de Uberlândia, Brazil.

NAKAMURA, EMILIO TISSATO. **SEGURANÇA DE REDES EM AMBIENTES COOPERATIVOS**. Berkeley 2003.

OWASP FOUNDATION. Disponível em: https://owasp.org

SIMONSSON, J. et al. **Observability and chaos engineering on system calls for containerized applications in docker**. CoRR, abs/1907.13039, 2019. Disponível em: <http://arxiv.org/abs/1907.13039>.

XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

DEEPDREAM

Lucas Henrique de Lima Antonio[1]; Pamela Taga[2]; Rodolfo Ipolito Meneguette[3]; Antonio Carlos Sementille[4].
[1]Mestrando– Universidade Estadual Paulista – UNESP – lucas-henrique.antonio@unesp.br;
[2]Mestrando– Universidade Estadual Paulista – UNESP – pamela.taga@nunesp.br;
[3]Professor Doutor – Universidade de São Paulo – USP – meneguette@icmc.usp.br;
[4]Professor Doutor – Universidade Estadual Paulista – UNESP – antonio.sementille@unesp.br.

Grupo de trabalho: Ciência da Computação

Palavras-chave: Sonho, Imagem, Python, Inteligência Artificial, Rede Neural Convolucional.

Introdução: Ao longo do tempo, o campo da visão computacional e do processamento de imagens evoluiu significativamente, explorando novos horizontes artísticos e científicos. A técnica DeepDream, desenvolvida pelos engenheiros da Google em 2015, é um exemplo notável dessa evolução. Utilizando redes neurais convolucionais (CNNs), o DeepDream foi criado com o objetivo de visualizar as camadas internas das CNNs e entender como essas redes processam e reconhecem imagens. De acordo com LaFrance (2015), "Quando uma coleção de cérebros artificiais no Google começou a gerar imagens psicodélicas a partir de fotos aparentemente comuns, os engenheiros compararam o que viam a paisagens de sonho. Eles nomearam sua técnica de geração de imagens de Inceptionism e chamaram o código usado para impulsioná-la de DeepDream" (tradução nossa).

Objetivos: Explorar e destacar a relevância do DeepDream no contexto da visão computacional, expondo seus princípios de funcionamento e seu impacto na criação artística e na pesquisa científica, almejando inspirar desenvolvedores e pesquisadores a incorporar o DeepDream em suas práticas.

Relevância do Estudo: O estudo do DeepDream possui uma relevância multifacetada que se estende por várias disciplinas e áreas de aplicação. No campo da arte digital por exemplo, muitos artistas usam o DeepDream e suas variantes para criar obras visualmente intrigantes e surreais, aplicando o algoritmo a imagens existentes ou utilizando as imagens geradas como ponto de partida para criar peças originais. Como menciona Hayes (2015), "Algumas semanas após a primeira postagem no blog, Mordvintsev, Tyka e Olah publicaram seu programa DeepDream, tornando-o gratuito para qualquer pessoa baixar e executar. Outros começaram imediatamente a experimentar com os algoritmos, e vários sites agora oferecem o DeepDream como um serviço" (tradução nossa).

Materiais e métodos: O trabalho, de natureza teórica, é resultado de pesquisa bibliográfica, utilizando-se da análise da visão de alguns autores contidas na literatura especializada. Conforme Cervo e Bervian (2012) argumentam, essa pesquisa visa explicar as vantagens tendo como base as contribuições de outros autores considerados relevantes, podendo ser realizada independentemente ou como parte de pesquisa descritiva ou experimental.

Resultados e discussões: O DeepDream é um algorítmo notável por sua eficiência em reconhecer padrões em imagens. Este utiliza essa capacidade para identificar e amplificar padrões específicos, empregando um método de otimização iterativo. Segundo Mordvintsev, Olah e Tyka (2015), “treinamos uma rede neural artificial mostrando a ela milhões de exemplos de treinamento e ajustamos gradualmente os parâmetros da rede até que ela forneça as classificações que desejamos” (tradução nossa). Durante esse processo, a imagem de entrada é modificada com o objetivo de maximizar a ativação de unidades específicas da rede neural. Essa otimização ocorre em cada camada da CNN, resultando em imagens que exibem

padrões visualmente interessantes e complexos. Os usuários têm a possibilidade de controlar diversos parâmetros durante a execução do DeepDream, como a escala dos padrões gerados e a interpretação do computador por meio de diversas camadas de compreensão, sendo as primeiras direcionadas ao reconhecimento de coisas simples, e as últimas utilizadas para o reconhecimento de padrões complexos (TECHTUDO, 2020). À medida que o algoritmo altera a imagem, os usuários recebem feedback visual em tempo real sobre as mudanças resultantes, permitindo ajustes e iterações ao longo do processo. lém de sua aplicação artística, o DeepDream é utilizado no contexto do melhoramento de imagens, destacando características específicas ou realçando detalhes que podem não ser facilmente perceptíveis na imagem original. No âmbito da pesquisa em inteligência artificial, essa técnica oferece uma poderosa ferramenta para entender melhor como as redes neurais convolucionais interpretam e reconhecem padrões em dados visuais. Pesquisadores têm explorado o DeepDream para analisar conjuntos de dados científicos, como imagens astronômicas ou microscópicas, ajudando a identificar padrões e características importantes, e facilitando a análise e interpretação desses dados.

Conclusão: Em resumo, o DeepDream se destaca como uma ferramenta inovadora na exploração visual e na análise de padrões, utilizando redes neurais convolucionais para gerar imagens surpreendentes. Embora exija condições específicas para seu uso eficaz, como a qualidade da imagem e a escolha precisa das camadas de ativação, que não foram mencionadas neste artigo, e enfrente desafios como a necessidade de processamento intensivo, o DeepDream continua a ser uma valiosa contribuição para essas áreas.

Referências:

CERVO, A. L.; BERVIAN, A. **Metodologia Científica. 5. ed.** São Paulo: Prentice Hall, 2012.

HAYES, Brian. **Computer Vision and Computer Hallucinations**. Disponível em: https://www.americanscientist.org/article/computer-vision-and-computer-hallucinations. Acesso em: 01 out. 2024.

LAFRANCE, Adrienne. **If You Give a Robot Acid**. Disponível em: https://www.theatlantic.com/technology/archive/2015/09/robots-hallucinate-dream/403498/. Acesso em: 01 out. 2024.

MORDVINTSEV, Alexander; OLAH, Christopher; TYKA, Mike. **Incepcionismo**: Aprofundando-se nas Redes Neurais. Disponível em: https://ai.googleblog.com/2015/06/inceptionism-going-deeper-into-neural.html. Acesso em: 01 out. 2024.

TECHTUDO. Google Deep Dream: tecnologia gera imagens com resultados psicodélicos. Disponível em: <https://www.techtudo.com.br/noticias/2015/07/google-deep-dream-tecnologia-gera-imagens-com-resultados-psicodelicos.ghtml>. Acesso em: 2 out. 2024.

XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

NEURÔNIOS DE SILÍCIO: UMA INTRODUÇÃO AOS FUNDAMENTOS E APLICAÇÕES DA COMPUTAÇÃO NEUROMÓRFICA

Lucas Henrique de Lima Antonio[1]; Rodolfo Ipolito Meneguette[2]
Mestrando– Universidade Estadual Paulista – UNESP – lucas-henrique.antonio@unesp.br;
[2]Professor Doutor – Universidade de São Paulo – USP – meneguette@icmc.usp.br.

Grupo de trabalho: Ciência da Computação

Palavras-chave: Cérebro, Computação, Inteligência Artificial, Computação Neuromórfica.

Introdução: A computação neuromórfica é uma área da tecnologia que se inspira na neurobiologia para desenvolver circuitos eletrônicos mais eficientes, imitando a arquitetura do cérebro humano. Criada por Carver Mead, na década de 1980, essa abordagem busca criar computadores que se comportem de maneira semelhante ao cérebro. Conforme relata Mead (2020), “a engenharia neuromórfica visa criar hardware de computação que imita sistemas nervosos biológicos, e espera-se que desempenhe um papel chave na próxima era do desenvolvimento de hardware” (tradução nossa).
Essa tecnologia utiliza sistemas de integração em larga escala, chamados VLSI (Very Large Scale Integration), que incorporam circuitos analógicos projetados para imitar as arquiteturas neurobiológicas do sistema nervoso. O termo "neuromórfico" refere-se a esses sistemas, que podem incluir componentes analógicos, digitais ou uma combinação de ambos. A computação neuromórfica também pode envolver software que implementa modelos neurais, com aplicações em percepção, controle motor e integração multimodal.

Objetivos: Apresentar a computação neuromórfica, explicando seu funcionamento e seus fundamentos. Além disso, busca-se explorar as principais diferenças entre essa abordagem inovadora e os modelos de computação tradicionais, destacando suas vantagens e desafios

Relevância do Estudo: A relevância do estudo sobre Computação Neuromórfica está nas limitações da computação tradicional, especialmente com o fim da Lei de Moore e do Escalonamento de Dennard. A Lei de Moore, que previa um crescimento contínuo no número de transistores em circuitos integrados, está se aproximando de limites físicos. Da mesma forma, o Escalonamento de Dennard, que relacionava a miniaturização dos transistores à redução do consumo de energia, enfrenta barreiras como o vazamento de corrente e o aumento do calor, dificultando melhorias de desempenho sem aumentar o consumo energético. Nesse contexto de desafios, a Computação Neuromórfica surge como uma alternativa promissora. Como apontado por Schuman et al. (2022), com o fim da Lei de Moore e o término do Escalonamento de Dennard, a comunidade científica busca novas tecnologias para manter o avanço do desempenho computacional.

Materiais e métodos: Este trabalho teórico resulta de uma pesquisa bibliográfica que analisa as perspectivas de diversos autores na literatura especializada para explicar as vantagens da computação neuromórfica, podendo ser feito de forma independente ou como parte de uma pesquisa descritiva ou experimental.

Resultados e discussões: A computação neuromórfica apresenta vantagens significativas em comparação à arquitetura tradicional Von Neumann, destacando-se pela eficiência energética e pelo processamento paralelo. Enquanto a computação convencional enfrenta limitações de energia e latência devido à separação entre unidade de processamento e memória, a abordagem neuromórfica, inspirada na estrutura cerebral, permite uma maior eficiência. Antony S. (2014) observa que chips tradicionais podem consumir milhares ou milhões de vezes mais energia do que um cérebro humano para realizar tarefas similares.

ISSN 2358-6044
2024

Uma característica distintiva dos sistemas neuromórficos é sua capacidade de aprendizado autônomo, que lhes permite ajustar conexões internas com base nos dados recebidos, ao contrário da computação tradicional, que necessita de programação explícita para novas tarefas. Os memristores, fundamentais para essa tecnologia, possibilitam eficiência energética e resistência a falhas. Como menciona Marques (2023), os memristores "lembram" a carga elétrica que passou por eles, mesmo quando desligados, aumentando a eficiência e a durabilidade dos dispositivos. As aplicações da computação neuromórfica são amplas, abrangendo áreas como inteligência artificial (IA), robótica e medicina. Na IA, sistemas neuromórficos permitem aprendizado em tempo real e processamento paralelo de grandes volumes de dados, sendo ideais para análise de tendências e processamento de linguagem natural. Na robótica, eles contribuem para o desenvolvimento de robôs mais autônomos e energeticamente eficientes, enquanto na medicina promovem avanços em diagnósticos e tratamentos, como próteses neurais e interfaces cérebro-máquina (Barreto, 2024). Contudo, a computação neuromórfica ainda enfrenta desafios significativos, especialmente em relação aos altos custos de desenvolvimento e implementação. A criação de circuitos que emulam funções neurais exige conhecimento avançado em neurociência e design de hardware, o que eleva os custos (Marques, 2023). Além disso, a integração desses sistemas com a infraestrutura de TI existente pode demandar adaptações complexas, comprometendo a eficiência inicial.

Conclusão: Assim sendo, a computação neuromórfica surge como uma solução promissora para as limitações da computação tradicional, oferecendo melhorias em eficiência energética e processamento paralelo, inspirada no cérebro humano. Contudo, os altos custos de desenvolvimento e a complexa integração com tecnologias existentes dificultam sua adoção em larga escala. Para alcançar seu potencial transformador, são necessários investimentos contínuos em pesquisa e desenvolvimento de soluções para superar essas limitações.

Referências:

ANTONY, S. **IBM cracks open a new era of computing with brain-like chip: 4096 cores, 1 million neurons, 5.4 billion transistors.** Disponível em: https://www.extremetech.com/extreme/187612-ibm-cracks-open-a-new-era-of-computing-with-brain-like-chip-4096-cores-1-million-neurons-5-4-billion-transistors. Acesso em: 03 out. 2024.

BARRETO, M. **Inovações nas Aplicações da Computação Neuromórfica.** Disponível em: https://nexusnerd.com.br/inovacoes-nas-aplicacoes-da-computacao-neuromorfica/. Acesso em: 03 out. 2024

MARQUES, E. J. **O que é um Memristor? Como funciona, Vantagens e Aplicações!** Disponível em: https://www.fvml.com.br/2023/04/o-que-e-um-memristor-como-funciona.html. Acesso em: 03 out. 2024.

MEAD, C. **How we created neuromorphic engineering.** Nature Electronics, v. 3, p. 434-435, 2020.

SCHUMAN, C. D.; KULKARNI, S. R.; PARSA, M. et al. **Opportunities for neuromorphic computing algorithms and applications.** Nature Computational Science, v. 2, p. 10-19, 2022.

XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

USO DAS TÉCNICAS DE DATA AUGMENTATION EM DATASETS DE ÁUDIO PARA TREINAR MODELOS DE RECONHECIMENTO DA FALA EM PYTHON

[1]Marcelo Machado Pereira; [2]Lyan Gabriel Ruiz Morales; [3]Ivan Leal Morales
[1]Cientista de Dados Bauru – Cientista da Computação – FIB - machado.pereira@unesp.br
[2]Aluno do Curso Ciência da Computação - FIB - lyan.grmorales@gmail.com
[3]Ms Professor do Curso de Ciência da Computação – FIB – ilmoralesbr@hotmail.com

Grupo de trabalho: Ciência da Computação

Palavras-chave: técnicas, data, augmentation, datasets, áudio

Introdução: O uso de técnicas para aumentar a quantidade de dados é fundamental para um resultado satisfatório tanto nas etapas de treinamento, validação bem como na de testes, seja com áudios ou qualquer outro tipo de dado não estruturado. O presente estudo tem como objetivo investigar a eficácia das técnicas de Data Augmentation na melhoria do desempenho de modelos de reconhecimento de fala treinados com conjuntos de dados de áudio. Especificamente, exploraremos a aplicação dessas técnicas em um ambiente Python, buscando compreender como a ampliação artificial dos dados pode mitigar problemas comuns em conjuntos de dados limitados e contribuir para a construção de modelos mais robustos e precisos.

Objetivos: Aumentar a quantidade e diversidade dos dados de treinamento além de melhorar a robustez e generalização dos modelos de reconhecimento de fala, tornando possível avaliar o impacto dessas técnicas no desempenho final dos modelos.

Relevância do Estudo: Este estudo é relevante pois busca melhorar a precisão de modelos de reconhecimento de fala através da aplicação de técnicas de Data Augmentation em conjuntos de dados de áudio limitados. Ao aumentar artificialmente a quantidade e diversidade dos dados, o objetivo é tornar os modelos mais robustos e capazes de lidar com diferentes variações da fala humana.

Materiais e métodos: Este trabalho, de abordagem teórica e prática, resultou de uma pesquisa bibliográfica que analisou as opiniões de diferentes autores. Conforme Cervo e Bervian (2012), essa pesquisa busca explicar um problema com base nas contribuições relevantes de outros autores e pode ser conduzida de forma independente ou como parte de uma pesquisa descritiva ou experimental usando programação em Python.

Resultados e discussões: Coletar dados de áudios que possuam um vasto volume, variedade, veracidade e velocidade pode representar um problema que uma das soluções propostas é uma técnica chamada Data Augmentation. Toda modificação feita em um algoritmo com a intenção de reduzir o erro de generalização (mas não o erro de treinamento) é uma técnica de regularização. A técnica de Data Augmentation se encaixa exatamente nesse perfil. (Melo, 2019) O ruído, no contexto do áudio, refere-se a qualquer som indesejado que interfere na clareza e na qualidade de uma gravação ou reprodução sonora. (Lopes, 2024) Intensidade do som é a quantidade de energia que as ondas sonoras transferem, através de uma área, durante o intervalo de tempo de um segundo. Ela é usada para medir o fluxo de energia que é transportado por uma onda sonora. (Helerbrock, 2024) Um pitch é a frequência percebida de um som. Podemos atribuir diferentes valores de notas com base na frequência de um pitch. As alturas são mais frequentemente organizadas em séries de nomes de notas, escalas e melodias, embora possam ser replicadas até um T, alinhando-as com o valor Hertz (Hz) específico da onda sonora.(Brunotts, 2023) Para este estudo foram coletados dados de áudios gravados por diversos usuários do aplicativo Whatsapp que correspondem ao círculo

ISSN 2358-6044
2024

de amizades mais próximo e à partir do áudios originais que foram enviados, aplicou-se as respectivas técnicas de injeção de ruído, alteração do tempo/posição, pitch e velocidade para gerar novos arquivos para compor a base do dataset de treinamento. As transformações nos arquivos foram feitas através da programação em Python usando funções matemáticas e pacotes específicos para áudios como o Librosa. Para expandir ainda mais os testes que foram realizados com os áudios originais, foi proposto realizar combinações entre as quatro técnicas utilizadas no estudo, formando pares de técnicas que geram um novo arquivo, trios de técnicas que geram um outro novo arquivo e até mesmo quartetos das técnicas utilizadas, onde a ordem do que é executado primeiro impacta no resultado final do áudio do arquivo, podendo contribuir ou atrapalhar a base do dataset de treinamento. Para um melhor aproveitamento do estudo foi considerado um Data Augmentation usando apenas uma técnica isolada e as variações de pares de técnicas aplicadas, onde aqui também a ordem de execução também importa no resultado final do áudio do novo arquivo.

Conclusão: Ao aplicar técnicas de Data Augmentation como injeção de ruído, alteração de tempo/posição, pitch e velocidade, observou-se uma melhoria significativa na precisão dos modelos de reconhecimento de fala. Os modelos treinados com dados aumentados demonstraram maior robustez e capacidade de generalização, tornando-os mais aptos a lidar com a diversidade da fala humana em diferentes condições acústicas e linguísticas. Como uma proposta de continuidade do estudo fica proposto a exploração e pesquisa de outros tipos de técnica que não foram abordados neste estudo e que também possam trazer contribuições significativas no processo de Data Augmentation dos dados de áudios de um estudo futuro.

Referências

BRUNOTTS, Kate. **O que é afinação na música?** E-Mastered Blog. Ago/2023. https://emastered.com/pt/blog/what-is-pitch-in-music. Acesso em: Out 2024.

CERVO, A. L.; BERVIAN, A. **Metodologia Científica**. 5. ed. São Paulo: Prentice Hall, 2012.

HELERBROCK, Rafael. **Intensidade do som**. Mundo Educação. Out/2024. https://mundoeducacao.uol.com.br/fisica/velocidade-intensidade-som.htm acessado em Out/2024.

LOPES, Renato. **O que é: ruído(áudio)**. IlustraBrasil. Set/2024. https://ilustrabrasil.com.br/glossario/o-que-e-ruido-audio/ acessado em Out/2024.

MELO, Carlos. **Reduzindo o overfitting com data augmentation**. Sigmoidal. Jun/2019. https://sigmoidal.ai/reduzindo-overfitting-com-data-augmentation/ acessado em Out/2024.

XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

SQL E NOSQL VANTAGENS E DESVANTAGENS

Luan Alves Camargo Marques [1], Marco Aurelio Migliorini Antunes [2]
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – luancamargo.fib@gmail.com;
[2]Professor Me. do Curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB - mamantunes@gmail.com;

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: SQL, NoSQL, Banco de Dados Relacional, Banco de Dados Não Relacional.

Introdução: A escolha do tipo de banco de dados (BD) é um ponto chave para qualquer projeto de software. Os bancos de dados SQL relacionais são frequentemente escolhidos devido à sua robustez e confiabilidade (ELMASRI, 2021). No entanto, com a crescente necessidade de escalabilidade e flexibilidade, os bancos de dados NoSQL vêm ganhando espaço em projetos que lidam com grandes volumes de dados e arquiteturas distribuídas (MONGODB, 2024). Este trabalho descreve as vantagens e desvantagens de ambos os tipos de BDs.

Objetivos: O objetivo deste trabalho é realizar uma análise comparativa entre bancos de dados SQL e NoSQL, destacando suas principais vantagens e desvantagens, a fim de responder à pergunta: "Qual é a melhor opção, SQL ou NoSQL?". A pesquisa fornece uma base para auxiliar desenvolvedores e engenheiros de software na tomada de decisões informadas sobre a escolha da solução mais adequada para seus projetos, conforme suas necessidades específicas (ALMEIDA, 2024).

Relevância do Estudo: Com a necessidade crescente de gerenciar grandes volumes de dados de maneira eficiente, entender as diferenças entre SQL e NoSQL é fundamental para a arquitetura de sistemas. Enquanto o SQL oferece consistência e integridade com seu suporte às propriedades ACID, o NoSQL traz mais flexibilidade e desempenho para arquiteturas de alta escalabilidade, o que torna essa comparação crucial para decisões estratégicas (ARILO, 2011). Essa análise também é relevante porque uma escolha errada pode resultar em problemas de desempenho e custos operacionais elevados (ANDERSON; NICHOLSON, 2024).

Materiais e métodos: Foram analisados artigos, publicações e documentação técnica sobre bancos de dados SQL e NoSQL. As principais características de cada tipo de banco de dados foram comparadas em termos de estrutura, linguagem, consistência, escalabilidade, flexibilidade, desempenho, ferramentas e suporte.

Resultados e discussões: Os bancos de dados SQL, que utilizam uma Structured Query Language (SQL), são baseados em uma estrutura relacional de tabelas e esquemas rígidos que garantem a integridade e consistência dos dados, com suporte às propriedades ACID (MONGODB, 2024). Uma ampla adoção do SQL deve ser robusta, fácil de integração e suporte por parte de grandes fornecedores de computação em nuvem (ALMEIDA, 2024). No entanto, a escalabilidade vertical e a flexibilidade limitada são suas principais características, pois exigem a adição de mais poder de processamento em um único servidor, o que aumenta os custos à medida que o sistema cresce (ANDERSON; NICHOLSON, 2024). Por outro lado, o NoSQL (Not Only SQL) oferece uma variedade de modelos de dados, como chave-valor, documentos, gráficos e colunas, permitindo maior flexibilidade para diferentes tipos de aplicação (MONGODB, 2024). O NoSQL supera o SQL em termos de escalabilidade horizontal, onde novos servidores podem ser aumentados facilmente para lidar com grandes

volumes de dados, o que o torna mais adequado para arquiteturas distribuídas e de alta performance (ALMEIDA, 2024). No entanto, a falta de suporte total às propriedades ACID em muitos bancos NoSQL e a consistência eventual podem ser problemas para aplicações que requerem consistência imediata (ANDERSON; NICHOLSON, 2024). Além disso, a curva de aprendizado para dominar diferentes modelos de NoSQL pode ser mais íngreme, exigindo habilidades específicas dos desenvolvedores. A adoção do NoSQL também pode resultar em custos adicionais de manutenção e operação de ambientes distribuídos. Por isso, a escolha entre SQL e NoSQL deve sempre considerar o equilíbrio entre complexidade e os requisitos de negócio de cada projeto.

Conclusão: A resposta à pergunta “usar SQL ou NoSQL” depende das necessidades específicas de cada projeto. Bancos de dados SQL são ideais para aplicações que exigem transações confiáveis, integridade e consistência de dados, enquanto o NoSQL oferece escalabilidade e flexibilidade para lidar com grandes volumes de dados e desenvolvimento ágil. Avaliar os requisitos de consistência, escalabilidade e flexibilidade é fundamental para determinar se deve-se usar SQL, NoSQL ou uma abordagem híbrida (ARILO, 2011). Além disso, é importante considerar o tempo de resposta desejado, o custo de manutenção e a facilidade de adaptação a futuras mudanças no sistema. Dessa forma, a escolha correta pode otimizar o desempenho do projeto e garantir maior longevidade à solução adotada.

Referências

ALMEIDA, M. **Banco de dados relacionais: conhecendo conceitos, terminologias e ferramentas**. 2024. Disponível em: https ://www .alura .com .br /artigos /banco -dados -relacionais -conceitos -terminologias -ferramentas ?srsltid =AfmBOoowNosO8I2udygpRO5uLIMEWhXUTg5J4RHUJXi2jqVinjv18SNn. Acesso em: 14 out. 2024.

ANDERSON, B.; NICHOLSON, B. **Bancos de dados SQL vs. NoSQL: qual é a diferença?** 2024. Disponível em: https://www.ibm.com / think / topics / sql -vs -nosql . Acesso em: 14 out. 2024.

ARILO. **Bancos de Dados Relacionais**. 2011. Disponível em: https://www.devmedia.com.br/bancos-de-dados-relacionais/20401. Acesso em: 14 out. 2024.

ELMASRI, R.; NAVATHE, S. **Introdução a Sistemas de Bancos de Dados**. 8. ed. São Paulo: Pearson, 2021.

MONGODB. **Entendendo bancos de dados SQL vs NoSQL**. 2024. Disponível em: https://www.mongodb.com / resources / basics /databases /nosql -explained / nosql -vs -sql . Acesso em: 14 out. 2024.

XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

A IMPORTÂNCIA DE UM PROFISSIONAL DE *QUALITY ASSURANCE* DENTRO DE UMA EMPRESA

Julia Almeida Ayub[1], Saulo Henrique de Oliveira Matos[2], Erick Vinicius Vasconcelos[3], Ronaldo César Dametto[4], Elaine Cristina Gomes de Moraes[5]
[1]Aluno de Ciência da Computação– Faculdades Integradas de Bauru – FIB – juliaayub19@gmail.com;
[2]Aluno de Ciência da Computação– Faculdades Integradas de Bauru – FIB – matossaulo.h@gmail.com;
[3]Aluno de Ciência da Computação– Faculdades Integradas de Bauru – FIB – Erickviniciusvas@gmail.com;
[4]Professor do Curso de Ciência da Computação – Faculdades Integradas de Bauru – FIB – rdametto2011@gmail.com;
[5]Professora do Curso de Ciência da Computação – Faculdades Integradas de Bauru – FIB - moraes.e@gmail.com

Grupo de trabalho: CIÊNCIA DA COMPUTAÇÃO

Palavras-chave: Quality Assurance, Qualidade, Automação, Testes.

Introdução: A importância de um profissional de *Quality Assurance* (QA) tem crescido nas empresas devido ao progresso tecnológico e à demanda por produtos de alta qualidade. O controle de qualidade não se limita a testar produtos antes do lançamento, mas é integrado em todas as fases do desenvolvimento para garantir a identificação e resolução de problemas antes que se tornem falhas graves. Com o avanço da automação, o QA colabora para melhorar procedimentos e aperfeiçoar a experiência final do cliente (Descubra [...], 2024).

Objetivos: Este trabalho busca entender e ressaltar o papel essencial do profissional de *Quality Assurance* (QA) nas empresas. O objetivo é mostrar como o QA vai além dos testes finais, sendo responsável por garantir que os produtos estejam livres de falhas ao longo de todo o processo de desenvolvimento. Através da implementação de métodos eficazes, o QA previne problemas futuros, melhora a qualidade dos produtos, reduz custos operacionais e, acima de tudo, ajuda a construir a confiança dos clientes, algo crucial para o sucesso de qualquer empresa.

Relevância do Estudo: Com a crescente necessidade de produtos digitais impecáveis, o papel do QA tem se mostrado crucial. Ele não só melhora a experiência do cliente, como também economiza recursos, evitando que falhas só sejam percebidas após o lançamento de um produto. Este estudo busca destacar como as práticas de QA são indispensáveis para a qualidade final do produto e para o sucesso das empresas no mercado competitivo de hoje.

Materiais e métodos: Para a realização deste trabalho, foi realizada uma pesquisa bibliográfica, que consiste na utilização de fontes bibliográficas, como livros, artigos, publicações periódicas ou, ainda, textos extraídos da internet (Menezes *et al.*, 2019).

Resultados e discussões: De acordo com o estudo, o profissional de QA é de grande relevância para garantir a qualidade dos produtos de tecnologia. *Quality Assurance* pode ser traduzido como “garantia de qualidade” e sua atuação é na checagem dos critérios e métodos ao longo dos processos operacionais, visando garantir a qualidade no desenvolvimento de um produto ou serviço (Quality [...], 2019). QA se refere aos procedimentos para supervisionar as operações internas de modo a garantir a conformidade com os padrões, destacando que ele ajuda a identificar problemas precocemente, reduzindo retrabalhos e custos operacionais. Além disso, o uso da automação de testes é mencionado como uma prática essencial para

aumentar a eficiência e a confiabilidade, sendo crucial para a entrega de produtos em ciclos de desenvolvimento mais rápidos. Por isso, a pressão crescente sobre as empresas para oferecer produtos de alta qualidade justifica a necessidade de um processo robusto de *Quality Assurance.* Adicionalmente, é fundamental assegurar que os produtos estejam prontos para serem lançados no mercado, devido à aceleração dos ciclos de desenvolvimento e à implementação de automação. O QA oferece uma maneira eficaz de diminuir despesas com manutenção e melhora a confiabilidade do produto (Entenda [...], 2023). Nesse sentido, quando se fala em *quality assurance*, há três importantes aspectos a serem considerados: segurança, pois os sistemas devem ser seguros para que não se coloque as informações em risco; desempenho, para que haja uma boa performance, com fluxo rápido e ágil; e controle de custos, a fim de organizar as despesas, que devem ser previsíveis e facilmente gerenciáveis. Com o aumento da concorrência no mercado digital, contar com um bom processo de QA faz toda a diferença para a reputação e o sucesso das empresas (Entenda [...], 2023). Portanto, atualmente é de suma importância a presença de um profissional de QA em uma empresa de tecnologia, para desenvolver projetos, auxiliar os processos e garantir a eficiência (QA [...], 2023).

Conclusão: O profissional de *Quality Assurance* é indispensável para garantir que os produtos e serviços oferecidos pelas empresas atendam às expectativas dos clientes. Sua atuação vai além dos testes, abrangendo a automação, a prevenção de falhas e a melhoria contínua dos processos. Além disso, o QA contribui para a eficiência operacional, ajudando a detectar e resolver problemas antecipadamente, o que economiza tempo e recursos. Empresas que adotam práticas robustas de QA conseguem lançar produtos mais confiáveis, o que aumenta a confiança do cliente e fortalece sua posição no mercado.

Referências

DESCUBRA o que é QA, quais são os benefícios e como implementar. **Blog da Omie**, 2024. Disponível em: https://blog.omie.com.br/descubra-o-que-e-qa-quais-sao-os-beneficios-e-como-implementar/. Acesso em: 15 out. 2024.

ENTENDA a importância do quality assurance para empresas de tecnologia. **Gaea**, 2023. Disponível em: https://gaea.com.br/importancia-do-quality-assurance/. Acesso em: 15 out. 2024.

MENEZES, A. H. N. et al. **Metodologia científica:** teoria e aplicação na educação a distância. Petrolina: Universidade Federal do Vale do São Francisco, 2019.

QA: o que é, o que faz a área de *Quality Assurance* e como implementar na sua empresa. **Totvs,** 2023. Disponível em: https://www.totvs.com/blog/developers/qa/. Acesso em: 17 out. 2024.

QUALITY Assurance: entenda o que é e como aplicar na gestão de TI. **Kalendae**, 2019. Disponível em: https://kalendae.com.br/blog/quality-assurance/. Acesso em: 15 out. 2024.

XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

USO DE NLTK NAS MÚSICAS DE BANDAS DE DEATH METAL PARA ANÁLISE DE SENTIMENTOS COM PROCESSAMENTO DE LINGUAGEM NATURAL

[1]Marcelo Machado Pereira; [2]Lyan Gabriel Ruiz Morales; [3]Ivan Leal Morales
[1]Cientista de Dados Bauru – Cientista da Computação – FIB - machado.pereira@unesp.br
[2]Aluno do Curso Ciência da Computação - FIB - lyan.grmorales@gmail.com
[3]Ms Professor do Curso de Ciência da Computação – FIB – ilmoralesbr@hotmail.com

Grupo de trabalho: Ciência da Computação

Palavras-chave: análise, músicas, bandas, linguagem, sentimentos

Introdução: Death Metal pode não ser um dos gêneros mais fáceis de apresentar para quem está chegando no mundo do metal. Influenciado pelo thrash metal, o "metal da morte" começou fazendo jus ao nome, com andamento acelerado, vocais guturais, blast beats e letras que abordam a morte, horror, violência e anti-religião.(Seagal, 2022)
Sendo assim este gênero musical oferece um terreno fértil para a aplicação de técnicas de processamento de linguagem natural. Este estudo propõe utilizar o NLTK para analisar o sentimento expresso nas letras de bandas de death metal, abrindo novas perspectivas para a compreensão da expressão artística e emocional.

Objetivos: Extrair e quantificar o sentimento presente nas letras de bandas de Death Metal com o uso de análise de sentimentos de forma a identificar padrões emocionais recorrentes, nuances semânticas e, potencialmente, novas dimensões interpretativas para esse gênero musical.

Relevância do Estudo: Este estudo contribui para a interseção entre a musicologia, a ciência da computação e a linguística, oferecendo uma abordagem inovadora para a análise de letras de música e expandindo os limites da análise de sentimentos.

Materiais e métodos: Este trabalho, de abordagem teórica e prática, resultou de uma pesquisa bibliográfica que analisou as opiniões de diferentes autores. Conforme Cervo e Bervian (2012), essa pesquisa busca explicar um problema com base nas contribuições relevantes de outros autores e pode ser conduzida de forma independente ou como parte de uma pesquisa descritiva ou experimental usando programação em Python.

Resultados e discussões: O Natural Language Toolkit (NLTK) é uma biblioteca conhecida de código aberto para processamento de linguagem natural (PLN) em Python. O NLTK é muito usado por pesquisadores, desenvolvedores e cientistas de dados em todo o mundo para desenvolver aplicações de PLN e analisar dados de textos.(Ali, 2024) Análise de Sentimentos, também conhecida como mineração de opinião ou Emotion AI é o processamento da linguagem natural e análise de texto para extrair o conteúdo emocional por trás das palavras.(Vicente, 2023) Após a aplicação, o VADER retorna um dicionário com as pontuações para cada polaridade, elas representam o quanto o texto se encaixa em cada categoria e juntas somam 1. Há também uma pontuação composta que soma todas as três classificações depois de normalizá-las entre -1 e 1. Com as pontuações calculadas, define-se a polaridade da frase, ou seja, se é positiva, negativa ou neutra. Foi definido que para frases com pontuação composta maior ou igual a 0,05, a polaridade é positiva e menor ou igual a-0,05 a polaridade é negativa, caso contrário, a polaridade é neutra.(Lima, 2021) Este estudo usou a letra completa de cinco bandas de Death Metal da Flórida, Estados Unidos, muito conhecidas e de notório saber do público fã de Metal. Os resultados podem ser vistos na tabela abaixo:

ISSN 2358-6044
2024

Banda	Música	Negativo	Neutro	Positivo
Cannibal Corpse	Necropedophile	35.10 %	60.40 %	4.60 %
Deicide	Dead by Dawn	**44.40 %**	52.70 %	2.90 %
Obituary	Cause of Death	38.20 %	61.80 %	**0.00 %**
Death	Scream Bloody Gore	34.00 %	62.10 %	3.90 %
Six Feet Under	The Enemy Inside	14.40 %	74.90 %	**10.70 %**

Como é possível observar a música “Dead by Dawn” foi a que apresentou o maior valor de sentimento negativo entre todas as músicas analisadas. A música “The Enemy Inside” teve o valor mais alto de sentimento positivo entre os testes realizados. O fato curioso do estudo ficou com a música “Cause of Death” que “zerou” o valor de sentimento positivo entre todas as músicas analisadas.

Conclusão: A aplicação do NLTK na análise de sentimentos de letras de Death Metal revelou a predominância de emoções negativas em face das positivas. Essa pesquisa demonstra que a análise de sentimentos por meio do NLTK pode contribuir para uma compreensão mais profunda das nuances semânticas e emocionais presentes nas letras de Death Metal, abrindo novas perspectivas para estudos futuros na intersecção entre música, linguagem e inteligência artificial.

Referências:

ALI, Moez. **Tutorial de análise de sentimentos com nltk para iniciantes**. DataCamp. Ago/2024. Disponível em: https://tinyurl.com/mt748a93. Acesso em Out/2024.

CERVO, A. L.; BERVIAN, A. **Metodologia Científica**. 5. ed. São Paulo: Prentice Hall, 2012.

LIMA, Yasmin Silva Amaro de. **Análise de sentimentos em cenários intensivos em conhecimento**. PUC-RIO. Ago/2021. Disponível em: https://tinyurl.com/45ctpe59. Acesso em Out/2024

SEAGAL, Emanuel. **Death Metal: Um Guia Para Começar A Ouvir O Estilo**. Whiplash. Dez/2022. Disponível em: https://whiplash.net/materias/biografias/347334.html. Acesso em Out/2024.

VICENTE, Eduarda. **Análise de sentimentos, uma aplicação da inteligência artificial que avalia o comportamento do seu público**. Programmers. Out/2023. Disponível em:. https://tinyurl.com/3b63cd7y. Acesso em Out/2024.

XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

GESTÃO DE AUTENTICAÇÃO MULTIFATOR (MFA)

[1]Marcelo Machado Pereira; [2]Lyan Gabriel Ruiz Morales, [2]Ivan Leal Morales,
[1]Bacharel em Ciências da Computação – FIB - machado.pereira@unesp.br
[2]Aluno Ciência da Computação – FIB – drlyanmorales@gmail.com
[2]Me. Professor do Curso de Ciência da Computação – FIB – ilmoralesbr@hotmail.com

Grupo de trabalho: Ciência da Computação

Palavras-chave: Segurança, Identidade, sensíveis, computação em nuvem.

Introdução: A Gestão de Autenticaçao Multifactor (MFA) ou também conhecida como IAM - *Identity and Access Management* é um componente essencial para a segurança digital em organizações de qualquer porte. Com o aumento do volume de dados e a complexidade das infraestruturas de TI, o MFA garante que apenas usuários autorizados acessem os recursos adequados, minimizando riscos de violações de segurança. À medida que as organizações adotam ambientes de trabalho híbridos, computação em nuvem e políticas de trabalho remoto, as práticas de MFA tornam-se ainda mais cruciais para proteger informações sensíveis e manter a conformidade com regulamentações.

Objetivos: Este estudo tem como objetivo explorar as melhores práticas para a implementação eficaz de sistemas de MFA. O foco será em práticas que não apenas garantam a segurança dos dados, mas também proporcionem uma experiência de usuário positiva e escalável. São discutidas as principais estratégias de autenticação, controle de acesso e monitoramento contínuo, além de como a adoção dessas práticas pode mitigar vulnerabilidades e responder a ameaças emergentes.

Relevância do Estudo: A crescente onda de ciberataques e a Lei Geral de Proteção de Dados (LGPD) , impõem um rigoroso controle de identidades e acessos dentro das organizações. Estudos demonstram que falhas de autenticação e credenciais comprometidas estão entre as principais causas de violações de dados. Com isso, a adoção de práticas robustas de MFA é fundamental não apenas para evitar incidentes de segurança, mas também para garantir a conformidade com normas de proteção de dados.

Materiais e métodos: O trabalho, de natureza teórica e prática, é resultado de pesquisa bibliográfica, utilizando-se da análise da opinião de alguns autores contidas na literatura especializada e da elaboração de código com os testes realizados. Conforme Cervo e Bervian (2012), considerando-se que essa pesquisa visa explicar um problema tendo como base as contribuições de outros autores considerados relevantes, podendo ser realizada independentemente ou como parte de pesquisa descritiva ou experimental.

Resultados e discussões: Segundo FEBRABAN (2024), uma identidade é uma representação exclusiva de um usuário, que contenha seu nome, senha, número de identificação ou credenciais biométricos. Uma MFA tem um papel importante para as organizações. A adoção de autenticação multifatorial é uma das principais práticas recomendadas para reforçar a segurança de acessos. Combina-se dois ou mais fatores de autenticação, como senha, biometria ou tokens de hardware. Estudos indicam que a IAM pode reduzir significativamente o risco de acessos não autorizados, sendo eficaz contra-ataques baseados em credenciais roubadas. Para CloudFlare (2024) há verificação da identidade, com múltiplos meios, antes de acesso a aplicativos e banco de dados, estabelecendo uma camada mais consistente na segurança da informação. Organizações que implementaram a MFA notaram uma redução drástica nas tentativas de login maliciosas e maior confiança por parte dos clientes e parceiros comerciais. Outro aspecto crítico é o controle de acesso baseado no

ISSN 2358-6044
2024

princípio do privilégio mínimo. Isso significa que os usuários devem ter apenas os acessos necessários para executar suas funções, limitando a exposição a informações sensíveis. O uso de soluções de MFA que implementam políticas de acesso granulares facilita a aplicação dessa prática, reduzindo o impacto de acessos indevidos em caso de comprometimento de uma conta. Uma gestão eficaz do ciclo de vida de identidade envolve a criação, gerenciamento e remoção de contas de usuários em tempo hábil. Isso é particularmente relevante em organizações com grande rotatividade de funcionários e contratados. A automatização desse processo com MFA reduz a probabilidade de contas órfãs, que podem ser um vetor de ataque. O monitoramento contínuo de acessos e a auditoria regular de privilégios são práticas indispensáveis para identificar comportamentos anômalos e corrigir brechas de segurança. Ferramentas de MFA modernas oferecem recursos de monitoramento em tempo real, facilitando a detecção precoce de tentativas de acesso suspeitas e a geração de alertas. As combinações por MFA podem ser feitas por: senha com token de segurança, biometrias, certificados digitais.

Conclusão: As melhores práticas de Gestão de Acesso e Identidade, quando implementadas corretamente, não apenas fortalecem a segurança de uma organização, mas também garantem conformidade regulatória e otimizam a gestão de usuários. Soluções que envolvem autenticação multifatorial, gestão de ciclo de vida e monitoramento contínuo são pilares fundamentais para qualquer sistema robusto de MFA. À medida que o ambiente digital se torna mais complexo, essas práticas se destacam como fundamentais para manter a segurança e a integridade dos sistemas corporativos.

Referências

CERVO, A. L.; BERVIAN, A. Metodologia Científica. 5. ed. São Paulo: Prentice Hall, 2012.

CLOUDFARE (2024). **O que é Autenticador MultiFator?** Disponível em https://www.cloudflare.com/pt-br/learning/access-management/what-is-multi-factor-authentication/ Acesso out/2024
.
FEBRABAN. **Fundamentos de Gestão de Acesso e Identiidade (IAM).** CYBER ACADEMI. Disponível em https://cyberlabfbb.neolude.com.br/ Acesso out/2024.

LGPD. **Lei Geral de Proteção de Dados (2018).** Disponível em Lei Geral de Proteção de Dados Pessoais (LGPD) — Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome Acesso out/2024

TRF (2022). **MultiFator Autenticação**. Disponível em https://www.trf3.jus.br/imprensa/2023/mfa. Acesso out/2024

XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

ANÁLISE DE VULNERABILIDADE: O USO DO NMAP PELOS TIMES DE CIBER SEGURANÇA

[1]Marcelo Machado Pereira; [2]Lyan Gabriel Ruiz Morales, [2]Ivan Leal Morales,
[1]Bacharel em Ciências da Computação – FIB - machado.pereira@unesp.br
[2]Aluno Ciência da Computação – FIB – drlyanmorales@gmail.com
[3]Me. Professor do Curso de Ciência da Computação – FIB – ilmoralesbr@hotmail.com

Grupo de trabalho: Ciência da Computação

Palavras-chave: Nmap, Red Team, Blue Team, Segurança, Procedimentos.

Introdução: As empresas têm buscado a presença contínua na Internet para realizar todo tipo de transação eletrônica. A implantação de técnicas de defesa é crucial para proteger os ativos computacionais, pois qualquer acesso indevido às informações da empresa pode causar prejuízos operacionais significativos. A proteção da rede de computadores visa identificar, proteger e eliminar ou manter sob controle as tentativas de invasão. Dentro desse contexto, a cibersegurança torna-se um componente essencial, e a colaboração de equipes bem treinadas, como os times Red Team, é vital para a eficácia das estratégias de defesa. A ferramenta NMAP (Network Mapper) colabora para as estratégias de defesa.

Relevância do Estudo: Este estudo demonstra teoricamente que scaneadores são softwares que buscam informações das portas de comunicação na fase de preparação do atacante para a rede da empresa. Além disso, discutimos a importância de ferramentas de defesa e de alertas aos administradores de rede. A cibersegurança não se limita apenas ao uso de tecnologias, mas também requer uma equipe capacitada e consciente dos riscos e das melhores práticas de segurança, que possa interpretar os dados obtidos por ferramentas como o Nmap para identificar e mitigar vulnerabilidades.

Materiais e métodos: O trabalho foi realizado por meio de pesquisa bibliográfica, utilizando-se da opinião de alguns autores. Conforme Cervo; Bervian (2002), a pesquisa bibliográfica visa explicar um problema tendo como base às referências publicadas por outros autores, podendo ser realizada independentemente ou como parte de pesquisa descrita ou experimental.

Resultados e discussões: O Nmap (2024) é uma ferramenta open source amplamente utilizada para varredura de redes e auditoria de segurança. NMAP tem por objetivo descobrir hosts e serviços em uma rede de computadores, identificando portas abertas, serviços ativos, versões de software, e possíveis vulnerabilidades. Os times Red Team desempenham um papel crucial na cibersegurança ao simular ataques reais para identificar vulnerabilidades em sistemas, redes e processos. Usando ferramentas como o Nmap, o Red Team realiza varreduras detalhadas na rede, identificando portas abertas e serviços vulneráveis. Essa abordagem proativa permite que as organizações fortaleçam suas defesas antes que um ataque real aconteça. A interpretação dos resultados obtidos pelo Nmap, feita pelos profissionais do Red Team, são essenciais para identificar potenciais vetores de ataque e sugerir ações e recomendações a fim de preservar os dados das empresas. A colaboração entre os Red Teams e os Blue Teams (responsáveis pela defesa) é fundamental para o aprimoramento contínuo das estratégias de segurança e o aumento da resiliência das organizações frente às ameaças. O escaneamento da rede ocorre pelo reconhecimento das portas de comunicação existentes nos protocolos TCP e UDP. Para Tanenbaum (2003), o TCP/IP é o protocolo padrão das comunicações de internetworks, servindo como transporte de informação entre computadores. TCP é um protocolo confiável e orientado para conexão, e o UDP, que não estabelece conexão e é menos confiável, sendo utilizado para transmissões

ISSN 2358-6044
2024

rápidas como vídeos e voz. O Nmap é uma ferramenta open source amplamente usada em auditorias de segurança, especialmente em varreduras de portas TCP e UDP. Identifica portas abertas ou fechadas, que podem ser exploradas por atacantes caso não estejam devidamente protegidas. NMAP (2024) pode identificar seis estados de conexão: Aberto (*open*): Uma aplicação aceita conexões TCP ou pacotes UDP, Fechado (closed): A porta está acessível, mas não há aplicação ativa, Filtrado (*filtered*): O Nmap não consegue identificar portas abertas devido a filtragens, Não-filtrado (*unfiltered*): A porta está acessível, mas o status (aberta/fechada) não pode ser determinado, Open | *filtered*: Não foi possível determinar se a porta está aberta ou filtrada, *Closed* | *filtered*: O Nmap não conseguiu determinar se a porta está fechada ou filtrada. Portas abertas são um sinal de ausência de um firewall eficaz, fornecendo ao atacante informações essenciais para planejar um ataque. Por exemplo, ao detectar a porta RDP (3389) aberta, o invasor pode identificar um serviço de Terminal Service e a versão do sistema operacional em uso, facilitando o uso de técnicas como ataques de força bruta. Ferramentas de defesa, como Firewalls e Sistemas de Detecção de Intrusões (IDS), são indispensáveis na prevenção de ataques cibernéticos. Moraes (2020) define o firewall como um ponto de controle que atua entre a rede privada e a pública, com a capacidade de bloquear ou aceitar requisições e registrar o tráfego que passa por ele. Funciona como a primeira linha de defesa, restringindo o acesso a portas e serviços críticos, prevenindo possíveis tentativas de invasão. Já o IDS, Moraes (2020), tem a função de detectar varreduras de rede e atividades maliciosas, emitindo alertas e, em alguns casos, atuando de forma automatizada para fechar portas vulneráveis ou até responder à fonte do ataque. A combinação dessas ferramentas com estratégias proativas, como as conduzidas por Red Teams, possibilita uma defesa mais robusta e reativa. O Red Team, ao simular ataques reais e utilizar ferramentas como o Nmap, ajuda a identificar vulnerabilidades em tempo hábil. O time analisa os resultados das varreduras e colaboram com o Blue Team para implementar medidas corretivas antes que uma exploração real ocorra.

Conclusão: O uso de ferramentas como Firewall e IDS oferece aos administradores de rede os alertas necessários para identificar tentativas de invasão, como escaneamentos realizados por softwares como o Nmap. Agir de forma preventiva é sempre mais eficaz do que adotar medidas corretivas após um ataque bem-sucedido. Embora detectar ataques nem sempre seja uma tarefa fácil, os alertas gerados por essas ferramentas, especialmente pelo IDS, podem fornecer os sinais necessários para os administradores tomarem ações preventivas contra invasores, aumentando significativamente a segurança da rede. O trabalho em conjunto e Red Teams e Blue Teams colaborar para uma análise profunda da situação da infraestrutura de redes da empresa, propondo ações, visando minimizar possíveis tentativas de invasão.

Referências:

BETINE.C; **Segurança em Servidores Linux** – Ataque e Defesa. 1. Ed. São Paulo: Novatec, 2016.

CERVO, A. L.; BERVIAN, A. **Metodologia científica**. 5. ed. São Paulo: Prentice Hall, 2002.

FEBRABAN. **Carreiras em CiberSegurança.** CYBER ACADEMI. Disponível em https://cyberlabfbb.neolude.com.br/ Acesso out/2024.

FERNANDES, A. MORAES. **Redes de Computadores: fundamentos**. 8. Ed. São Paulo: Érica, 2020.

NMAP: http://nmap.org/man/pt_BR/man-port-scanning-basics.html. Acesso em 20/10/2024

TANENBAAUM, A: **Redes de Computadores**. 5. Ed. São Paulo: Campus, 2010.

XIX Jornada Científica
Faculdades Integradas de Bauru - FIB
ISSN 2358-6044
2024

COBOTS NA AUTOMAÇÂO INDUSTRIAL: A REVOLUÇÂO DA COLOBORAÇÂO HUMANO-ROBÔ

Matheus Ferreira Lima[1]; Rafaela Caroline Dias[2]; Ítalo Augusto S. R. da Rocha[3]; Ronaldo César Dametto[4]
[1]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB – matheuslima_f@hotmail.com;
[2]Aluna de Ciência da Computação – Faculdades Integradas de Bauru – FIB rafaelacaroldias111@gmail.com;
[3]Aluno de Ciência da Computação – Faculdades Integradas de Bauru – FIB italoet2009@hotmail.com;
[4]Professor do curso de Ciências da Computação – Faculdades Integradas de Bauru – FIB rdametto@uol.com.br

Grupo de trabalho: Ciência da Computação

Palavras-chave: Cobots; automação industrial; robôs colaborativos; colaboração humano-robô; segurança industrial;

Introdução: Nos últimos anos, a automação industrial tem evoluído significativamente com a introdução de robôs colaborativos, conhecidos como cobots. Esses cobots, são desenvolvidos para trabalhar diretamente com seres humanos em ambientes compartilhados, proporcionando maior flexibilidade e segurança em comparação aos robôs industriais convencionais, que normalmente requerem segregação física para garantir a segurança. A integração de cobots com trabalhadores humanos na fabricação traz benefícios e desafios notáveis (VILLANI et al., 2018). Segundo Neves et al. (2024), esses robôs colaborativos não apenas aumentam a eficiência ao unir a adaptabilidade humana à precisão robótica, mas também resultam em uma maior produtividade e redução da carga de trabalho dos operadores. Essa sinergia entre humanos e robôs é fundamental para otimizar processos e garantir um ambiente de trabalho eficiente.

No entanto para se ter um ambiente mais seguro os cobots acabam tendo algumas desvantagens, como redução da capacidade de carga, limitando os cobots a tarefas leves e operar com movimentos mais lentos para prevenir colisões e lesões. Essas medidas ajudam a evitar acidentes como esmagamento, tornando as atividades mais seguras para humanos (ROSENSTRAUCH e KRUGER, 2017).

Objetivos: O objetivo deste artigo é analisar a crescente integração de robôs colaborativos, conhecidos como cobots, na automação industrial e seu impacto nos ambientes de trabalho. A pesquisa busca explorar como a colaboração entre humanos e robôs pode otimizar processos produtivos, aumentar a eficiência e melhorar a segurança nas operações industriais.

Relevância do Estudo: O estudo sobre robôs colaborativos na automação industrial mostra como as indústrias estão se transformando para se tornarem mais eficientes e flexíveis. Com o aumento do uso de cobots, as empresas conseguem aumentar a produtividade ao combinar a capacidade de adaptação dos humanos com a precisão dos robôs, algo muito importante em um mercado que está sempre mudando.

Materiais e métodos: O método utilizado uma pesquisa bibliográfica abrangente. Foram analisados artigos acadêmicos sobre robôs colaborativos na automação industrial. Os materiais foram selecionados com cuidado, levando em conta sua relevância e atualidade, e incluem investigações que discutem os seus benefícios, desvantagens e os desafios da implementação de cobots.

Resultados e discussões: Segundo Silva e Lucato (2021) sobre robôs colaborativos (cobots) indica um impacto positivo na automação industrial, com um aumento significativo na

produtividade e redução do tempo de ciclo das tarefas. Embora apresentem vantagens, os cobots têm limitações, como a menor capacidade de carga e a diminuição da velocidade, o que restringe sua aplicação a tarefas leves. A integração desses robôs com trabalhadores humanos pode enfrentar desafios culturais e de formação, afetando a colaboração efetiva. Contudo, um dos principais benefícios dos cobots é a melhoria da segurança no ambiente de trabalho, resultando em menos acidentes. Em resumo, os robôs colaborativos representam uma inovação valiosa na automação, mas é fundamental abordar os desafios associados à sua implementação (Mukherjee et al., 2024).

Conclusão: Os robôs colaborativos, ou cobots, trouxeram grandes avanços para a automação industrial, combinando a precisão das máquinas com a flexibilidade dos humanos. Apesar de terem limitações, como carregar menos peso e se mover mais devagar, eles aumentam a produtividade e tornam o ambiente de trabalho mais seguro. Para aproveitar todo o potencial dos cobots, as empresas precisam lidar com os desafios de adaptação e treinamento dos funcionários. No geral, os cobots são uma solução promissora que pode transformar a automação industrial, trazendo mais segurança e eficiência.

Referências:

MUKHERJEE, Anshit; BANERJEE, Subhendra N.; DAS, Satadal; GUPTA, A.; SHOME, Arijit. **Cobots. In: Advances in Business Information Systems and Analytics Book Series.** 2024. Disponível em: https://doi.org/10.4018/979-8-3693-3550-5.ch013. Acesso em: 15 out. 2024.

NEVES, Miguel; DUARTE, Laura; NETO, Pedro. **A collaborative robot-assisted manufacturing assembly process.** arXiv preprint, 2024. Disponível em: https://doi.org/10.48550/arxiv.2403.05306. Acesso em: 11 out. 2024.

ROSENSTRAUCH, M. J.; KRUGER, J. **Safe human-robot collaboration-introduction and experiment using ISO/TS 15066**.2017 3rd Int. Conf. Control. Autom. Robot. ICCAR 2017, pp. 740–744, 2017. Disponível em: < https://ieeexplore.ieee.org/document/7942795> Acesso em: 05 out. 2024.

SOARES, R.; LUCATO, A. V. R. ROBÓTICA COLABORATIVA NA INDÚSTRIA 4.0, SUA IMPORTÂNCIA E DESAFIO. **Revista Interface Tecnológica**, *[S. l.]*, v. 18, n. 2, p. 747–759, 2021. DOI: 10.31510/infa.v18i2.1298. Disponível em: https://revista.fatectq.edu.br/interfacetecnologica/article/view/1298. Acesso em: 13 out. 2024.

VILLANI, V.; PINI, F.; LEALI, F.; SECCHI, C. **Survey on human–robot collaboration in industrial settings: safety, intuitive interfaces, and applications.** ***Mechatronics***, v. 55, p. 248-266, 2018.