Levantamento Bibliográfico e Revisão da Literatura sobre Modelos de Detecção de Anomalias em Redes IoT com o Uso de *Machine Learning*

Autores
Phelipe Gomes Correia de Franca[1]
Carlos Hideo Arima [2]

Resumo
A detecção de anomalias em redes de Internet das Coisas (IoT) em ambientes industriais é necessária para prevenir falhas entre equipamentos, reduzir o tempo de inatividade e otimizar a segurança operacional. O aumento no volume e complexidade dos dados dificulta a detecção manual por seres humanos, destacando a importância de técnicas de *machine Learning* (ML). Essas técnicas permitem a automação da detecção, analisando de forma eficiente os dados gerados por sensores e sistemas IoT. Este estudo revisa abordagens de detecção de anomalias utilizando ML em ecossistemas industriais de IoT, avaliando pesquisas publicadas entre 2014 e 2024. Ele apresenta algoritmos como Redes Neurais Convolucionais (CNNs), Redes Gerativas Adversariais Condicionais (cGANs), Random Forest e SVM.

Palavras-chave: Detecção de anomalias. Internet das coisas (IoT). *Machine Learning* (ML). Segurança operacional.

Bibliographic Survey and Literature Review on Anomaly Detection Models in IoT Networks Using Machine Learning

Abstract
Anomaly detection in Internet of Things (IoT) networks in industrial environments is essential to prevent equipment failures, reduce downtime, and optimize operational safety. The increasing volume and complexity of data make manual detection by humans challenging, highlighting the importance of machine Learning (ML) techniques. These techniques enable automated detection by efficiently analyzing data generated by IoT sensors and systems. This study reviews anomaly detection approaches using ML in industrial IoT ecosystems, evaluating research published between 2014 and 2024. It presents algorithms such as Convolutional Neural Networks (CNNs), Conditional Generative Adversarial Networks (cGANs), Random Forest, and SVM.

Keywords*: Anomaly detection. Internet of things (IoT). Machine Learning (ML). Operational safety.*

INTRODUÇÃO

Nos últimos anos, a automação de tarefas anteriormente realizadas por seres humanos tem sido impulsionada pelo avanço de novas tecnologias, especialmente no contexto da indústria 4.0. Esse conceito, que integra sistemas inteligentes e conectados, tem permitido o monitoramento em tempo real das linhas de produção, possibilitando a detecção de problemas

[1] Mestrando no Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos no Centro Estadual de Educação Tecnológica Paula Souza – CEETEPS. E-mail: posgraduacao@cps.sp.gov.br
[2] Doutorado em Controladoria e Contabilidade pela Universidade de São Paulo – FEA-USP e Docente no Programa de Mestrado Profissional em Gestão e Tecnologia em Sistemas Produtivos do Centro Estadual de Educação Tecnológica Paula Souza – CEETEPS. Orcid: 0000-0001-7922-0943

que poderiam levar a atrasos e à diminuição da produtividade. Interrupções em processos industriais, muitas vezes decorrentes de anomalias como falhas de equipamento ou mudanças nas condições operacionais, impactam negativamente a eficiência das empresas, podendo gerar perdas econômicas.

Com a crescente adoção de ecossistemas de Internet das Coisas (IoT) nas indústrias, tornou-se possível coletar grandes volumes de dados de máquinas industriais por meio de sensores que monitoram variáveis como temperatura, pressão, vibração e consumo de energia. Essa riqueza de dados oferece uma oportunidade para que especialistas possam acompanhar o estado das máquinas em tempo real, diagnosticando problemas antes que eles causem interrupções no processo produtivo. No entanto, o grande volume e a complexidade desses dados tornam a detecção manual de anomalias impraticável, aumentando a necessidade de técnicas automáticas e eficientes.

Neste cenário, algoritmos de aprendizado de máquina (ML) emergem como uma das soluções promissoras para automatizar a detecção de anomalias (DA), analisando e interpretando padrões nos dados gerados. Diversas abordagens de ML vêm sendo aplicadas para identificar comportamentos inesperados e anômalos em redes IoT industriais, cada uma com suas próprias vantagens e limitações, dependendo da natureza dos dados e das particularidades da aplicação industrial.

1.1 Objetivo

O trabalho propõe investigar como a adoção de métodos e algoritmos de *machine Learning*, aplicados na detecção de ameaças em redes IoT, enfrenta desafios relacionados à eficácia, precisão e adaptação a cenários dinâmicos e imprevisíveis, levantando a questão: os algoritmos de *machine Learning* são eficazes na detecção de ameaças emergentes? Este estudo busca revisar as estratégias de aprendizado de máquina mais utilizadas na detecção de anomalias em redes IoT industriais, com foco na aplicação de técnicas de ML, explorando suas potencialidades e os desafios futuros para aumentar a segurança e a eficiência no monitoramento de redes industriais. Os objetivos específicos deste estudo são:

1. Realizar uma busca em periódicos para obter metadados relevantes para análise.
2. Conduzir um estudo bibliométrico utilizando Bibliometrix e Biblioshiny, agregando dados em um arquivo .xlsx para facilitar a análise e seleção de artigos.
3. Identificar e destacar os principais aspectos da aplicação de ML na detecção de anomalias em redes IoT.

2 REFERENCIAL TEÓRICO

A Internet das Coisas (IoT) representa uma revolução no campo da tecnologia, caracterizada pela interconexão de sensores e dispositivos de computação que se comunicam entre si para resolver problemas e fornecer novos serviços. Essa rede de sensores em constante comunicação tem sido crucial na transformação digital de diversas indústrias e na oferta de soluções inovadoras para desafios complexos (Ullah; Mahmoud, 2021). No entanto, o crescimento exponencial do uso de dispositivos IoT também trouxe à tona novas vulnerabilidades, ampliando a superfície de ataque para cibercriminosos. Isso gerou uma demanda por pesquisas voltadas à proteção dessas redes, onde a detecção de ameaças se tornou um fator necessário para garantir o funcionamento adequado e seguro da infraestrutura IoT.

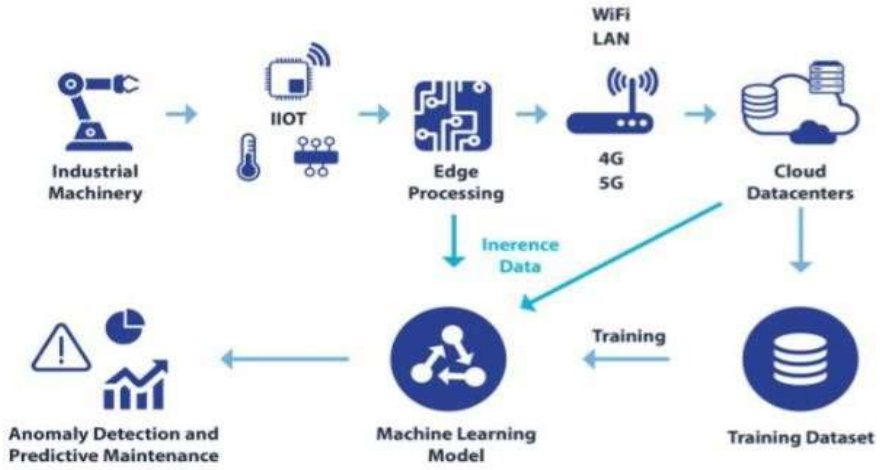
Governos ao redor do mundo têm reconhecido a importância de investir em infraestrutura de Tecnologias de Informação e Comunicação (TIC) para melhorar a gestão. Segundo Ullah e Mahmoud (2021), essas iniciativas governamentais são fundamentais para integrar e fortalecer as redes IoT dentro do contexto da gestão pública, garantindo que a infraestrutura esteja preparada para suportar a crescente demanda e complexidade dos serviços baseados em IoT.

Em ambientes inteligentes habilitados para IoT, três princípios críticos de segurança são essenciais: confidencialidade, integridade e disponibilidade. A confidencialidade garante que as informações trocadas entre os dispositivos sejam acessíveis apenas por entidades autorizadas; a integridade assegura que os dados não sejam alterados durante o trânsito; e a disponibilidade garante que os serviços estejam sempre acessíveis para os usuários legítimos (Ullah; Mahmoud, 2021). A detecção de anomalias desempenha um papel vital na manutenção desses princípios, atuando como uma barreira contra atividades maliciosas que possam comprometer a segurança e a eficácia das redes IoT.

As abordagens baseadas em aprendizado de máquina têm se mostrado promissoras, pois conseguem identificar padrões complexos de anomalias que métodos tradicionais poderiam não detectar. Ullah; Mahmoud (2021) enfatizam que a precisão na detecção de anomalias é crítica para manter a confiança nos serviços IoT, uma vez que dados comprometidos podem levar a decisões equivocadas e comprometer toda a cadeia de valor. O autor (Chevtchenko; Sérgio F., et al.,2023) destaca um fluxo de monitoramento em ambientes industriais, onde dados de sensores IoT são processados localmente e transmitidos para a nuvem. Modelos de *machine Learning* são treinados com esses dados para identificar anomalias e realizar manutenção preditiva. O processo permite a detecção antecipada de falhas,

otimizando a eficiência operacional conforme exemplifica na Figura 1, um modelo de aplicação de ML para detecção de anomalias dentre os dispositivos IoT.

Figura 1: Aplicação de ML no contexto de dispositivos IoT.



Fonte: Chevtchenko, Sérgio F., et al.

3 MÉTODO

Este estudo orienta-se no objetivo de apresentar os métodos e técnicas utilizadas na aplicação de *machine Learning* (ML) para detecção de anomalias dentro da rede de dispositivos IoT.

Para o atingimento do objetivo proposto, busca-se compreender a aplicação de técnicas de ML em redes de dispositivos IoT. Foram realizadas buscas conforme apresentado na Tabela 1, onde é possível observar as query's utilizadas para buscar periódicos dentro das bases Science Direct, IEEE e ACM.

Tabela 1: Relação de query a serem utilizadas na busca

Query
("anomaly detection" AND "artificial intelligence" AND "IoT")
("*machine Learning*" AND "industrial cybersecurity" AND "IoT")
("industrial IoT networks" AND "anomaly detection algorithms")
("predictive analytics" AND "IoT" AND "security" AND "Industry 4.0")
("artificial intelligence" AND "IoT" AND "industrial cybersecurity")

Fonte: Resultado da pesquisa

Foi utilizado a ferramenta Parsifal na categorização dos artigos a partir de seus respectivos títulos e resumos, utilizando seguinte protocolo PICOC:

- **Population:** Inteligência Artificial e Internet das Coisas
- **Intervention:** Anomaly detection

- **Comparison:** N/A
- **Outcome:** Método OR Algoritmo OR *Machine Learning*
- **Context:** Internet of Things

Após coleta de metadados, foram importados na ferramenta Parsifal e caracterizados conforme os critérios de inclusão e exclusão a seguir:

3.1 Critérios de inclusão:

- Artigos que apresentem resultados e algoritmos;
- Artigos que enfoquem IoT e modelagem de ameaças;
- Artigos Científicos;
- Artigos cuja o objetivo principal é uma pesquisa aplicada a modelagem de ameaças;
- Artigos dos últimos 10 anos;
- Artigos que contenham Título Aderente a modelagem de ameaças;
- Título e abstract aderentes ao objetivo da pesquisa.

3.2 Critérios de análise:

- Este artigo aborda a modelagem de ameaças em dispositivos IoT?
- Este artigo apresenta resultados prévios no resumo?
- Este artigo apresenta algoritmos para modelagem de ameaças?
- Este artigo trata de *Machine Learning*?

3.3 Critério de exclusão:

- Artigos de Conferência
- Resumo não aderente aos critérios de análise
- Título não aderente aos critérios de análise

4 RESULTADOS E DISCUSSÃO

Após definido os procedimentos metodológicos, foram feitas pesquisas nas bases de dados ACM, Science Direct e IEEE. Os metadados foram armazenados em pastas diferentes, editados e mesclados, resultando em um único arquivo para cada base de periódicos usando o notepad. Os resultados das buscas encontram-se na Tabela 2, onde é possível observar a quantidade de artigos encontrados pela query utilizada.

Tabela 2: Quantidade de artigos por query de busca

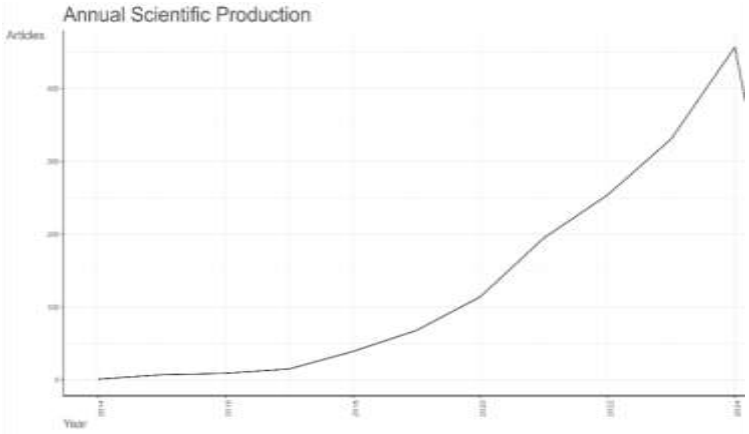
Query	ACM	IEEE	Science Direct
("anomaly detection" AND "artificial intelligence" AND "IoT")	345	194	1487
("*machine Learning*" AND "industrial cybersecurity" AND "IoT")	2	1	15
("industrial IoT networks" AND "anomaly detection algorithms")	1	0	2
("predictive analytics" AND "IoT" AND "security" AND "Industry 4.0")	31	0	327
("artificial intelligence" AND "IoT" AND "industrial cybersecurity")	2	0	11

Fonte: Resultado da pesquisa

Feito as buscas e o armazenamento dos metadados, prossegue-se com o *input* de dados utilizando a biblioteca bibliometrix disponível na linguagem R, que possibilitou a transformação de um arquivo bibtex em um .xlsx, partindo de uma categoria genérica no momento da transformação, já que nativamente o bibliometrix não aceita IEEE, *ACM* e *Sciencedirect* como parâmetros no *dbsource.*

A partir desta importação, o arquivo xlsx é gerado a partir do terminal R, fornecendo o arquivo em um padrão aceitável pelo biblioshiny. A Figura 2 ilustra a quantidade de publicações de artigos relacionados por ano, onde é possível identificar um aumento crescente desde 2016 a respeito dos resultados encontrados nas buscas em bases de periódicos até o ano de 2024.

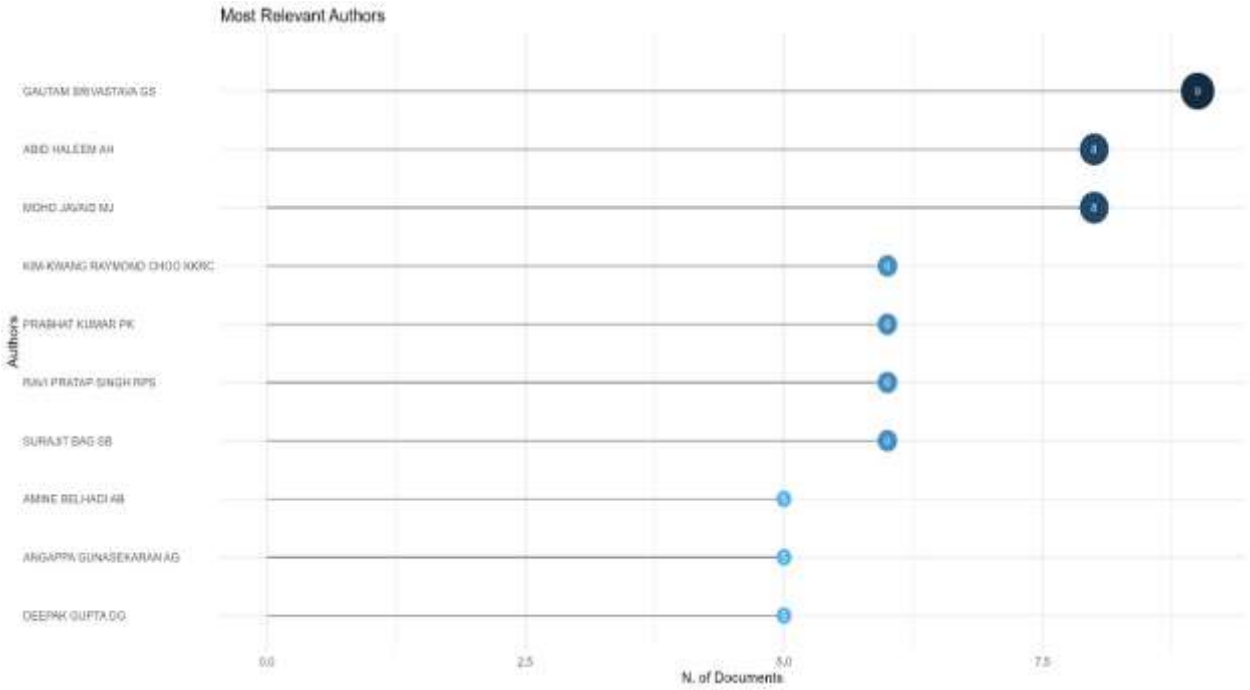
Figura 2: Relação de quantidade de artigos publicados por ano



Fonte: Resultado da pesquisa

É possível acompanhar na Figura 3, os autores mais relevantes devido ao seu número de publicações e aparições em documentos.

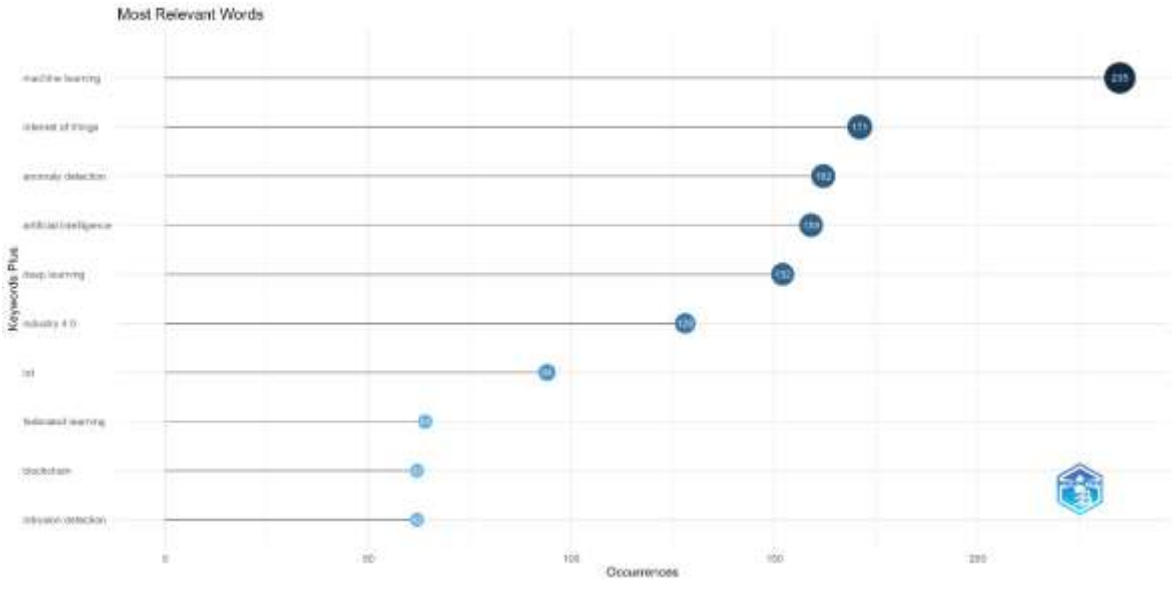
Figura 3: Ranking de autores que mais publicaram relacionados ao objetivo deste trabalho



Fonte: Resultado da pesquisa

Na Figura 4, é possível acompanhar as palavras mais utilizadas dentro da base de artigos analisadas.

Figura 4: Mapeamento de palavras utilizadas em periódicos da amostra analisada



Fonte: Resultado da pesquisa

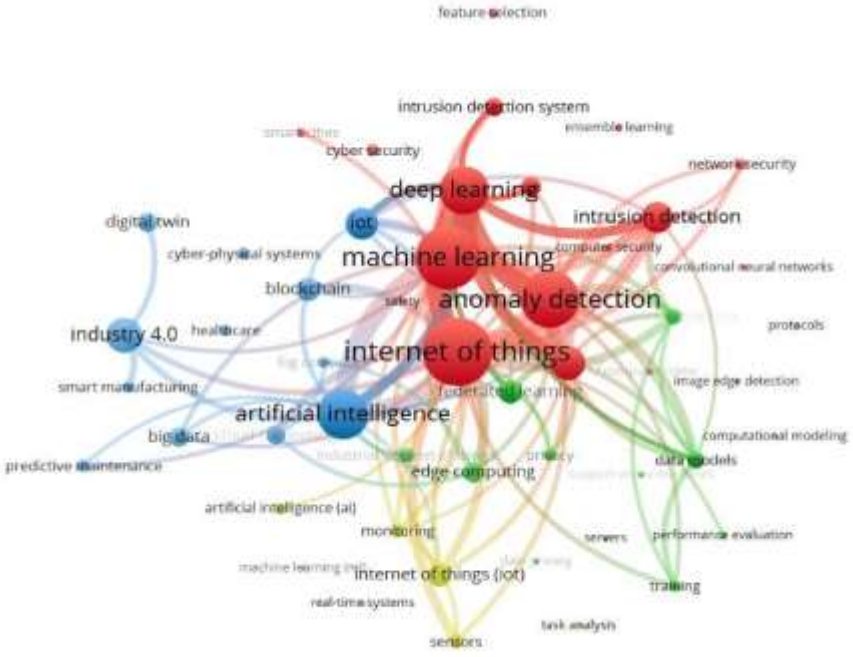
Já na Figura 5, observa-se uma nuvem de palavras, que enfatiza uso de *machine Learning, deep learning* e *artificial intelligence* na detecção de ameaças em dispositivos IoT e no treinamento de máquina para detecção de anomalias.

Figura 5: Nuvem de palavras

Fonte: Resultado da pesquisa

Em seguida, foi desenvolvido dentro da ferramenta VOSViewer, um mapa de correlação representado na Figura 6 entre palavras-chave, indicando uma forte correlação entre *Internet of Things, anomaly detection e machine Learning*, tendo em vista também a ligação entre *intrusion detection*.

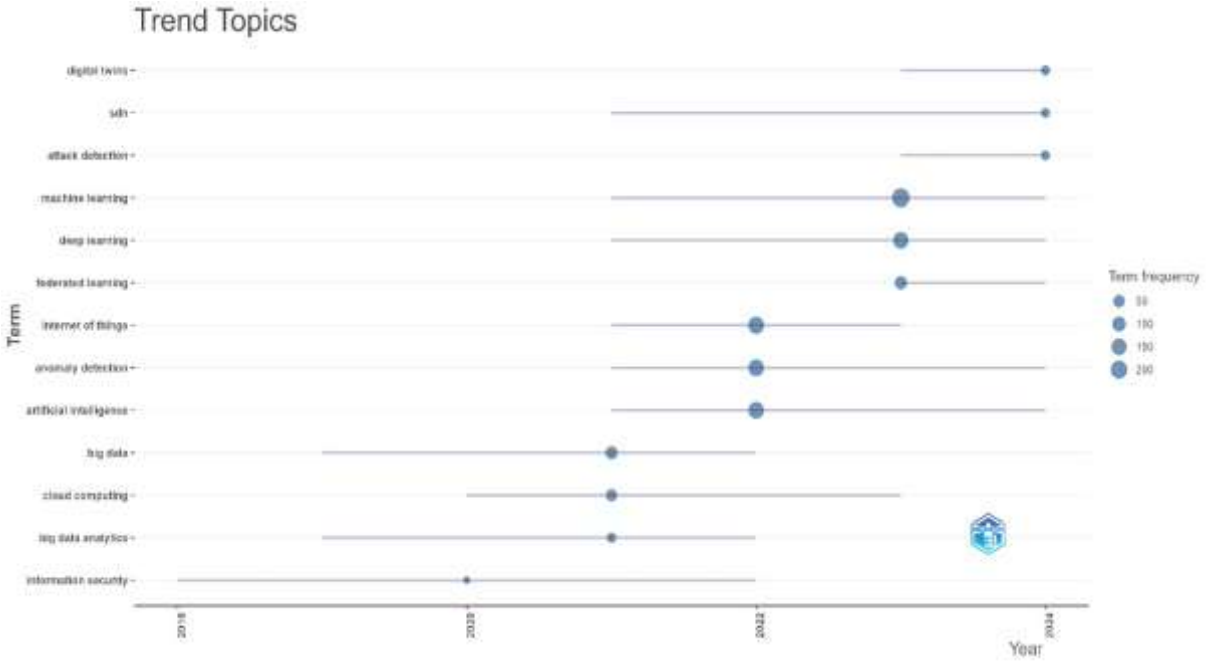
Figura 6: Correlação entre palavras-chave



Fonte: Resultado da pesquisa

Observa-se na Figura 7, a tendência de palavras utilizadas durante os últimos 10 anos, evidenciando o aumento da frequência dos termos nos últimos anos.

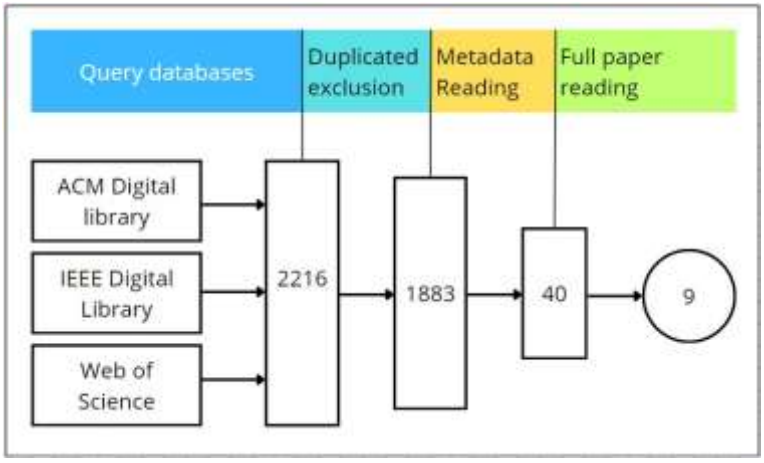
Figura 7: Tendência de termos e tópicos por ano



Fonte: Resultado da pesquisa

Por fim, após uma análise com base nos resultados obtidos, foi desenvolvido um fluxo de seleção de artigos para que possam ser lidos e selecionados para esta revisão conforme indicado na Figura 8, totalizando em 2216 artigos. Removendo os duplicados, esse número reduz para 1883, após a análise dos títulos e resumos, foram selecionados com base nos critérios já estabelecidos 40 artigos a serem analisados, até o presente momento, foram selecionados 9 artigos com base nas citações que sejam > 10 e autores mais relevantes, e que tenham relação com *machine Learning* para aplicação dados de dispositivos IoT, priorizando os autores mais influentes conforme a Figura 2.

Figura 8: Fluxo de seleção de artigos



Fonte: Resultado da pesquisa

Foi elaborado, a partir da leitura dos artigos selecionados, uma tabulação com o resumo de cada artigo conforme Tabela 3, evidenciando o uso de técnicas e estratégias relacionadas ao uso de *machine Learning* na detecção de anomalias para proteção de ambientes de infraestrutura IoT em diversos setores como indústria e medicina

Tabela 3: Artigos selecionados e seus respectivos resumos

Título	Autor	Resumo
A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network.	***Kumar, Randhir, et al.***	O artigo propõe um sistema de detecção de intrusões distribuído (IDS) usando computação em névoa para identificar ataques DDoS em redes IoT baseadas em blockchain. Utilizando algoritmos de aprendizado de máquina como Random Forest e XGBoost.
A framework for anomaly detection in IoT networks using conditional generative adversarial networks.	***Ullah, Imtiaz, and Qusay H. Mahmoud.***	O artigo explora o uso de Redes Gerativas Adversariais Condicionais (cGANs) para detecção de anomalias em redes IoT, abordando soluções para dados desbalanceados e aumento de dados.
Design and development of a deep learning-based model for anomaly detection in IoT networks.	***Ullah, Imtiaz, and Qusay H. Mahmoud.***	O artigo utiliza redes neurais convolucionais (CNNs) para detectar e classificar anomalias em redes IoT, combinando múltiplos conjuntos de dados de intrusão.
Digital twin virtualization with *machine Learning* for IoT and beyond 5G networks: Research directions for security and optimal control.	***Jagannath, Jithin, Keyvan Ramezanpour, and Anu Jagannath.***	O artigo resalta o uso da tecnologia de gêmeos digitais (DT), que permite o monitoramento em tempo real e o controle de sistemas inteligentes, virtualizando processos físicos e facilitando a tomada de decisão em redes 5G.
Evaluation of *machine Learning*-based anomaly detection algorithms on an industrial modbus/tcp data set.	***Anton, Simon Duque, et al.***	O artigo analisa a eficácia de SVM e Random Forest na detecção de anomalias de tráfego em redes industriais com dispositivos IoT, destacando a dificuldade em gerar dados válidos para treinamento.
Generative deep learning to detect cyberattacks for the IoT23 dataset.	***Abdalgawad, Nada, et al.***	O artigo avalia a eficácia de sistemas de detecção de intrusão (IDS) em redes IoT usando métodos baseados em assinatura e anomalia, destacando o uso de aprendizado profundo generativo com Adversarial Autoencoders (AAE) e GANs bidirecionais.
Hardware-assisted *machine Learning* in resource-constrained IoT environments for security: review and future prospective.	***Kornaros, Georgios.***	O artigo examina como metodologias de aprendizado de máquina abordam a segurança em redes IoT, com foco na realização de ataques, desenvolvimento de sistemas de detecção e proteção
Anomaly Detection in Industrial Machinery Using IoT Devices and *Machine Learning*: A Systematic Mapping.	***Chevtchenko, Sérgio F., et al.***	O artigo mapeia o uso de aprendizado de máquina, especialmente algoritmos não supervisionados em redes IoT, pois é eficaz na detecção de anomalias, como falhas raras, sem a necessidade de dados rotulados.
Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation.	***Khatun, Mirza Akhi, et al.***	O uso de *machine Learning* na saúde digital melhora o monitoramento remoto e o tratamento em tempo real. Tecnologias como redes neurais profundas, big data e 5G ajudam a mitigar vulnerabilidades, protegendo dados e comunicações sensíveis.

Fonte: Resultado da pesquisa

A revisão deste trabalho destaca o potencial das técnicas de aprendizado de máquina (ML) para a detecção de anomalias em redes IoT, revelando avanços, mas também desafios que demandam soluções inovadoras. Dentre esses desafios, o desbalanceamento de dados em redes IoT é um dos principais obstáculos, pois essas redes geram grandes volumes de dados, mas a ocorrência de anomalias é relativamente rara. Ullah e Mahmoud (2023) abordam essa questão ao propor o uso de cGANs (GANs condicionais) para gerar dados sintéticos e melhorar a detecção de anomalias raras, aumentando a capacidade dos modelos de ML. A combinação de dados reais e sintéticos é uma abordagem promissora que ainda requer aperfeiçoamento para garantir a representatividade e a qualidade dos dados gerados.

Outro grande desafio está relacionado à escalabilidade e eficiência computacional. Redes IoT frequentemente operam em dispositivos com recursos limitados, e algoritmos de ML, como Random Forest e CNNs, apresentam alta complexidade computacional. Kornaros (2021) sugere soluções hardware-assistidas e o uso de edge computing, onde o processamento é realizado na borda da rede, para melhorar a eficiência e reduzir o consumo de recursos. Kumar et al. (2024) propuseram uma abordagem distribuída baseada em blockchain e em algoritmos como Random Forest e XGBoost para melhorar a escalabilidade em redes IoT, aplicando o processamento de segurança diretamente nos dispositivos de borda, o que também assegura a integridade dos dados.

A precisão e robustez dos modelos de detecção de anomalias são outro ponto de atenção, especialmente em ambientes dinâmicos e heterogêneos. O uso de redes neurais profundas e gêmeos digitais (DT), como discutido por Jagannath et al. (2022), possibilita a integração contínua entre sistemas físicos e digitais, aprimorando o monitoramento em tempo real e o controle preditivo. A tecnologia dos gêmeos digitais, aplicada em redes 5G, é um avanço para redes IoT, permitindo um maior controle de decisões baseadas em dados em tempo real.

Em contrapartida, o aprendizado não supervisionado tem se mostrado eficaz na detecção de anomalias em ambientes com falta de dados rotulados. Chevtchenko et al. (2020) exploram essa abordagem em redes IoT industriais, onde o aprendizado supervisionado nem sempre é viável devido à escassez de dados rotulados. Além disso, no contexto da saúde digital, Khatun et al. (2022) destacam o uso de aprendizado profundo e redes 5G para aprimorar o monitoramento remoto e a proteção de dados, áreas que demandam altos padrões de segurança.

CONSIDERAÇÕES FINAIS

O trabalho revisa o uso de técnicas de aprendizado de máquina para a detecção de anomalias em redes de Internet das Coisas (IoT). Destacou-se, com o aumento das vulnerabilidades nessas redes, os métodos tradicionais de segurança não são suficientes, tornando as abordagens de aprendizado de máquina essenciais. A revisão baseia-se em uma análise bibliométrica de artigos de bases como Science Direct, IEEE e ACM, cobrindo os últimos 10 anos.

Dentre as abordagens destacadas, técnicas supervisionadas, como Random Forest, XGBoost e CNNs, mostraram-se eficazes em cenários com dados rotulados, enquanto métodos não supervisionados e generativos, como GANs e AAEs, foram úteis para dados não rotulados ou desbalanceados. Tecnologias emergentes, como blockchain e gêmeos digitais, também foram exploradas, com potencial para aumentar a segurança e a escalabilidade.

A partir dos dados obtidos, este artigo elencou as técnicas mais promissoras e os principais aspectos da utilização de ML na detecção de anomalias. A pesquisa reflete um aumento significativo no número de publicações recentes sobre o tema, evidenciando o crescente interesse da comunidade científica em desenvolver soluções de segurança para redes IoT. Adicionalmente, o trabalho apresenta os critérios de inclusão e exclusão na seleção dos artigos, bem como as ferramentas e técnicas aplicadas para a análise dos dados. Os resultados mostram a detecção de anomalias como uma estratégia central na proteção de redes IoT e o papel importante do *machine Learning* na evolução dessas técnicas.

O trabalho conclui que, embora o aprendizado de máquina tenha mostrado resultados promissores, desafios permanecem, como o desbalanceamento de dados, alta complexidade computacional e a necessidade de maior precisão. A pesquisa contínua e o desenvolvimento de novas técnicas são essenciais para fortalecer a segurança em redes IoT em crescimento

REFERÊNCIAS

Abdalgawad, Nada, et al. "**Generative deep learning to detect cyberattacks for the IoT-23 dataset**". IEEE Access 10 (2021): 6430-6441.

Anton, Simon Duque, et al. "**Evaluation of *machine Learning*-based anomaly detection algorithms on an industrial modbus/tcp data set**". Proceedings of the 13th international conference on availability, reliability and security. 2018.

Chevtchenko, Sérgio F., et al. "**Anomaly Detection in Industrial Machinery Using IoT Devices and *Machine Learning***: A Systematic Mapping". IEEE Access 11 (2023): 128288-128305.

Jagannath, Jithin, Keyvan Ramezanpour, and Anu Jagannath. "**Digital twin virtualization with *machine Learning* for IoT and beyond 5G networks**: Research directions for security and optimal control". Proceedings of the 2022 ACM workshop on wireless security and *machine Learning*. 2022.

Khatun, Mirza Akhi, et al. "***Machine Learning* for Healthcare-IoT Security**: A Review and Risk Mitigation". IEEE Access (2023).

Kornaros, Georgios. "**Hardware-assisted *machine Learning* in resourceconstrained IoT environments for security**: review and future prospective". IEEE Access 10 (2022): 58603-58622.

Kumar, Randhir, et al. "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network". ***Journal of Parallel and Distributed Computing*** 164 (2022): 55-68

Ullah, Imtiaz, and Qusay H. Mahmoud. "**A framework for anomaly detection in IoT networks using conditional generative adversarial networks**". IEEE Access 9 (2021): 165907-165931.

Ullah, Imtiaz, and Qusay H. Mahmoud. "**Design and development of a deep learning-based model for anomaly detection in IoT networks**". IEEE Access 9 (2021): 103906-103926.