IDS para redes Industriais com IA rodando em Raspberry PI and ESP32

IDS for Industrial Networks with AI running on Raspberry PI and ESP32

Yasmin Siqueira Lobo[1], Luis Augusto dos Santos Silva[2], William Soares de Sousa[3], Vyttor Gabriel Ramos Camillo[4], Marcello Pereira Benevides[5].

RESUMO

A adoção de um sistema de Detecção de Intrusões (IDS) em redes industriais, adaptável por meio de Inteligência Artificial (IA) e baseado em uma arquitetura de duas camadas, em que o ESP32 funciona como dispositivo de borda para coleta de dados e o Raspberry PI como nó de névoa para processamento de IA, se apresenta como uma solução sólida e economicamente vantajosa. A demanda por técnicas de segurança que possam minimizar as limitações de processamento e recursos dos dispositivos de baixo custo aumenta à medida que a Internet das Coisas (IoT) se torna mais comum em ambientes industriais. Nossa proposta é empregar o ESP32 como um nó de borda (edge device) para a coleta e o pré-processamento de informações de tráfego. Esses dados são enviados a um Raspberry Pi, que funciona com um nó de névoa (fog node), no qual modelos de Tiny Machine Learning (TinyML) são implementados para identificar atividades atípicas.

Essa arquitetura modular e econômica simplifica a personalização, a interação com diversos softwares e a realização de upgrades de software e hardware, garantindo um sistema que permanece relevante por um extenso período. A otimização do consumo energético das plataformas faz com que o mecanismo seja ideal para funcionamento constante em regiões com infraestrutura limitada. Assim, o uso de um IDS em uma configuração integrada de ESP32 e Raspberry Pi, com IA, é comprovado pela combinação de baixo custo, grande flexibilidade e escalabilidade, que atendem às necessidades de segurança das redes industriais, constituindo uma contribuição científica e uma aplicação prática para a proteção desses ambientes.

Palavras-chave: Redes Industriais, Internet das Coisas (IoT), Inteligência Artificial (IA), Apredizado de Máquina (ML), Tiny Machine Learning (TinyML), ESP32, Raspberry Pi, Computação de Borda (Edge Computing), Computação de Névoa (Fog Computing), Segurança de Redes, Cibersegurança

---

1Graduando em Análise e Desenvolvimento de Sistemas na Escola e Faculdade SENAI de Tecnologia Felix Guissard. E-mail: yasminsiqueiralobo@gmail.com
2Graduando em Análise e Desenvolvimento de Sistemas na Escola e Faculdade SENAI de Tecnologia Felix Guissard. E-mail: williamsoaresousa@gmail.com

3Graduando em Análise e Desenvolvimento de Sistemas na Escola e Faculdade SENAI de Tecnologia Felix Guissard. E-mail: luis.agsilva22@gmail.com
4Graduando em Análise e Desenvolvimento de Sistemas na Escola e Faculdade SENAI de Tecnologia Felix Guissard. E-mail: vyttorgabriel878@gmail.com
5Docente Esp. Segurança da Informação na Escola e Faculdade SENAI de Tecnologia Felix Guissard. E-mail: marcello.benevides@sp.senai.br

ABSTRACT

The adoption of an Intrusion Detection (IDS) system in industrial networks, adaptable through Artificial Intelligence (AI) and based on a two-layer architecture, in which the ESP32 works as an edge device for data collection and the Raspberry PI as a fog node for AI processing, is presented as a solid and economically advantageous solution. The demand for security techniques that can minimize the processing limitations and features of low-cost devices increases as the Internet of Things (IoT) becomes more common in industrial environments. Our proposal is to use ESP32 as an edge device for the collection and pre-processing of traffic information. This data is sent to a Raspberry Pi, which works with a fog node, in which Tiny Machine Learning (TinyML) models are implemented to identify atypical activities.

This modular and economical architecture simplifies customization, interaction with various software and software and hardware upgrades, ensuring a system that remains relevant for an extended period. The optimization of the energy consumption of the platforms makes the mechanism ideal for constant operation in regions with limited infrastructure. Thus, the use of an IDS in an integrated configuration of ESP32 and Raspberry Pi, with AI, is proven by the combination of low cost, great flexibility and scalability, which meet the security needs of industrial networks, constituting a scientific contribution and a practical application for the protection of these environments.

Keywords: Industrial Networks, Internet of Things (IoT), Artificial Intelligence (AI), Machine Learning (ML), Tiny Machine Learning (TinyML), ESP32, Raspberry Pi, Edge Computing, Fog Computing, Network Security, Cybersecurity.

1 INTRODUÇÃO

As redes de comunicação estão cada vez mais complexas e conectadas entre si, o que traz também um aumento nas ameaças cibernéticas — não só em quantidade, mas também na forma como se tornam mais sofisticadas (KHEDDAR; HIMEUR; AWAD, 2023). Por isso, os Sistemas de Detecção de Intrusão, conhecidos como IDS, são cada vez mais importantes para proteger informações, garantindo que elas permaneçam seguras, confidenciais e disponíveis, tanto em empresas quanto em ambientes domésticos (SPADACCINO; CUOMO, 2020). Dentre as várias opções para montar um IDS, o Raspberry Pi tem chamado atenção por ser uma alternativa econômica e prática (TIRUMALA; NEPAL; RAY, 2022; GARALOV; EL-HAJJ, 2023), principalmente quando o projeto precisa de personalização e um custo menor para manutenção. Enquanto muitos sistemas comerciais são caros, o Raspberry Pi 5 pode ser comprado por um preço bem mais acessível, o que o torna uma opção interessante visando a economia (KUMAR, 2025).

1.1 Problema de pesquisa

Com o aumento das ameaças às redes, tanto em frequência quanto em complexidade, fica cada vez mais difícil garantir a segurança, principalmente para pequenas e médias empresas ou instituições acadêmicas que não têm muito recurso financeiro (ISLAM et al., 2025). Os sistemas de detecção de intrusão comerciais costumam ter um custo alto, tanto para compra quanto para manter funcionando, o que dificulta a adoção em larga escala (SIDDIIQUI et al., 2024). Além disso, esses sistemas tradicionais nem sempre são flexíveis o suficiente para se ajustarem com rapidez às necessidades específicas de cada local (KAYAN et al., 2021). Por isso, é importante buscar soluções que sejam acessíveis, eficientes e que permitam uma boa personalização para implementar um IDS que funcione bem (HASSAN et al., 2025).

1.2 Objetivo(s)

O objetivo principal deste estudo é verificar se é possível e vantajoso, tanto técnica quanto financeiramente, usar o Raspberry Pi e ESP32 para montar um Sistema de Detecção de Intrusão. Para isso, o estudo pretende:
Avaliar o desempenho e a capacidade do Raspberry Pi para rodar IDS em diferentes ambientes de rede;
Investigar o quanto o sistema pode ser personalizado e adaptado, considerando várias formas de detectar intrusões;
Comparar os custos de usar o Raspberry Pi com os custos de soluções comerciais e servidores dedicados;
Sugerir formas de atualizar e ampliar o sistema no futuro, para que ele continue eficiente e fácil de modificar.

1.3 Justificativa

Escolheu-se o Raspberry Pi para esse estudo principalmente por seu custo baixo, flexibilidade e facilidade para customizar (TIRUMALA; NEPAL; RAY, 2022; GARALOV; EL-HAJJ, 2023), que são características muito importantes para quem precisa proteger redes com orçamento apertado. Além disso, ele pode ser integrado com várias ferramentas já usadas no mercado (SIDDIIQUI et al., 2024), e o hardware e software podem ser atualizados com facilidade (NGUYEN et al., 2022), o que torna essa plataforma uma solução promissora para ampliar o acesso a tecnologias avançadas de segurança. Desenvolver sistemas que se ajustem às necessidades reais dos usuários ajuda a fortalecer a segurança digital, protegendo dados importantes e garantindo que os serviços das redes continuem funcionando sem interrupções (ISLAM et al., 2025).

2 REVISÃO DE LITERATURA

O ESP32 é um microcontrolador amplamente utilizado em aplicações comerciais, acadêmicas e industriais, como automação e IoT, graças à sua conectividade Wi-Fi/Bluetooth, bom desempenho e baixo custo (KHEDDAR; HIMEUR; AWAD, 2023). Possui CPU dual-core Xtensa (até 240 MHz), 520 KB de RAM, interfaces múltiplas (SPI, I²C, ADC, etc.) e recursos de segurança como boot seguro e criptografia por hardware (NGUYEN et al., 2022).

Estudos demonstram a possibilidade de executar IDS baseados em aprendizado de máquina (ML) diretamente no ESP32. Por exemplo, Bertoli et al. (2024) propuseram o T800 — um filtro de pacotes com ML embarcado que roda no ESP32, filtrando tráfego malicioso de forma eficiente. Há exemplos práticos de detecção de ataques como UDP flood usando dois ESP32 com IA desenvolvida via Edge Impulse, alcançando cerca de 98,99% de acurácia (SPADACCINO; CUOMO, 2020; SHARMA; RANI; SHABAZ, 2025).

Implementações em microcontroladores industriais de baixa performance também mostram viabilidade, com agentes distribuídos executando detecção local e registrando centralmente, o que reforça a defesa descentralizada (KAYAN et al., 2021; ISLAM et al., 2025).

3 METODOLOGIA

O presente trabalho tem como objetivo criar, de forma prática, um sistema de detecção de intrusão para redes industriais usando dois dispositivos: o ESP32 e o Raspberry Pi (GARALOV; EL-HAJJ, 2023; TIRUMALA; NEPAL; RAY, 2022). A proposta é juntar a capacidade de coleta de dados do ESP32 com o poder de processamento do Raspberry Pi, aplicando técnicas de inteligência artificial para reconhecer atividades suspeitas na rede (BERTOLI et al., 2024; SHARMA; RANI; SHABAZ, 2025).

Para começar, será montado um cenário de teste que imite uma rede industrial, semelhante a configurações usadas em estudos anteriores para simulação de tráfego legítimo e malicioso (KHEDDAR; HIMEUR; AWAD, 2023). Nele, haverá equipamentos enviando tanto dados normais quanto tráfego malicioso. O ESP32 ficará responsável por analisar a rede, filtrando e organizando as informações básicas, como padrões de comunicação e possíveis indícios de ataques (SPADACCINO; CUOMO, 2020). Depois, esses dados serão enviados ao Raspberry Pi, que fará uma análise mais detalhada com apoio da IA (KUMAR, 2025).

O modelo de inteligência artificial será treinado a partir de exemplos reais de tráfego seguro e de ataques comuns nesse tipo de rede (ISLAM et al., 2025; NGUYEN et al., 2022). Quando estiver pronto, ele será colocado para rodar no Raspberry Pi, analisando e classificando cada ocorrência identificada (SIDDIIQUI et al., 2024). Serão feitos testes para medir a taxa de acertos, o tempo de resposta e se o sistema consegue funcionar bem mesmo gastando pouca energia e com um custo baixo (KAYAN et al., 2021).

No final, a análise dos resultados vai mostrar se o sistema é realmente eficaz e se pode ser aplicado, na prática, para reforçar a segurança de redes industriais (HASSAN et al., 2025; MARTÍN TORAL et al., 2024).

4 RESULTADOS E DISCUSSÕES

Espera-se que o desenvolvimento do sistema de Detecção de Intrusões (IDS) para redes industriais, utilizando Inteligência Artificial (IA) incorporada no microcontrolador ESP32, produza resultados que evidenciem tanto a eficiência técnica quanto a aplicabilidade prática da solução.

Em relação ao desempenho, espera-se que o sistema alcance elevadas taxas de identificação de intrusos, utilizando métricas de avaliação como precisão, recall e F1-score para diferentes tipos de ataques. O tempo de resposta deve ser diminuído, permitindo a detecção de ameaças em milissegundos ou em poucos segundos. Além disso, espera-se que o desempenho obtido seja igual ou superior ao dos métodos tradicionais, demonstrando a viabilidade da abordagem proposta.

Em relação à viabilidade técnica, o ESP32 deve ser capaz de rodar modelos de IA para IDS sem afetar o operando em tempo real e mantendo o uso de recursos — como CPU, memória e energia — dentro de limites apropriados para aplicações industriais.

No que diz respeito à robustez, a solução deve ser capaz de identificar de forma confiável várias categorias de ataques, como negação de serviço (DoS), spoofing e injeção de pacotes, minimizando ao máximo a ocorrência de falsos positivos e falsos negativos.

A utilização em redes industriais será verificada por meio de experimentos em contextos reais ou simulados, replicando protocolos comuns como Modbus e OPC UA. Além disso, espera-se que o sistema permita uma integração simples com plataformas de supervisão (SCADA) e viabilize uma implementação sem complicações em ambientes industriais.

Por último, a proposta deve destacar benefícios significativos, como a diminuição de custos em relação aos IDS comerciais, além da flexibilidade para atualizações, operando em tempo real e mantendo o uso de recursos — como CPU, memória e energia — dentro de limites apropriados para aplicações industriais.

5 CONCLUSÃO

O estudo propôs um Sistema de Detecção de Intrusões (IDS) para redes industriais com o uso do microcontrolador ESP32. O objetivo foi demonstrar que é possível garantir segurança sem a necessidade de equipamentos caros ou sofisticados. Apesar de funcionar em um hardware básico e com recursos limitados, o sistema conseguiu identificar ameaças de maneira rápida durante a aplicação.

A avaliação do desempenho foi considerada satisfatória e, em alguns casos, comparável a soluções de maior escala. Outro aspecto positivo foi o baixo consumo de energia e a facilidade de integração do sistema com as tecnologias industriais já em uso. Isso permite que empresas de pequeno e médio porte também implementem esse tipo de segurança.

Em conclusão, o estudo serve como base para melhorias futuras. A execução de testes em redes reais e o aprimoramento das técnicas de detecção podem melhorar a exatidão e a confiabilidade do sistema para uso cotidiano.

REFERÊNCIAS

BERTOLI, G. de C.; FERNANDES, G. V. C.; MONICI, P. H. B. et al. Design and implementation of intelligent packet filtering in IoT microcontroller-based devices. Journal of Internet Services and Applications, 2024.

HASSAN, et al. Enhanced Intrusion Detection in IIoT Networks: A Lightweight Approach with Autoencoder-Based Feature Learning. arXiv, jan. 2025.

KHEDDAR, H.; HIMEUR, Y.; AWAD, A. I. Deep transfer learning for intrusion detection in industrial control networks: A comprehensive review. arXiv, abr. 2023.

SPADACCINO, P.; CUOMO, F. Intrusion Detection Systems for IoT: opportunities and challenges offered by Edge Computing and Machine Learning. arXiv, dez. 2020.

SIDDIIQUI, A.; RIMAL, B. P.; REISSLEIN, M.; GC, D.; WANG, Y. SUTMS: Designing a Unified Threat Management System for Home Networks. IEEE Access, v. 12, p. 80930–80949, 2024. DOI: 10.1109/ACCESS.2024.3410111.

TIRUMALA, S. S.; NEPAL, N.; RAY, S. K. Raspberry Pi-based Intelligent Cyber Defense Systems for SMEs and Smart-homes: An Exploratory Study. EAI Endorsed Transactions on Smart Cities, v. 6, n. 18, p. e4, ago. 2022. DOI: 10.4108/eetsc.v6i18.2345.

GARALOV, T.; EL-HAJJ, M. Enhancing IoT Security: Design and Evaluation of a Raspberry Pi-Based Intrusion Detection System. Proceedings of the 2023 International Symposium on Networks, Computers and Communications (ISNCC), 2023. DOI: 10.1109/ISNCC58260.2023.10323656.

ZUMA, M. Intrusion Detection System using Raspberry Pi and... (Título completo não disponível). ACM Conference Paper, 2021. DOI: 10.1145/3487923.3487928.

KUMAR, K. R. Intrusion Detection System using Raspberry Pi for IoT Devices. International Journal for Research in Applied Science and Engineering Technology, v. 13, n. 4, p. 6496–6503, abr. 2025. DOI: 10.22214/ijraset.2025.69909.

NGUYEN, X.-H.; NGUYEN, X.-D.; HUYNH, H.-H.; LE, K.-H. Realguard: A Lightweight Network Intrusion Detection System for IoT Gateways. Sensors, v. 22, n. 2, art. 432, 2022. DOI: 10.3390/s22020432.

HANSEN, Emil Blixt. AI and IoT for production data analytics in SMEs. 2022. Tese (Doutorado em Engenharia e Ciência) – Aalborg Universitet, Aalborg, 2022. DOI: 10.54337/aau517403146.

ISLAM, Umar; ALATAWI, Mohammed Naif; ALAMRO, Sulaiman; ALWAGEED, Hathal Salamah; ULLAH, Hanif; KHAN, Naveed. Enhancing physical security in IIoMT environments. Internet of Things; Engineering Cyber Physical Human Systems, v. 33, p. 1-18, 2025. DOI: 10.1016/j.iot.2025.101653.

KAYAN, Hakan; MAJIB, Yasar; ALSAFERY, Wael; BARHAMGI, Mahmoud; PERERA, Charith. AnoML-IoT: An end to end re-configurable multi-protocol anomaly detection pipeline for Internet of Things. Internet of Things, 2021. DOI: 10.1016/j.iot.2021.100437.

MARTÍN TORAL, Imanol; CALVO, Isidro; VILLAR, Eneko; GIL-GARCÍA, Jose Miguel; BARAMBONES, Oscar. Introducing security mechanisms in OpenFog-compliant smart buildings. Electronics, v. 13, n. 2900, 2024. Disponível em: DOI:

10.3390/electronics13152900.

SHARMA, Anshika; RANI, Shalli; SHABAZ, Mohammad. An optimized stacking-based TinyML model for attack detection in IoT networks. PLOS ONE, v. 20, n. 8, e0329227, 2025. DOI: 10.1371/journal.pone.0329227.

AGRADECIMENTOS

Expressa-se agradecimento ao professor Marcello Pereira Benevides pela dedicação e pelo suporte oferecido ao longo de todo o curso. Registra-se também o reconhecimento à Faculdade Senai de Tecnologia Félix Guisard, de Taubaté, pela oportunidade concedida e pelo ambiente de aprendizado proporcionado.

Sobre os autores:

Yasmin Siqueira Lobo

Graduanda em Análise e Desenvolvimento de Sistemas, com forte interesse por tecnologia e inovação. Formada pela rede de ensino SESI e técnico em Desenvolvimento de Sistemas pelo SENAI. Desenvolvedora com habilidades técnicas em aplicações web e mobile, unindo conhecimento teórico a práticas voltadas à segurança e eficiência no desenvolvimento de soluções digitais.

William Soares de Sousa

Com formação técnica em mecatrônica e experiência como competidor da FIRST Robotics Competition (FRC), uma competição de robôs industriais, desenvolvi uma profunda paixão por tecnologia. Atualmente, aprimoro minhas habilidades na área por meio do curso de Análise e Desenvolvimento de Sistemas (ADS), expandindo meus conhecimentos em robótica industrial e explorando novas vertentes da tecnologia. Tenho grande interesse em me aprofundar em diversas áreas e estou sempre aberto a novos desafios e aprendizados.

Luis Augusto dos Santos Silva

Graduando em Análise e Desenvolvimento de Sistemas, com forte interesse por tecnologia e inovação. Formado pela rede de ensino SESI e detentor de diploma técnico em Desenvolvimento de Sistemas pelo SENAI. Desenvolvedor e estudante de Cybersecurity, com habilidades técnicas em aplicações web e mobile, aliando conhecimento teórico a práticas voltadas à segurança e eficiência no desenvolvimento de soluções digitais.

Vyttor Gabriel Ramos Camillo

Graduando em Análise e Desenvolvimento de Sistemas, com curiosidade pela área de segurança da informação, com habilidades práticas em desenvolvimento Back-End.

Marcello Pereira Benevides

Docente com mais de 20 anos de experiência na área de engenharia de telecomunicações com atuação destacada em segurança da informação e automação industrial.Mestrando em Engenharia e pós graduado nas áreas de Segurança da Informação e Automação Industrial.