15º Congresso de Inovação, Ciência e Tecnologia do IFSP - 2024

Avaliação do desempenho do MicroAI Atom em ambientes de recursos limitados durante ataques DoS

CRISTIAN G. B. AGUIAR[1], CLODOALDO DE SOUZA FARIA JUNIOR[2], JOÃO DOMINGOS AUGUSTO DOS SANTOS PEREIRA[3], JOSÉ GUILHERME MAGALINI DOS SANTOS DECANINI[4].

[1]Graduando em Engenharia Elétrica, Bolsista PIBIFSP, Campus Presidente Epitácio, cristian.gabriel@aluno.ifsp.edu.br.
[2]Mestrando em Ciências Cartográficas, UNESP, Campus Presidente Prudente, clodoaldo.souza@unesp.br.
[3]Docente – IFSP – Campus Presidente Epitácio, joao.pereira@ifsp.edu.br
[4]Docente – IFSP – Campus Presidente Epitácio, guilhermedecanini@ifsp.edu.br.

Área de conhecimento (Tabela CNPq): 1.03.04.00-2 Sistemas de Computação

RESUMO: A implementação de inteligência artificial (IA) em dispositivos embarcados, como o Raspberry Pi, tem avançado significativamente, especialmente com o uso de técnicas de otimização para superar limitações computacionais. O MicroAI Atom é uma solução de IA leve projetada para executar em microcontroladores e dispositivos com recursos limitados, como o Raspberry Pi 3. Nos testes do MicroAI Atom, foi realizado um ataque de negação de serviço (DoS) controlado em um PC conectado ao mesmo ambiente de rede, com o objetivo de avaliar a capacidade do MicroAI Atom em identificar comportamentos anômalos. O sistema utilizado de 32GB foi configurado para monitorar uma variedade de sinais e dados de entrada, incluindo tráfego de rede, atividades de CPU e operações de I/O. O sistema registrou um aumento no tráfego de rede, com a precisão do modelo atingindo 92,41% na detecção de picos durante o ataque. O uso de memória durante a execução dos algoritmos foi de 3958 bytes resultando em 0,00037%. A latência entre a detecção de anomalias e emissão de alertas foi mantida em níveis mínimos, garantindo uma resposta rápida aos eventos. Esses resultados indicam que o MicroAI Atom é uma solução viável para operações prolongadas em ambientes com recursos limitados, como os dispositivos embarcados.

PALAVRAS-CHAVE: MicroAI Atom; dispositivos embarcados; inteligência artificial; detecção de anomalias Ataque DoS.

The Implementation of Neural Networks and AI in Embedded Devices: A Study on the MicroAI Atom on the Raspberry Pi

ABSTRACT: The implementation of artificial intelligence (AI) in embedded devices, such as the Raspberry Pi, has advanced significantly, especially with the use of optimization techniques to overcome computational limitations. MicroAI Atom is a lightweight AI solution designed to run on microcontrollers and resource-constrained devices like the Raspberry Pi 3. During the MicroAI Atom tests, a controlled denial-of-service (DoS) attack was conducted on a PC connected to the same network environment to assess MicroAI Atom's ability to identify anomalous behaviors. The 32GB system used was configured to monitor a variety of signals and input data, including network traffic, CPU activities, and I/O operations. The system recorded an increase in network traffic, with the model's accuracy reaching 92.41% in detecting spikes during the attack. Memory usage during algorithm execution was 3958 bytes, resulting in 0.00037%. The latency between anomaly detection

and alert issuance was kept at minimal levels, ensuring a quick response to events. These results indicate that MicroAI Atom is a viable solution for prolonged operations in resource-limited environments, such as embedded devices.

KEYWORDS: MicroAI Atom; embedded devices; artificial intelligence; anomaly detection DoS attack.

INTRODUÇÃO

A aplicação de inteligência artificial (IA) em dispositivos embarcados, como o Raspberry Pi, tem ganhado relevância devido à necessidade crescente de soluções que processam grandes volumes de dados de maneira eficiente, mesmo em ambientes com recursos computacionais limitados. Dispositivos como o Raspberry Pi enfrentam restrições de processamento e consumo de energia, o que torna a otimização de algoritmos uma questão crucial para garantir a acurácia e a velocidade do sistema. Nesse cenário, o MicroAI Atom surge como uma solução eficiente e leve, desenvolvida especificamente para operar em microcontroladores e sistemas com recursos reduzidos.

O MicroAI Atom, implementado no Raspberry Pi, foi projetado para realizar a detecção de anomalias, previsões e ataques de negação de serviço (DoS) com base em dados de séries temporais. A IA utiliza esses dados para definir limites de operação aceitáveis, garantindo que futuras entradas sejam analisadas em tempo real. Esse tipo de abordagem é fundamental para ambientes que exigem monitoramento constante e decisões rápidas, especialmente em contextos de segurança cibernética e computação de borda (Mohsenin; Partin-Vaisband; Homayoun; Seo; Zhang, 2021).

Este trabalho tem como objetivo demonstrar a implementação do MicroAI Atom no Raspberry Pi, avaliando sua viabilidade para a detecção em tempo real de anomalias. Além disso, busca validar a eficiência do sistema em termos de consumo de recursos tanto em condições normais de operação quanto durante ataques cibernéticos, destacando sua adequação para aplicações de borda e ambientes com recursos limitados, onde respostas rápidas e operações eficientes são cruciais.

MATERIAL E MÉTODOS

Durante os testes do MicroAI Atom, foi utilizado um Raspberry Pi 3 B para execução dos algoritmos de detecção de anomalias, enquanto um notebook Dell com processador Intel Core i7-8565U, 512GB SSD e 8GB DDR4 que foi usado para análises complementares. Bibliotecas como psutil, time, tensorflow.keras.models e numpy foram usadas para coletar dados sobre o uso de CPU e memória durante a atividade normal e um ataque DoS, permitindo avaliar o desempenho do MicroAI Atom em diferentes ambientes.

Para a configuração do ambiente de desenvolvimento, o Raspberry Pi 3B foi configurado com o sistema operacional Raspberry Pi OS e o Python 3.7. Essa versão do Python foi escolhida por suas melhorias de desempenho, como inicialização mais rápida e melhor suporte à programação assíncrona, características cruciais em dispositivos com recursos limitados. Além disso, o uso de *dataclasses facilitou a organização dos dados, simplificando o desenvolvimento*.

A integração do MicroAI Atom no Raspberry Pi foi otimizada para lidar com as limitações de hardware do dispositivo, aproveitando recursos como a GPU para melhorar o desempenho. Testes e ajustes foram realizados para garantir a execução eficiente de algoritmos de IA, especialmente em aplicações de borda que exigem processamento local.

Para garantir o funcionamento eficiente do MicroAI Atom no Raspberry Pi, foram integradas bibliotecas como *Bottle* (para criação de APIs), *Libtorrent-Rasterbar* (para comunicação P2P) e NumPy (para processamento de dados). Além disso, scripts de inicialização foram modificados para configurar variáveis de ambiente, automatizar a inicialização de serviços e monitorar o desempenho do sistema, otimizando o uso de recursos no Raspberry Pi.

Adicionalmente, a Figura 1 apresenta um diagrama simplificado das etapas e do processo de configuração e preparação utilizados na implementação do projeto.

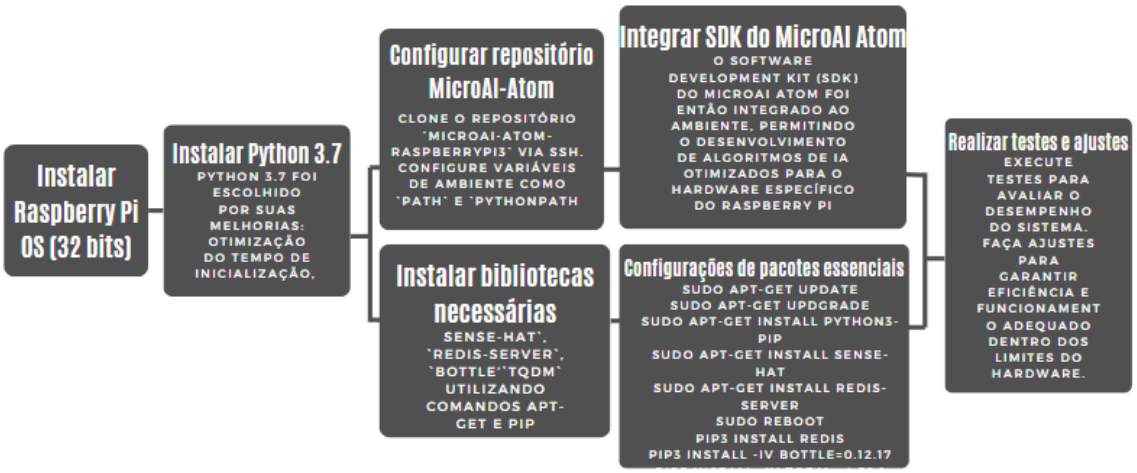

FIGURA 1. Fluxograma de Desenvolvimento

RESULTADOS E DISCUSSÃO

A Tabela 1 apresenta os resultados para a detecção e quantificação dos picos de atividade de rede. Foram monitorados o uso de CPU e a memória utilizada durante os períodos de atividade normal e durante o ataque de negação de serviço (*Denial Of Service DoS*) registrado com:

1. Uso de CPU: cpu_usage_end = psutil.cpu_percent(interval=None) e;
2. Memória utilizada: memory_usage_end = psutil.virtual_memory().used / (1024 ** 2)

TABELA 1. Detecção de quantificação da atividade de rede em períodos de atividade normal e durante ataque.

Métrica	Atividade normal	Durante ataque
Uso de CPU [%]	39.2	55.8
Memória utilizada [Megabytes]	3940	3958

O aumento abrupto no uso de CPU e memória durante o ataque foi correlacionado com a sobrecarga de rede, confirmando a ocorrência de picos de atividade de rede típicos de um ataque *DoS*.A Tabela 2 apresenta a detecção de tentativas de acesso não autorizado, juntamente com o monitoramento contínuo do uso de recursos do sistema. Durante a execução dos algoritmos, foram registrados 3958 bytes, representando 0,00037% do uso de memória. O tempo de resposta do sistema às anomalias foi medido usando a função time.time() para capturar a latência entre a detecção de um evento anômalo e a geração de um alerta:

1. Tempo inicial: start_time = time.time.
2. Tempo final: end_time = time.time().
3.

TABELA 2. Detecção de tentativas de acesso não autorizado durante ataque.

Métrica	Tempo de identificação de ataque
Tempo Identificação[ms]	50

Essa abordagem garante que o MicroAI Atom dados em tempo real e emitir alertas rapidamente, ajudando a mitigar ataques. A eficiência de processamento foi avaliada por meio do monitoramento do uso de CPU e memória após as execuções de detecção de anomalias, assegurando que o sistema operasse dentro dos limites aceitáveis sem sobrecarregar o hardware do Raspberry Pi. Embora o consumo de energia não tenha sido medido diretamente, a baixa utilização de recursos sugere uma operação eficiente, tornando o MicroAI Atom adequado para dispositivos embarcados em ambientes com recursos limitados.

Desempenho Geral do Sistema

Durante o ataque, o sistema detectou um aumento significativo no tráfego de rede, alcançando uma precisão de 92,41% na identificação desses picos de atividade. Além disso, foram identificadas tentativas de acesso não autorizadas, com o sistema emitindo alertas sobre comportamentos que divergiam dos padrões normais de operação do dispositivo. O MicroAI Atom processa esses dados em tempo real, garantindo uma latência mínima entre a detecção das anomalias e a emissão dos alertas.

Mesmo durante a execução de algoritmos intensivos, o consumo de energia permaneceu dentro de níveis aceitáveis, ajustando-se ao ambiente de operação prolongada com recursos limitados. A baixa latência e o controle eficiente do consumo de energia são interdependentes, e a capacidade do MicroAI Atom de processar dados rapidamente, sem consumir recursos excessivos, contribui para manter o consumo de energia reduzido. Isso é essencial para a operação eficiente em dispositivos embarcados com recursos limitados.

CONCLUSÕES

A avaliação do MicroAI Atom durante os testes demonstrou que o sistema é capaz de identificar anomalias e ataques cibernéticos com alta precisão, atingindo 92,41% na detecção de picos de atividade de rede durante ataques de negação de serviço (DoS). O monitoramento contínuo do uso de CPU e memória permitiu identificar acessos irregulares, com o sistema gerando alertas em tempo real, comprovando sua eficácia na detecção de comportamentos anômalos. A configuração experimental, que envolveu o uso de um Raspberry Pi 3 B para a execução dos algoritmos e um *notebook* Dell Inspirion 3583 para o desenvolvimento, confirmou a viabilidade de operar o MicroAI Atom em dispositivos embarcados com recursos limitados.

CONTRIBUIÇÕES DOS AUTORES

M.F.R e C.S.F.J contribuíram com a curadoria e análise dos dados, bem como na metodologia e pesquisa, J.D.A.S.P, J.G.M.S.D e C.S.F.J. contribuíram com a supervisão e revisão, M.F.R também atuou na redação. Todos os autores contribuíram ativamente com a revisão do trabalho e aprovaram a versão submetida. Todos os autores contribuíram com a revisão do trabalho e aprovaram a versão submetida.

AGRADECIMENTOS

A todos que participaram, direta ou indiretamente do desenvolvimento deste trabalho de pesquisa, enriquecendo o meu processo de aprendizado.

REFERÊNCIAS

NOVAC, Pierre-Emmanuel; HACENE, Ghouthi Boukli; PEGATOQUET, Alain; MIRAMOND, Benoît; GRIPON, Vincent. **Quantization and Deployment of Deep Neural Networks on Microcontrollers. Sensors**, [S.L.], v. 21, n. 9, p. 2984, 23 abr. 2021. MDPI AG. http://dx.doi.org/10.3390/s21092984.

MOHSENIN, Tinoosh; PARTIN-VAISBAND, Inna; HOMAYOUN, Houman; SEO, Jae-Sun; ZHANG, Xin. **Guest Editorial Cross-Layer Designs, Methodologies, and Systems to Enable Micro AI for On-Device Intelligence**. Ieee Journal On Emerging And Selected Topics In Circuits And Systems, [S.L.], v. 11, n. 4, p. 527-531, dez. 2021. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/jetcas.2021.3130743.

HOSSEINI, Morteza; MOHSENIN, Tinoosh. **QS-NAS: optimally quantized scaled architecture search to enable efficient on-device micro-ai**. Ieee Journal On Emerging And Selected Topics In Circuits And Systems, [S.L.], v. 11, n. 4, p. 597-610, dez. 2021. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/jetcas.2021.3127932.

ORăşAN, Ioan Lucan; SEICULESCU, Ciprian; CăLEANU, Cătălin Daniel. **A Brief Review of Deep Neural Network Implementations for ARM Cortex-M Processor**. Electronics, [S.L.], v. 11, n. 16, p. 2545, 14 ago. 2022. MDPI AG. http://dx.doi.org/10.3390/electronics11162545.

CONTOLI, Chiara; LATTANZI, Emanuele. **A Study on the Application of TensorFlow Compression Techniques to Human Activity Recognition**. Ieee Access, [S.L.], v. 11, p. 48046-48058, 2023. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/access.2023.3276438.

SHUVO, Md. Maruf Hossain; ISLAM, Syed Kamrul; CHENG, Jianlin; MORSHED, Bashir I.. **Efficient Acceleration of Deep Learning Inference on Resource-Constrained Edge Devices: a review**. Proceedings Of The Ieee, [S.L.], v. 111, n. 1, p. 42-91, jan. 2023. Institute of Electrical and Electronics Engineers (IEEE). http://dx.doi.org/10.1109/jproc.2022.3226481.

LIMA, Leonardo Bruscagini de. **DETECÇÃO DE ANOMALIAS EM TEMPO DE RESPOSTA DE SERVIDORES WEB: UMA ABORDAGEM AUTOMATIZADA PARA APRIMORAR A SEGURANÇA E A EFICIÊNCIA**. 2023. 107 f. Dissertação (Mestrado) - Curso de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas Faculdade de Engenharia Elétrica e de Computação, Campinas, 2023.