Simpósio de Integração Acadêmica
"Das Montanhas de Minas ao Oceano: Os Caminhos da Ciência para um Futuro Sustentável"
SIA UFV 2025

Universidade Federal de Viçosa

Cibersegurança em Redes 5G: Detecção de Anomalias com LSTM Autoencoder

Yasmin Souza Lima, Rodrigo Moreira

ODS 9 – Indústria, Inovação e Infraestrutura

Categoria: Computação / Inteligência Artificial

Introdução

A crescente utilização de funções em nuvem traz consigo desafios relacionados à segurança e confiabilidade dos sistemas distribuídos. Ataques, como os de Negação de Serviço (DDoS), podem comprometer a disponibilidade dos serviços, causando prejuízos.

Neste contexto, técnicas de **aprendizado profundo**, como Autoencoders LSTM, têm se mostrado promissoras para **detecção de anomalias**, analisando padrões de execução e identificando desvios de comportamento em tempo real

Objetivos

- Aplicar um modelo de Autoencoder LSTM para detecção de anomalias em funções em nuvem.
- Avaliar a eficiência do modelo em identificar desvios relacionados a tráfego anômalo (como ataques).
- Contribuir para o desenvolvimento de soluções de segurança baseadas em IA para ambientes de computação em nuvem.

Material e Métodos ou Metodologia

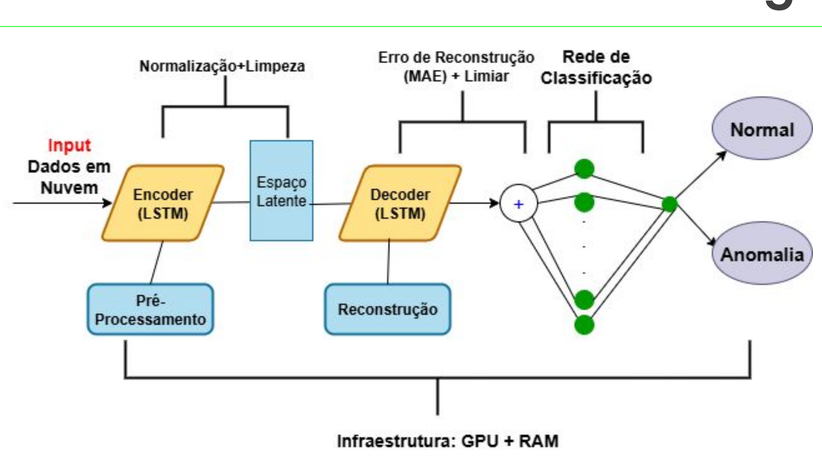

Figura 1. Pipeline do modelo

1. **Base de Dados** – Logs de funções em nuvem com métricas de CPU, RAM, latência e rede.
2. **Pré-processamento** – Normalização dos dados com *MinMaxScaler* e divisão em treino (normais) e teste (normais + anômalos).
3. **Modelo Proposto** – Autoencoder LSTM com camadas codificadoras (compressão) e decodificadoras (reconstrução).
4. **Treinamento** – Utilização apenas de dados normais para aprender o comportamento típico do sistema.
5. **Reconstrução** – O modelo reconstrói as sequências a partir do espaço latente.
6. **Erro de Reconstrução (MAE)** – Diferença entre entrada e saída é medida para identificar desvios.
7. **Classificação** – Aplicação do limiar:Erro ≤ limiar → **Tráfego Normal** || Erro > limiar → **Tráfego Anômalo.**

Apoio Financeiro

CAPES FAPEMIG CNPq

Resultados e/ou Ações Desenvolvidas

A distribuição do erro MAE evidencia uma clara separação entre tráfego normal e de ataque, validando a eficácia do modelo na detecção de anomalias.

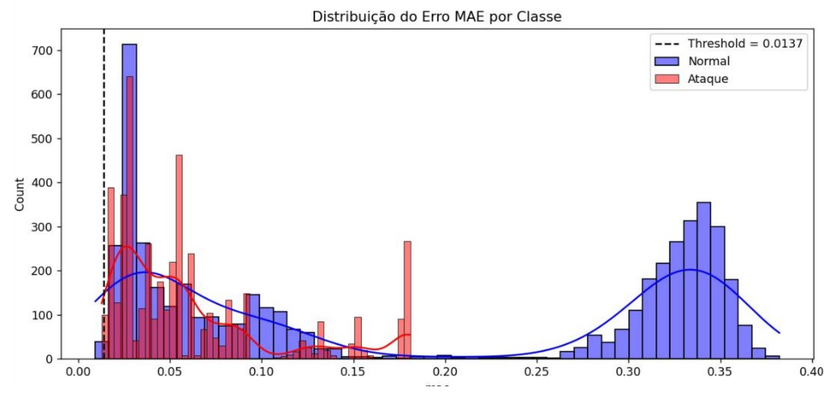

Figura 2. Distribuição dos grupo no dataset

Além disso, a comparação de algoritmos mostra que métodos supervisionados, como Random Forest e Decision Tree, obtiveram desempenho próximo de 100%, enquanto abordagens não supervisionadas, como Isolation Forest, apresentaram menor eficácia.

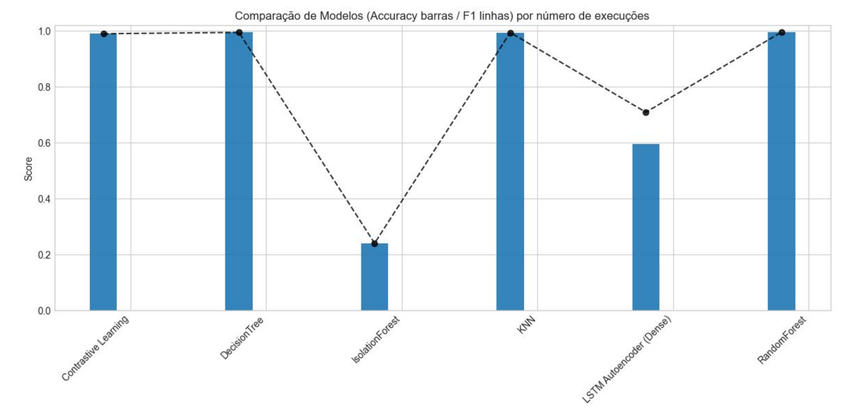

Figura 3. Comparação de algoritmos (Accuracy em barras / F1 em linhas) por número de execuções

Conclusões

O uso de **Autoencoders LSTM** se mostra eficaz na detecção de anomalias em funções em nuvem, sendo capaz de distinguir comportamentos normais de tráfego suspeito.

Os resultados preliminares indicam que a técnica pode apoiar a mitigação de ataques e aumentar a resiliência dos serviços.

Como próximos passos, pretende-se expandir a análise com diferentes arquiteturas de redes neurais e explorar técnicas de ajuste dinâmico de limiar.

REFERÊNCIAS

Goodfellow, I.; Bengio, Y.; Courville, A. *Deep Learning*. MIT Press, 2016.

Chalapathy, R.; Chawla, S. *Deep Learning for Anomaly Detection: A Survey*. arXiv:1901.03407, 2019.

Moreira, R.; Lima, Y. S. *Aprendizado Profundo para a Predição de Ataques de Negação de Serviço Distribuído*. SBC, 2023.