

Uma Implementação Distribuída em Névoa do Algoritmo de Detecção de Novidade em Fluxos de Dados MINAS

Luís Henrique Puhl de Souza

Orientador: Prof. Dr. Hermes Senger

Fevereiro 2020

Universidade Federal de São Carlos

Centro de Ciências Exatas e de Tecnologia

Departamento de Computação

Programa de Pós-Graduação em Ciência da Computação

1. Introdução
2. Fundamentos
3. Estado da Arte e Trabalhos Relacionados
4. Proposta
5. Resultados Preliminares
6. Considerações Finais

Introdução

- Crescimento do número de dispositivos IoT e riscos associados;
- Detecção de intrusão em redes por novidade
- Um sistema para detecção de intrusão em Redes IoT implementando em névoa
- A hipótese do trabalho é que o algoritmo MINAS pode ser distribuído em nós de nuvem e névoa reduzindo a latência e com pouco comprometimento na qualidade de detecção.

Fundamentos

- Ambientes de computação Distribuída;
- Plataformas de processamento distribuído de fluxos;
- Métodos Detecção de Novidade;

Ambientes de computação Distribuída;

- Computação em Nuvem (*Cloud Computing*) como definido em Mell e Grance (2012):
 - **Características:** Serviço sob Demanda, Amplo acesso à rede, Agrupamento de recursos, Elasticidade, Serviço mensurado;
 - **Implementações:** Nuvem privada, Nuvem comunitária, Nuvem pública, Nuvem híbrida.
- Computação de Borda (*Edge Computing*) como definido em Shi et al. (2016):
- Computação em Névoa (*Fog Computing*)

Plataformas de processamento distribuído de fluxos;

Métodos Detecção de Novidade;

Estado da Arte e Trabalhos Relacionados

- Extensões do Algoritmo MINAS;
- Sistemas de detecção de intrusão em redes;

Proposta

- Plataforma de processamento distribuído;
- Arquitetura IDS-IoT;
- M-FOG e a distribuição do algoritmo MINAS;

Proposta

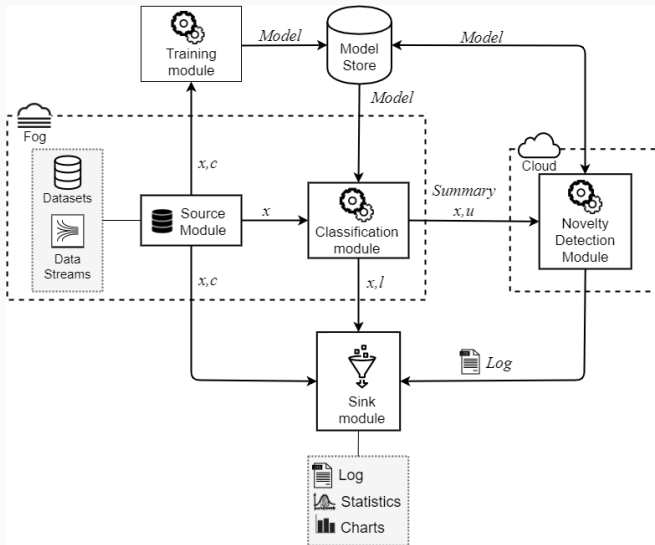


Figura 1: Arquitetura e fluxos de dados do sistema M-FOG.


Resultados Preliminares


- Python e Kafka;
- Flink;

Considerações Finais

Trabalho continua com a finalização da implementação e validação do MFOG com MINAS.

Obrigado!

 MELL, P.; GRANCE, T. The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology. In: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *Public Cloud Computing: Security and Privacy Guidelines*. 2012. p. 97–101. ISBN 9781620819821. Disponível em: <http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf>.

 SHI, W. et al. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, Institute of Electrical and Electronics Engineers Inc., v. 3, n. 5, p. 637–646, oct 2016. ISSN 23274662. Disponível em: <https://ieeexplore.ieee.org/abstract/document/7488250>.

Recomendações de Leitura

empty