Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities

Arthur Braga de Campos Tinoco

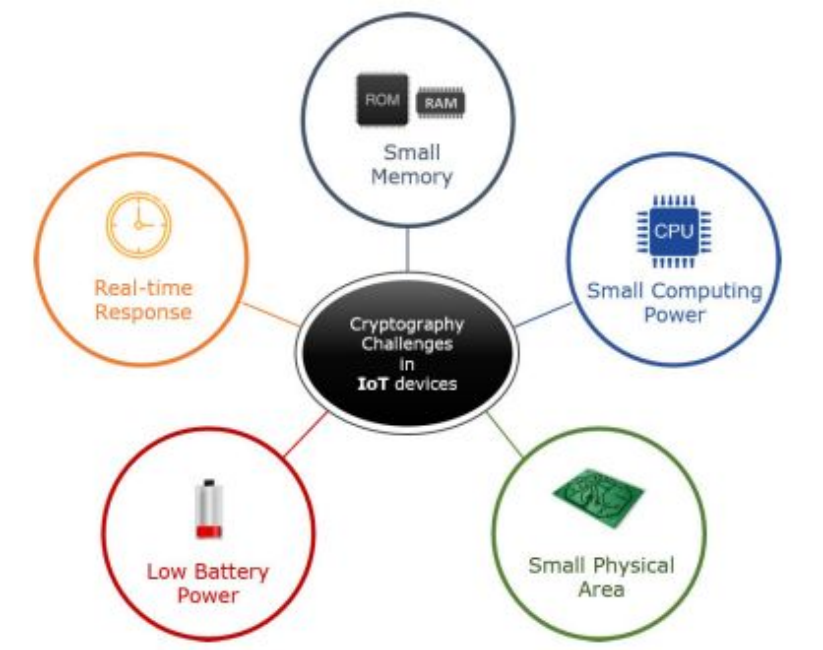
Arthur Gonçalves de Moraes

Dados do artigo

- IEEE Access - 2020
- Vishal A. Thakor
- Mohammad Abdur Razzaque
- Muhammad R. A. Khandaker

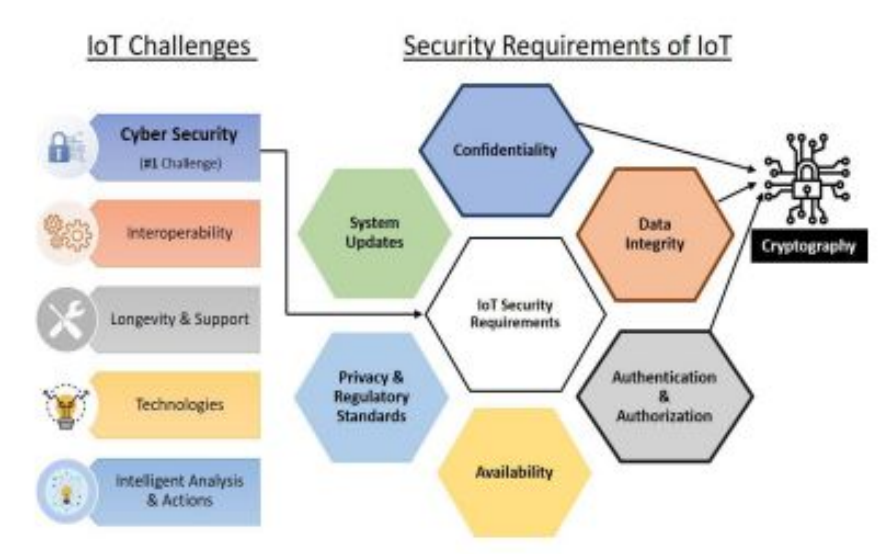
Problema

O desafio da implementação da criptografia em dispositivos IoT, uma vez que possuem recursos físicos e lógicos limitados



Motivação

Com o crescente aumento dos dispositivos IoT é de extrema importância garantir que a criptografia da comunicação desses dispositivos seja feita de forma eficiente



Objetivo

Comparar algoritmos existentes em termos de:

- Custo de implementação
- Performance de hardware e software
- Resistência a ataques

Assim como discutir a demanda de pesquisa na área de "lightweight cryptography (LWC)"

Conclusão

- Nenhuma implementação preenche todos os critérios de eficiência, porém performam melhor no ambiente tratado
- PRESENT e CLEFIA x SIMON e SPECK
- Aumento dos ataques em dispositivos que implementam LWC