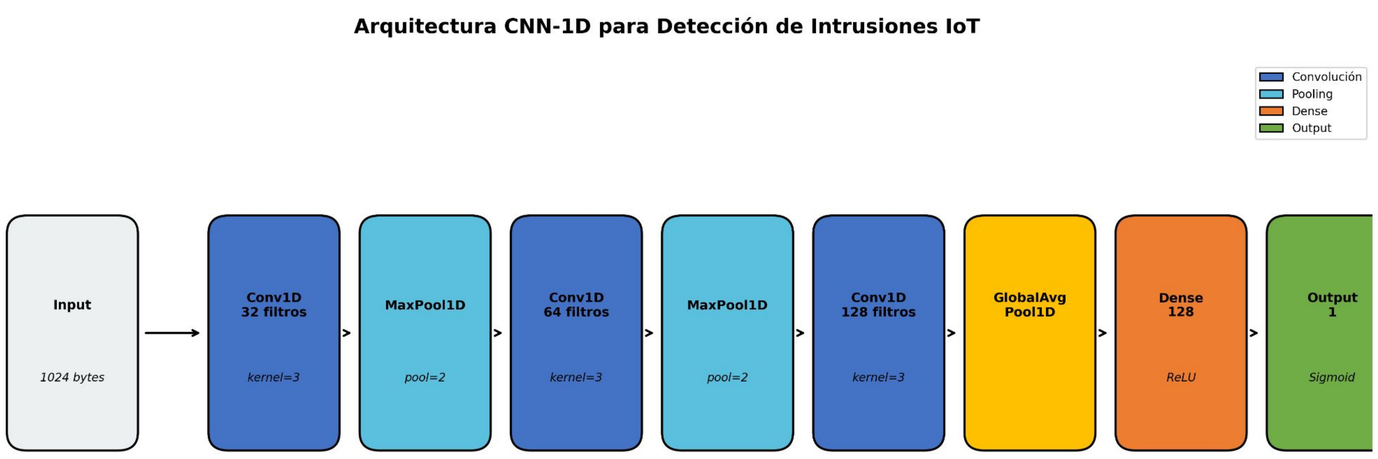
Departamento de Ingeniería Informática
Universidad de Santiago de Chile
DEPARTAMENTO DE INGENIERÍA INFORMÁTICA

Evaluación de una arquitectura CNN-1D para detección de ciberataques IoT en gateways domésticos con recursos limitados

Autor Jorge Morales Ramírez, Profesor guía Juan Iturbe Araya
jorge.morales.r@usach.cl, juan.iturbe@usach.cl
Laboratorio / Grupo de investigación - https://csl.diinf.usach.cl/

Contexto

Los dispositivos IoT en hogares inteligentes mejoran la calidad de vida pero introducen vulnerabilidades críticas. Más del 87% de los ciberataques IoT tienen como objetivo hogares, mientras que menos del 15% cuenta con mecanismos de detección. En Chile, el mercado Smart Home proyecta un crecimiento del 85% hacia 2029, amplificando la urgencia de soluciones accesibles.

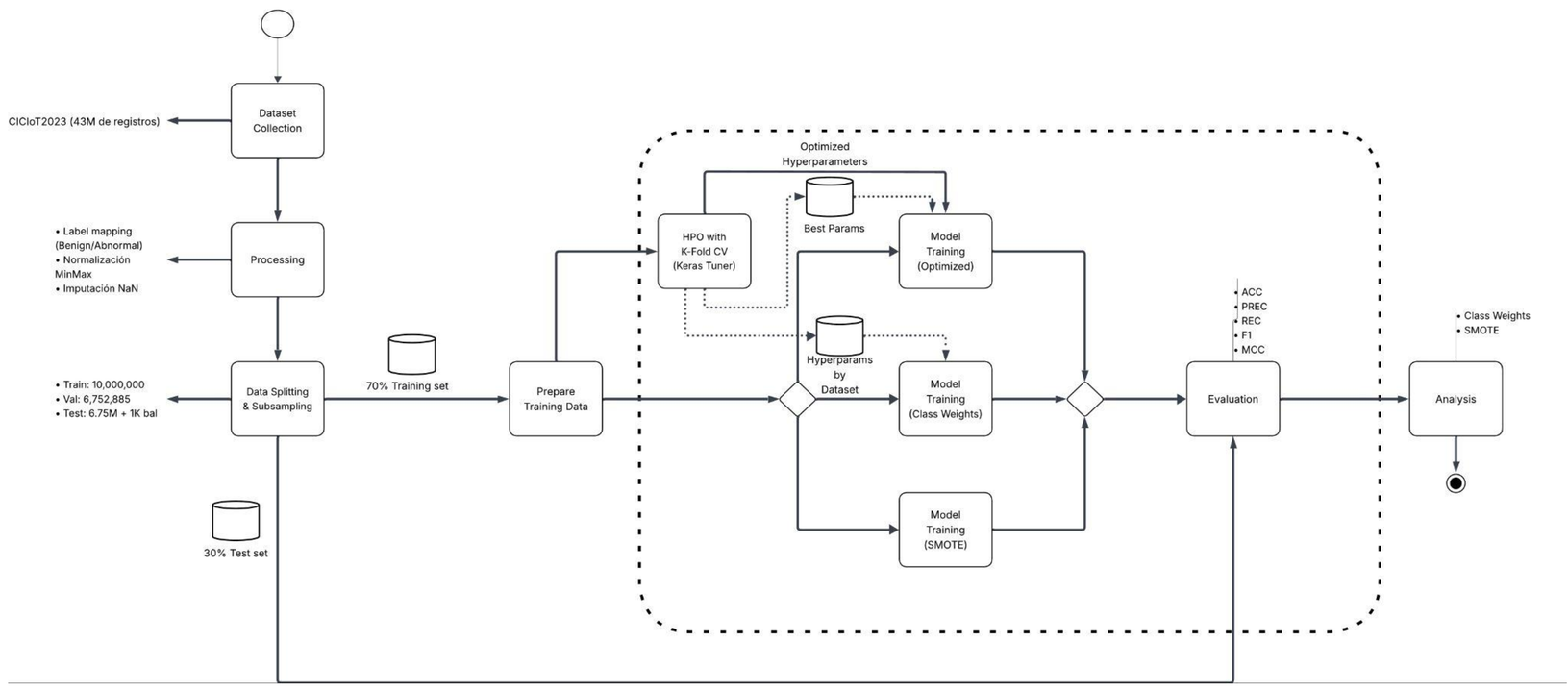


Descripción del problema

Implementar un IDS en gateways domésticos enfrenta una tensión fundamental entre precisión y eficiencia computacional. Arquitecturas complejas como CNN-LSTM superan el 99% de accuracy pero requieren varios GB de RAM, siendo inviables en hardware doméstico típico. Las CNN-1D son una alternativa eficiente, pero sin validación en hardware físico real.

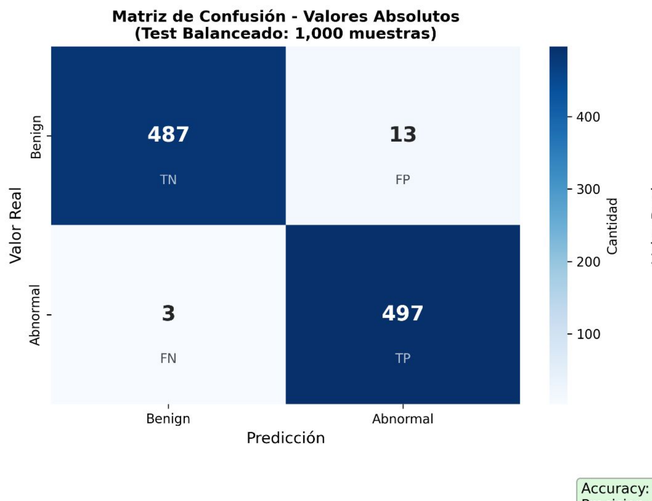
Metodología

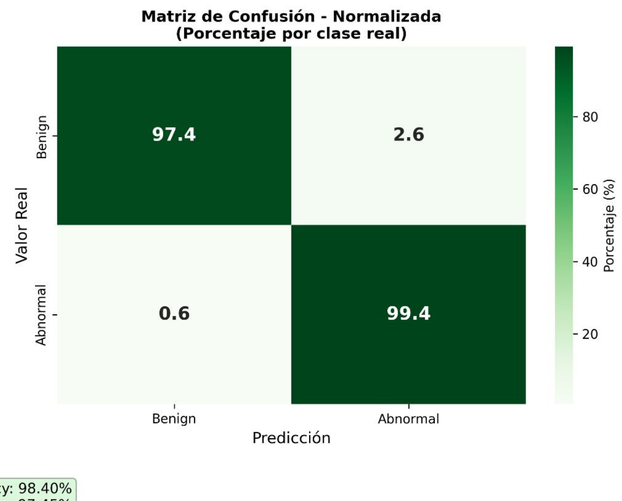
El estudio sigue el marco CRISP-DM en 6 fases: comprensión del problema, análisis de datos, preprocesamiento, modelado, evaluación y despliegue en hardware real.



Solución propuesta

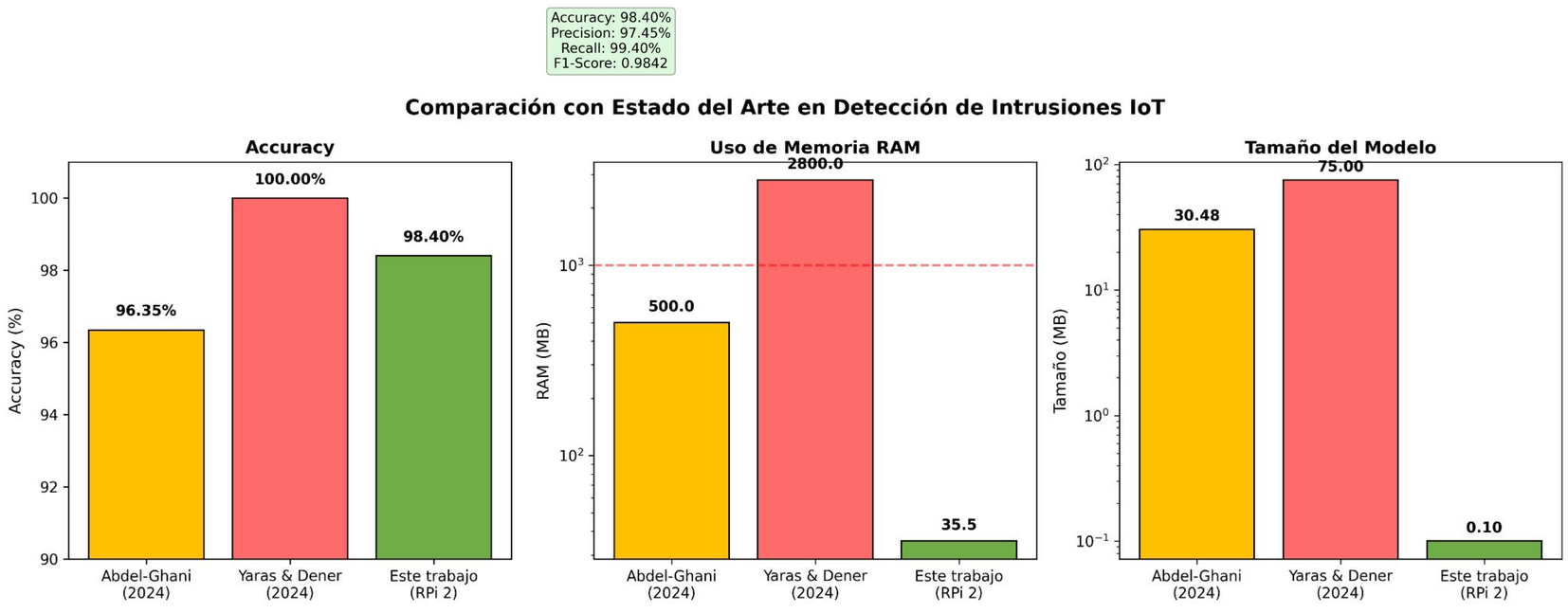
- Arquitectura CNN-1D optimizada con cuantización Float16
- Entrenada sobre CICIoT2023 con estrategia Class Weights
- Desplegada en Raspberry Pi 2 con TensorFlow Lite





Resultados

- **98.40% de accuracy** preservado al migrar de Google Colab a Raspberry Pi 2
- **Class Weights reduce falsos negativos en 88%** vs SMOTE (3 vs 25 ataques no detectados)
- **0.10 MB** de modelo y **35.5 MB de RAM**. Solo 3.5% del sistema
- **72 inferencias/segundo** con latencia de **14 ms** . 7x mejor que el requisito
- Sin degradación bajo carga al **150% de capacidad**



Conclusiones

- IDS basado en CNN-1D viable en hardware doméstico real (Raspberry Pi 2, 2015)
- Cuantización Float16: de 0.63 MB a **0.10 MB** sin pérdida de precisión
- Class Weights como estrategia óptima para minimizar falsos negativos

Trabajos futuros

- Validar en Raspberry Pi 4/5 y dispositivos con TPU/NPU
- Extender a clasificación multiclase (7 tipos de ataque)
- Despliegue en entorno doméstico real con tráfico IoT físico