Caso de estudio

ESTUDIO DE CASO 2

Aplicaciones en Grandes Volúmenes de Datos de Seguridad (Análisis DDoS)

Contexto

Un proveedor de servicios en la nube detecta un ataque DDoS que genera más de 5 millones de solicitudes por minuto.

El sistema debe:

- Identificar IPs sospechosas.
- Detectar patrones repetitivos.
- Priorizar eventos críticos.
- Generar alertas en tiempo real.

Problema

El sistema inicial utilizaba:

- Búsqueda lineal para identificar IPs repetidas.
- Ordenamiento básico para clasificar tráfico.
- Procesamiento secuencial.

Resultado: Colapso del sistema bajo alta carga.

Solución Implementada

Se aplicaron estrategias de optimización:

Reducción de Complejidad Temporal

- Hash Table → O(1) promedio para identificar IPs sospechosas.
- Búsqueda binaria → O(log n) para listas ordenadas.

Procesamiento Eficiente

- Streaming en tiempo real.
- Procesamiento paralelo.
- Indexación de logs.

Uso de Estructuras Auxiliares

- Heap → priorización de IPs más activas.
- Árboles balanceados → mantenimiento ordenado de registros.

Resultados Medidos

Métrica	**Antes**	**Después**
Tiempo de detección	8 s	120 ms
Uso de CPU	95%	60%

Caso de estudio

Métrica	Antes	Después
Capacidad de procesamiento	1M req/min	6M req/min

Impacto

- Detección casi inmediata del ataque.
- Bloqueo automatizado de IPs maliciosas.
- Escalabilidad horizontal efectiva.

Reflexión

En escenarios de grandes volúmenes de datos, la optimización algorítmica no es opcional, es obligatoria. La combinación de:

- Algoritmos O(n log n)
- Hashing O(1)
- Paralelización
- Indexación

Permite mantener la disponibilidad del sistema incluso bajo ataques masivos.