Analizando datos en ciberseguridad

Alberto Fernández Isabel
Universidad Rey Juan Carlos

Universidad Rey Juan Carlos

DSLAB DATA SCIENCE LABORATORY

GOBIERNO DE ESPAÑA
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU
JUNTA DE EXTREMADURA

¿Qué es Big Data?

El Big Data se caracteriza por las 3 V:

- **Volumen**: gran cantidad de datos generados
- **Velocidad**: datos procesados en tiempo real
- **Variedad**: múltiples formatos, desde texto hasta vídeo

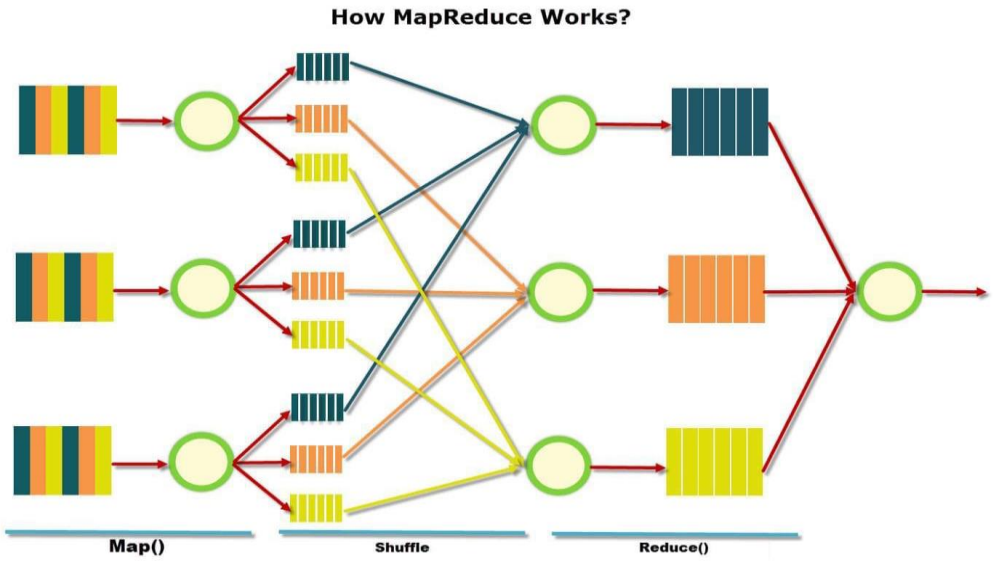
Big Data y el paralelismo

Paralelismo de instrucciones

- Superescalares predictivos
- Varias instrucciones se ejecutan simultáneamente
- Los datos se mantienen en su versión original

Paralelismo de datos

- Técnicas Map-Reduce
- Una única instrucción se ejecuta simultáneamente
- Los datos se simplifican en porciones más manejables



¿Qué es la Ciencia de Datos?

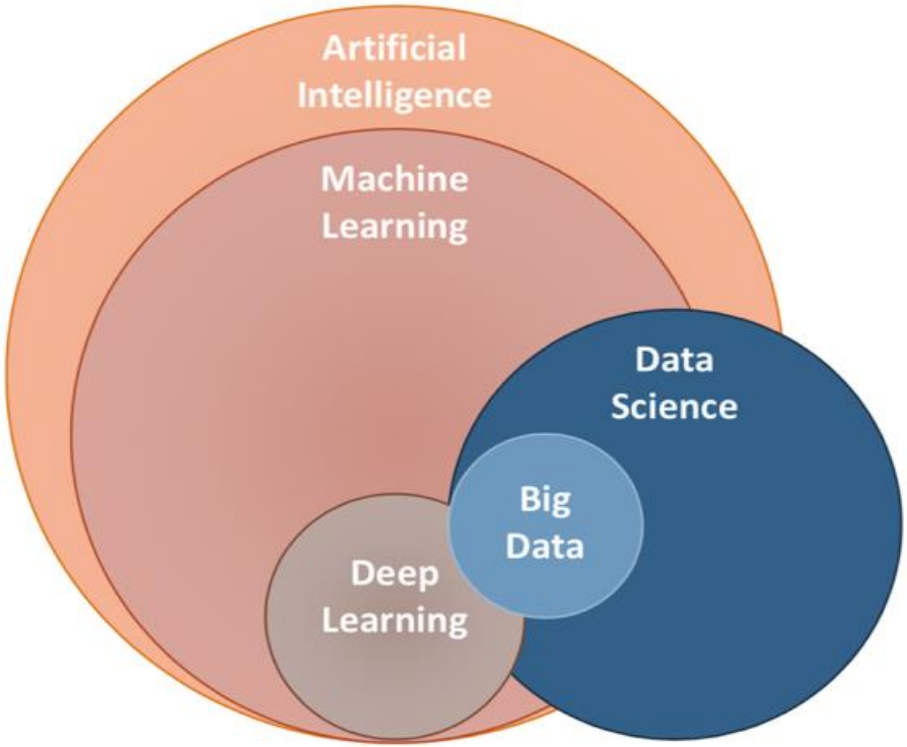
- Área interdisciplinar
- Combina estadística, computación y conocimiento del dominio
- Extrae valor de los datos
- Obtención de conocimiento y la detección de patrones
- Toma decisiones informadas
- Realiza predicciones más precisas

FUNDAMENTOS

APLICACIONES

Ciencia de Datos, Big Data y Aprendizaje Máquina

Big Data	Enfoque en infraestructura y volumen
Ciencia de Datos	Proceso completo desde la recogida hasta el despliegue
Aprendizaje Máquina	Subcampo centrado en crear modelos predictivos



Aplicaciones en Ciberseguridad

Detección de intrusiones en tiempo real	Algoritmos analizan patrones de tráfico para identificar accesos no autorizados
Análisis de comportamiento del usuario (UBA/UEBA)	Identificación de actividades anómalas comparadas con el comportamiento habitual
Prevención de ataques y amenazas persistentes avanzadas (APT)	Modelos predictivos permiten anticipar posibles vectores de ataque
Detección de phishing y spam	Clasificadores supervisados detectan correos maliciosos con alta precisión
Análisis de malware	Reconocimiento de patrones para clasificar software malicioso conocido y desconocido
Detección de fraude	Técnicas de machine learning aplicadas al monitoreo de transacciones bancarias
Análisis forense automatizado	Agrupamiento y visualización de eventos para reconstrucción de ataques
Visualización interactiva de amenazas	Cuadros de mando basados en análisis de datos para facilitar la toma de decisiones rápidas

Técnicas comunes en Big Data para Seguridad

Análisis de datos masivos (Data Mining)	Identificación de patrones ocultos en grandes volúmenes de logs y tráfico.
Aprendizaje Automático Supervisado	Entrenamiento de modelos para detectar malware, phishing o accesos ilegítimos.
Aprendizaje No Supervisado (Clustering)	Detección de comportamientos anómalos sin etiquetas previa.
Análisis de Series Temporales	Monitorización de eventos de seguridad en el tiempo para detectar desviaciones inusuales.
Reducción de Dimensionalidad	Técnicas como PCA o t-SNE para visualizar y entender datos de alta complejidad.
Aprendizaje Máquina Explicable (XAI)	Interpretación de decisiones de modelos complejos para auditorías de seguridad.
Procesamiento de Lenguaje Natural (PLN)	Análisis de correos, documentos y mensajes sospechosos para extraer indicadores de compromiso.

Herramientas tecnológicas

Lenguajes informáticos	Python, R, Scala
Marcos de desarrollo	Spark, Hadoop, H2O
Visualización	Tableau, PowerBI, Shiny
Explicabilidad	SHAP, LIME

Tratamiento de la desinformación

- Procesamiento de lenguaje natural (PLN) para identificar contenido manipulado
- Combinación de análisis semántico, redes sociales y análisis temporal
- Modelos entrenados con grandes corpus textuales
- Acceso a fuentes de información diversas
- https://www.factcheck.org/ y derivados

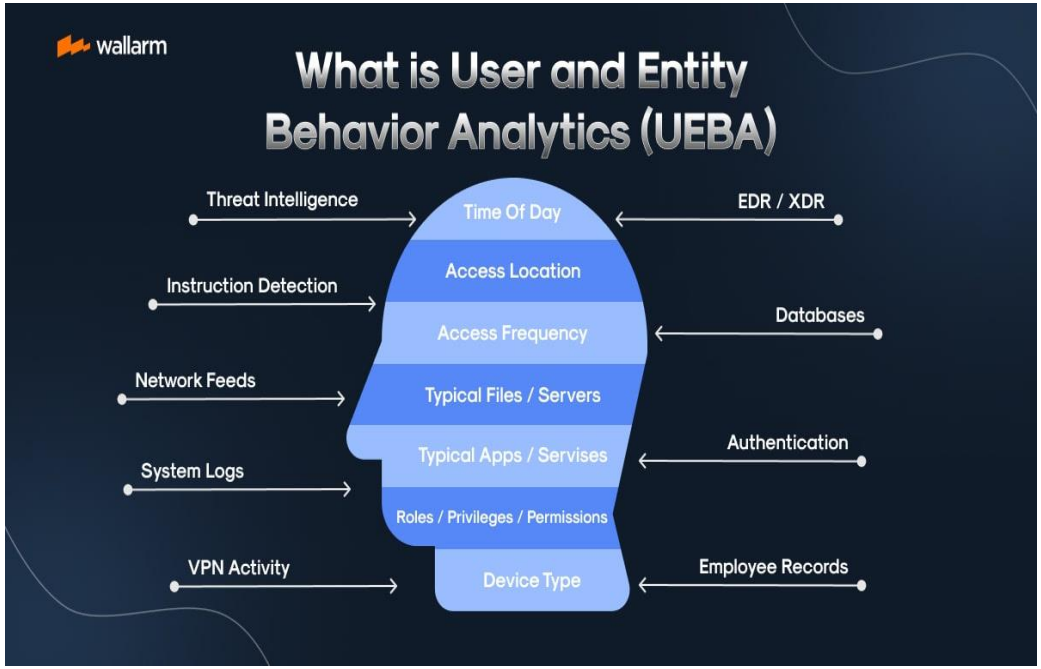
Suplantación de usuarios

Análisis del comportamiento de usuarios o entidades en la red

Técnicas como UEBA (User and Entity Behavior Analytics)

Modelos que aprenden el comportamiento "normal" y alertan ante desviaciones

Evaluan los elementos de interacción persona-ordenador



- Movimiento del ratón
- Pulsaciones de teclado

Análisis del riesgo (Proyecto DICYME)

- Los sistemas OT son vulnerables a los ciberataques
- Los marcos de ciberseguridad actuales (p. ej., NIST CSF) no abordan plenamente las necesidades de la industria
- DeRISK traduce las exposiciones y vulnerabilidades a los ciberriesgos de OT en métricas empresariales
- DICYME propone un nuevo enfoque para la cuantificación del ciberriesgo (CRQ)
- Item Recopilación de evidencia → Modelado → Visualización y soporte de decisiones
- Utiliza entidades reales y sintéticas
- Impulsado por LLM para convertir datos en conocimiento práctico

Novedades DICYME

- Incidentes cibernéticos: datos de incidentes de múltiples fuentes que utilizan PLN para eliminar duplicados y estructurar la información
- Perfil de la víctima: conjunto de datos a nivel de entidad con información financiera, reputación y señales de exposición para el modelado de riesgos (firmografía)
- Utiliza modelos de aprendizaje automático para mejorar la recopilación de datos, la fusión de múltiples fuentes y la imputación de valores faltantes
- Sugiere acciones de mitigación óptimas en función de la relación coste-eficacia y el impacto del riesgo
- Capacidad de simulación del riesgo y del impacto en informes descargables altamente explicativos

Retos Emergentes

Privacidad en IoT

- Funcionalidad de sistemas
- Comunicaciones seguras

Ciberataques a modelos de IA

- Ataques adversarios
- Clonado y robo de modelos

Modelos desactualizados

- Deriva conceptual
- Deriva de datos

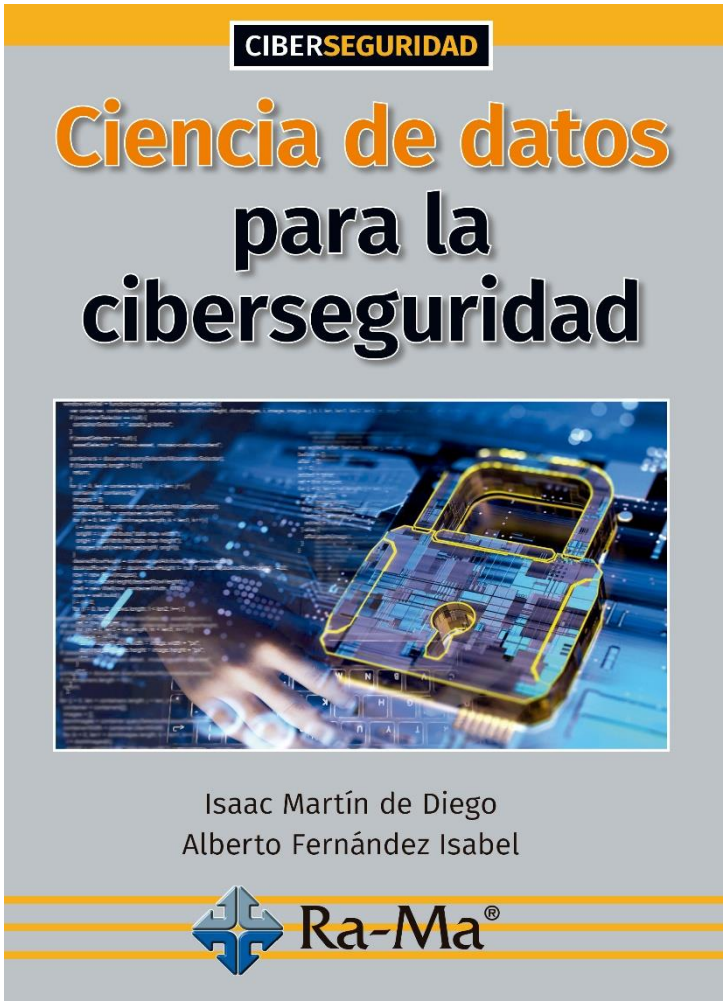
Desinformación y ataques automatizados

- Propagación en redes sociales
- Sesgos ideológicos

Conclusiones

- Sin conocimiento del dominio, los modelos fallan
- Aprender del dato requiere rigor, contexto y propósito
- La seguridad inteligente se construye, no se improvisa
- Big Data no es solo volumen: es visión estratégica
- Fallar rápido, aprender mejor: clave en proyectos de datos
- La colaboración entre expertos en datos y seguridad es esencial

Para saber más



Alberto Fernández Isabel
Universidad Rey Juan Carlos
Data Science Laboratory (DSLAB)
alberto.fernandez.isabel@urjc.es