

Unidad 5: Deep Learning y sus aplicaciones en ciberseguridad

Adarsh KUMAR

Universitat Politècnica de Catalunya
Department of Computer Science

Coordinador del proyecto:
Prof. Ilker Demirkol

Proyecto MERiT
3 de septiembre de 2025

Co-funded by the European Union

Diapositiva 2

Redes neuronales profundas (DNN) | Redes neuronales recurrentes (RNN) | Detección de malware

Esquema

1. Redes neuronales profundas (DNN)
2. Redes neuronales recurrentes (RNN)
3. Detección de malware

Diapositiva 3

Redes neuronales profundas (DNN) | Redes neuronales recurrentes (RNN) | Detección de malware (sección activa: Redes neuronales profundas (DNN))

Redes neuronales profundas (DNN)

- Redes feedforward multicapa para el modelado no lineal complejo.
- Extraen características jerárquicas mediante capas sucesivas.
- Estructura: capa de entrada, capas ocultas, capa de salida.
- Funciones de activación: ReLU, sigmoide, tanh.
- Entrenamiento: retropropagación y descenso de gradiente.
- Casos de uso en ciberseguridad: clasificación de malware, identificación del tipo de ataque.

Diapositiva 4

Redes neuronales profundas (DNN) | Redes neuronales recurrentes (RNN) | Detección de malware (sección activa: Redes neuronales profundas (DNN))

Redes neuronales convolucionales (CNN)

- Diseñadas para el análisis de datos espaciales o estructurados.
- Componentes clave: capas convolucionales, capas de agrupamiento (pooling) y capas totalmente conectadas.
- Adaptadas a datos de ciberseguridad como los gráficos de bytes de ejecutables.
- Casos de uso: clasificación de malware como imágenes, detección de anomalías en matrices de tráfico.
- Extraen eficazmente patrones locales, como secuencias de opcodes.
- Mejoran el análisis estático de código y la detección de amenazas.

Diapositiva 5

Redes neuronales profundas (DNN) | Redes neuronales recurrentes (RNN) | Detección de malware (sección activa: Redes neuronales recurrentes (RNN))

Co-funded by the European Union

Redes neuronales recurrentes (RNN)

- Diseñadas para datos secuenciales con dependencias temporales.
- Mantienen estados ocultos que evolucionan con el tiempo.
- Desafíos: el desvanecimiento/explosión del gradiente dificulta el aprendizaje de secuencias largas.
- Capacidad limitada para capturar dependencias de largo alcance.
- Útiles para analizar registros secuenciales y series temporales.
- Base de modelos secuenciales avanzados como las LSTM.

Diapositiva 6

Redes neuronales profundas (DNN) | Redes neuronales recurrentes (RNN) | Detección de malware (sección activa: Redes neuronales recurrentes (RNN))

Redes de memoria a corto y largo plazo (LSTM)

- Gestionan dependencias a largo plazo mediante puertas de entrada, olvido y salida.
- Modelan eficazmente secuencias con contexto de largo alcance.
- Aplicaciones: clasificación de tráfico de red, detección de anomalías en registros del sistema.
- Útiles en el modelado del comportamiento de usuarios (horas de inicio de sesión, rutas de acceso).
- Superan las limitaciones de las RNN tradicionales.
- Mejoran la detección de patrones temporales en ciberseguridad.

Diapositiva 7

Redes neuronales profundas (DNN) | Redes neuronales recurrentes (RNN) | Detección de malware (sección activa: Detección de malware)

Detección de malware mediante aprendizaje profundo

- Análisis estático: las CNN clasifican malware a partir de imágenes a nivel de byte o secuencias de opcodes.
- Análisis dinámico: las RNN/LSTM procesan trazas de comportamiento obtenidas en sandboxes.
- Los modelos híbridos combinan características estáticas y dinámicas con embeddings de DNN.
- Ejemplo de CNN: conjunto de datos del Microsoft Malware Classification Challenge.
- Mejora la precisión de la detección y la automatización.
- Permite detectar nuevas variantes de malware.

Diapositiva 8

Redes neuronales profundas (DNN) | Redes neuronales recurrentes (RNN) | Detección de malware (sección activa: Detección de malware)

Co-funded by the European Union

Análisis del tráfico de red

- Las CNN y las LSTM analizan flujos de paquetes y cargas útiles.
- Se utilizan para la detección de intrusiones, la detección de botnets y la clasificación de tráfico cifrado.
- Ejemplo: LSTM entrenada con el tamaño de los paquetes y los tiempos entre llegadas para detectar anomalías en SSH.
- Captura patrones de tráfico temporales y espaciales.
- Permite la monitorización del tráfico en tiempo real.
- Se adapta a las amenazas de red en constante evolución.

Diapositiva 9

Redes neuronales profundas (DNN) | Redes neuronales recurrentes (RNN) | Detección de malware (sección activa: Detección de malware)

Aplicaciones en inteligencia de amenazas

- El aprendizaje profundo procesa texto no estructurado de informes de amenazas y foros.
- Utiliza embeddings de palabras (Word2Vec, BERT) y modelos secuenciales (RNN, transformers).
- Extrae indicadores de compromiso (IoC).
- Las redes neuronales de grafos (GNN) modelan las relaciones entre familias de malware, IP y URL.
- Permite el reconocimiento automatizado de patrones de amenazas.
- Mejora el conocimiento de la situación y la defensa proactiva.

Diapositiva 10

Redes neuronales profundas (DNN) | Redes neuronales recurrentes (RNN) | Detección de malware (sección activa: Detección de malware)

Conclusión

- El aprendizaje profundo automatiza analíticas complejas de ciberseguridad.
- Las CNN destacan en el reconocimiento de patrones espaciales en malware y tráfico.
- Las RNN/LSTM modelan eficazmente datos secuenciales de eventos cibernéticos.
- La integración en sistemas en tiempo real refuerza la defensa.
- Responde a la sofisticación y la escala de las ciberamenazas actuales.
- Esencial para las infraestructuras de ciberseguridad de próxima generación.

Co-funded by the European Union