Unit 5: Deep Learning and its applications in Cybersecurity

Adarsh KUMAR

Universitat Politècnica de Catalunya
Department of Computer Science

Project Coordinator:
Prof. Ilker Demirkol

MERiT Project
September 3, 2025

Co-funded by
the European Union

Outline of

MERIT

Co-funded by
the European Union

Deep Neural Networks (DNNs)

- Multi-layered feedforward networks for complex nonlinear modeling.
- Extract hierarchical features through successive layers.
- Structure: input layer, hidden layers, output layer.
- Activation functions: ReLU, sigmoid, tanh.
- Training: backpropagation and gradient descent.
- Cybersecurity use cases: malware classification, attack type identification.

MERiT

Co-funded by the European Union

Convolutional Neural Networks (CNNs)

- Designed for spatial or structured data analysis.
- Key components: convolutional layers, pooling layers, fully connected layers.
- Adapted for cybersecurity data like byte plots of executables.
- Use cases: malware image classification, traffic matrix anomaly detection.
- Effectively extract local patterns such as opcode sequences.
- Improves static code analysis and threat detection.

MERIT

Co-funded by the European Union

Recurrent Neural Networks (RNNs)

- Designed for sequential data with temporal dependencies.
- Maintain hidden states evolving over time.
- Challenges: vanishing/exploding gradients hamper long sequence learning.
- Limited for capturing long-range dependencies.
- Useful for analyzing sequential logs and time-series data.
- Foundation for advanced sequential models like LSTMs.

MERiT

Co-funded by the European Union

Long Short-Term Memory Networks (LSTMs)

- Handle long-term dependencies using input, forget, and output gates.
- Effectively model sequences with long-range context.
- Applications: network traffic classification, system log anomaly detection.
- Useful in user behavior modeling (login times, access paths).
- Overcomes limitations of traditional RNNs.
- Improves detection of temporal patterns in cybersecurity.

MERiT

Co-funded by the European Union

Malware Detection Using Deep Learning

- Static analysis: CNNs classify malware using byte-level images or opcode sequences.
- Dynamic analysis: RNNs/LSTMs process behavior traces from sandboxes.
- Hybrid models combine static and dynamic features with DNN embeddings.
- CNN example: Microsoft Malware Classification Challenge dataset.
- Enhances detection accuracy and automation.
- Enables detection of novel malware variants.

MERiT

Co-funded by the European Union

Network Traffic Analysis

- CNNs and LSTMs analyze packet flows and payloads.
- Used for intrusion detection, botnet detection, encrypted traffic classification.
- Example: LSTM trained on packet size and inter-arrival times for SSH anomaly detection.
- Captures temporal and spatial traffic patterns.
- Supports real-time traffic monitoring.
- Adapts to evolving network threats.

MERIT

Co-funded by the European Union

Threat Intelligence Applications

- Deep learning processes unstructured text from threat reports and forums.
- Uses word embeddings (Word2Vec, BERT) and sequence models (RNNs, transformers).
- Extracts Indicators of Compromise (IoCs).
- Graph Neural Networks (GNNs) model relationships among malware families, IPs, URLs.
- Enables automated threat pattern recognition.
- Enhances situational awareness and proactive defense.

MERiT

Co-funded by the European Union

Conclusion

- Deep learning automates complex cybersecurity analytics.
- CNNs excel at spatial pattern recognition in malware and traffic.
- RNNs/LSTMs effectively model sequential cyber event data.
- Integration into real-time systems strengthens defense.
- Addresses sophistication and scale of modern cyber threats.
- Essential for next-generation cybersecurity infrastructures.

MERIT

Co-funded by the European Union