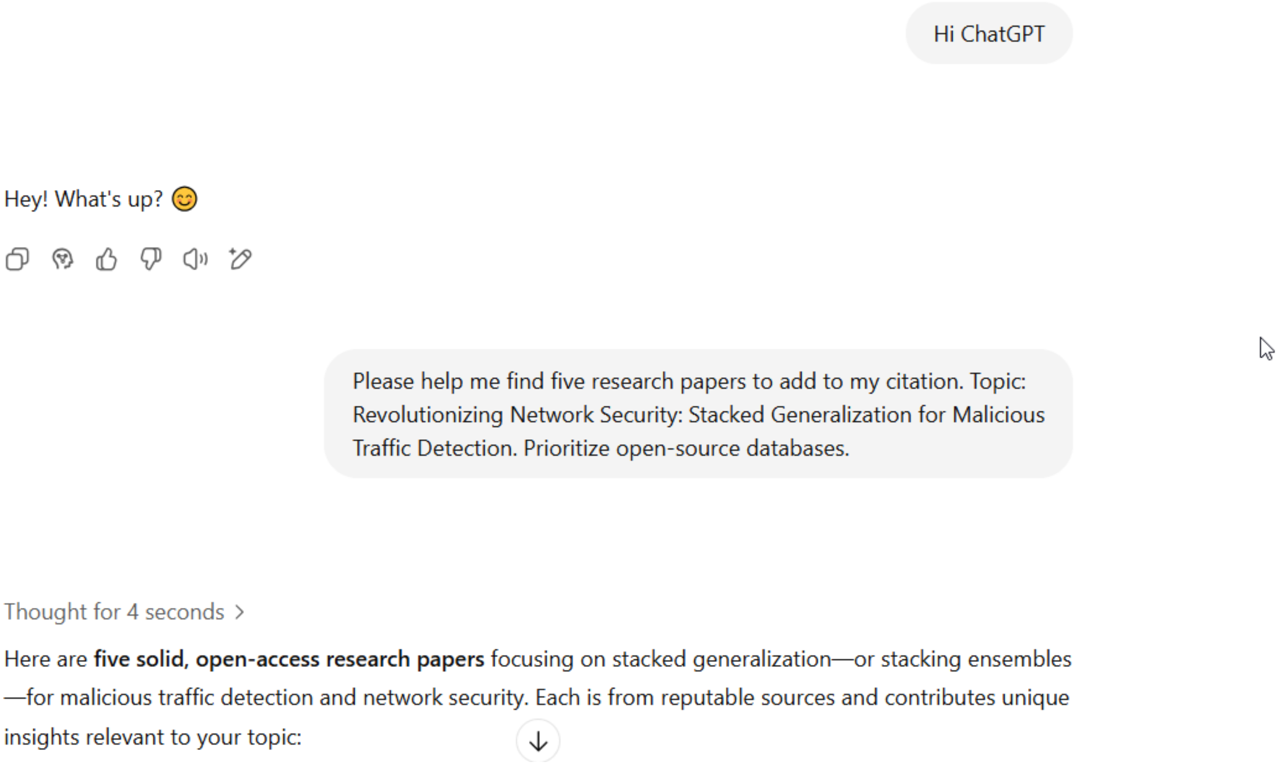

Hi ChatGPT

Hey! What's up? 😊

Please help me find five research papers to add to my citation. Topic: Revolutionizing Network Security: Stacked Generalization for Malicious Traffic Detection. Prioritize open-source databases.

Here are **five solid, open-access research papers** focusing on stacked generalization—or stacking ensembles—for malicious traffic detection and network security. Each is from reputable sources and contributes unique insights relevant to your topic:

📘 1. Malicious Traffic Detection in IoT and Local Networks Using Stacked Ensemble Classifier

- **Authors:** Pubudu et al. (2022)
- **Highlights:** Proposes "Extra Boosting Forest" (stacked ensemble combining Extra Trees, Gradient Boosting, and Random Forest) applied to merged IoT and local traffic datasets (UNSW-NB15 and IoTID20). Achieved ~98.5% accuracy using PCA for feature reduction researchoutput.csu.edu.au +10 .
- **Why include it:** Directly aligns with stacking methodologies on relevant datasets; open access.

📘 2. Web Attacks Detection Using Stacked Generalization Ensemble for LSTMs

- **Authors:** Lamrani Alaoui & Nf aoui (2023)
- **Highlights:** Utilizes Word2Vec embeddings and stacked LSTM ensembles for HTTP web request classification (CSIC-2010 dataset). Offers strong performance and efficiency with a deep-learning stacking approach researchgate.net +1 .
- **Why include:** Extends stacking to deep learning architectures—valuable for modern, application-layer malicious traffic detection.

📘 3. **Effective Network Intrusion Detection Using Stacking-Based Ensemble**

- **Authors:** Alamri et al./Springer (2023)
- **Highlights:** Demonstrates ~98.24% weighted F1-score on a new CIPMAIDS2023-1 dataset and CICIDS2017 using stacking (base models: SVM, KNN, RF; meta: XGBoost) link.springer.com +15 .
- **Why include:** Highlights the adaptability of stacking across diverse datasets and high performance with classical ML approaches.

📘 4. **SEDAT: A Stacked Ensemble Learning-Based Detection Model for Multiscale Network Attacks**

- **Authors:** Feng et al. (2024)
- **Highlights:** Introduces a stacked ensemble combining autoencoders and Random Forests to detect multiscale (light/medium/heavy, concealed) attacks. Demonstrates solid accuracy enhancement versus baselines on CIC-IDS2017 and UNSW-NB15 mdpi.com +4 .
- **Why include:** Unique focus on multiscale attack patterns and stacked learning—including unsupervised components—ideal for detecting sophisticated ↓ cious network behavior.

📘 5. **A Stacking Ensemble for Network Intrusion Detection Using Real-Time Dataset**

- **Authors:** Jain & Kumar (2020, Wiley)
- **Highlights:** Applies stacking ensembles in a real-time intrusion detection scenario; meta-learning improves base classifier predictions on real-world network flows onlinelibrary.wiley.com +15 .
- **Why include:** Offers empirical evidence for stacking's efficacy in practical, real-time NIDS environments.

🛠️ How to Use These in Your Work

Paper	Contribution	Relevance
Pubudu et al. (2022)	Ensemble of tree-based models	Real-world datasets, high accuracy
Lamrani & Nf aoui (2023)	LSTM stacking for HTTP web attacks	Deep learning adaptation
Alamri et al. (2023)	Stacking with XGBoost meta learner	Data generalization and meta-model design
Feng et al. (2024)	Autoencoder-enabled stacking for multiscale attacks	Unsup + sup ensemble structure
Jain & Kumar (2020)	Real-time stacked NIDS	Practical deployment validation