Difference between `.pkl` and `.h5` in Deployment Context

Aspect	.pkl (Pickle)	.h5 (HDF5)
Full Form	Pickle	Hierarchical Data Format version 5
Used with	scikit-learn, XGBoost	TensorFlow/Keras
Serialization Type	Python object serialization	Binary data format
Cross-language Compatibility	Limited (Python only)	Good (multi-language support)
Portability	Less portable	Highly portable
Model + Metadata	Model + pipeline/preprocessing	Architecture + weights + config
Security	Can execute code (unsafe if untrusted source)	Safer, no code execution
Example Use	`joblib.dump(model, 'model.pkl')`	`model.save('model.h5')`
Load Command	`joblib.load('model.pkl')`	`keras.models.load_model('model.h5')`

Deployment Context Summary

- **Use `.pkl`** for:
  - Traditional ML models (e.g., scikit-learn, XGBoost).
  - Pipelines that include preprocessing steps.
  - Python-only deployments.
- **Use `.h5`** for:
  - Deep learning models built with TensorFlow/Keras.
  - Cross-platform or cross-language model serving.
  - Scenarios requiring portability and structured metadata.