

Preface

The rapid advancements in deep learning have revolutionized both Natural Language Understanding (NLU) and Computer Vision (CV), significantly impacting cybersecurity applications. From detecting cyber threats in textual data to analyzing visual patterns for anomaly detection, deep learning architectures play a crucial role in securing digital infrastructures. This book explores cutting-edge deep learning models tailored for cybersecurity, covering transformer-based architectures for NLU and CNN-based, as well as hybrid models, for CV applications. We delve into adversarial attacks, threat intelligence, and robust model defenses, providing practical insights into securing AI-driven systems. Designed for researchers, practitioners, and security professionals, this book bridges the gap between AI advancements and cybersecurity challenges. Through theoretical foundations, real-world case studies, and hands-on implementations, we equip readers with the knowledge to leverage deep learning for cyber resilience. As threats evolve, so must our defenses—this book aims to be a guide in that ongoing battle.