RADemics

AI Based Anomaly Detection in Cybersecurity Using Python and Deep Autoencoders

R. Kranthi Kumar, I. Parvin Begum, Anusha C
VNRVJIET, B. S. ABDUR RAHMAN CRESCENT INSTITUTE OF SCIENCE AND TECHNOLOGY, T.J.S. ENGINEERING COLLEGE

AI Based Anomaly Detection in Cybersecurity Using Python and Deep Autoencoders

[1]R. Kranthi Kumar, Designation: Assistant Professor, CSE-(CyS, DS) and AI&DS, College: VNRVJIET, Mail id: kranthikumar.rudrarapu@gmail.com ,Mobile:99403 64303.

[2]I. Parvin Begum, Assistant Professor, Computer Applications B. S. Abdur Rahman Crescent Institute of science and Technology, Vandalur, Chennai- 600048. Mail id: parvin@cresint.education , Mobile no:824 800 2831.

[3]Anusha C, Assistant professor, EEE, T.J.S. Engineering college, TJS nagar, peruvoyal, near kavaraipettai, Gummidipoondi taluk, tiruvallur district, 601206 Mobile no.: 93615 95146, mail id: t.anushllaofficial05@gmail.com,

Abstract

The escalating frequency and sophistication of cyber threats have exposed critical limitations in traditional security mechanisms, necessitating the development of intelligent, adaptive, and data-driven approaches for anomaly detection. This book chapter presents a comprehensive exploration of deep autoencoder architectures integrated with Python-based frameworks to address the pressing challenges in cybersecurity anomaly detection. Emphasizing unsupervised learning paradigms, the chapter investigates how deep autoencoders can learn compact latent representations of normal behavior and effectively identify deviations through reconstruction errors. Various architectural variants, including convolutional, sparse, and attention-augmented autoencoders, are examined for their suitability in modeling complex, high-dimensional cyber data. Strategies for data preprocessing, feature engineering, threshold tuning, and model evaluation are detailed alongside visualization techniques for interpreting latent spaces and error distributions. The chapter also highlights implementation strategies using TensorFlow and Keras, applying these models to benchmark cybersecurity datasets such as KDDCup99 and UNSW-NB15. Finally, the discussion outlines current limitations, including model explainability, real-time scalability, and robustness to adversarial attacks, while offering future research directions to advance intelligent threat detection systems. This work contributes to the development of context-aware, interpretable, and scalable AI-based cybersecurity solutions.

Keywords: Anomaly Detection, Deep Autoencoders, Cybersecurity, Reconstruction Error, Python, Unsupervised Learning

Introduction

The increasing sophistication of cyberattacks has placed critical demands on modern information systems to remain resilient, adaptive, and secure [1]. Conventional intrusion detection systems (IDS) primarily depend on predefined rules, statistical thresholds, or signature databases, rendering them ineffective against novel and evolving threats [2]. These traditional systems struggle to detect previously unseen anomalies, such as zero-day attacks or polymorphic malware, due to their reliance on known behavioral patterns [3]. The growing volume, velocity, and variety

of data flowing through networks in real time challenge the scalability and responsiveness of manual or semi-automated security mechanisms [4]. Consequently, the cybersecurity domain requires intelligent systems capable of learning from data autonomously and responding dynamically to irregularities without explicit programming or human intervention [5].

Artificial intelligence (AI), and particularly deep learning techniques, have emerged as powerful tools to overcome these limitations in cybersecurity [6]. Among various deep learning models, deep autoencoders have gained prominence for their ability to detect anomalies in complex, high-dimensional datasets without labeled examples [7]. Autoencoders function by compressing input data into a lower-dimensional latent space and then reconstructing it as closely as possible [8]. When trained exclusively on benign data, the reconstruction error for normal inputs remains low, whereas anomalous or malicious inputs result in significantly higher error values. This inherent characteristic enables autoencoders to serve as robust anomaly detectors in environments where labeled attack data is sparse, imbalanced, or entirely unavailable [9]. Their unsupervised nature makes them particularly valuable in intrusion detection, fraud detection, and malware behavior analysis [10].

The architecture of deep autoencoders can be customized to suit different types of cybersecurity data and threat models [11]. Variants such as convolutional autoencoders are well-suited for spatially structured data like images or packet sequences, while recurrent and denoising autoencoders are preferred for time-series analysis and noise-resistant modelling [12]. Attention-augmented autoencoders introduce contextual awareness by assigning dynamic weights to input features, thereby enabling the network to prioritize critical components during encoding and reconstruction [13]. These architectural adaptations not only enhance the precision of anomaly detection systems but also allow for better generalization across diverse data sources, such as network traffic, system logs, authentication records, and access control data [14]. The flexibility in architectural design ensures that autoencoders can be adapted to varying cybersecurity use cases and evolving threat landscapes [15].