

Intelligent Anomaly Detection in Network Traffic Using Deep Autoencoders for Real-Time Cybersecurity Threat Identification

Garba Naif Yusuf

Department of Electrical Engineering, Faculty of Engineering, University of Jos, Jos, Nigeria

P. L. Damuut

Professor, Department of Electrical Engineering, Faculty of Engineering, University of Jos, Jos, Nigeria

Dr. E. M. David

Department of Electrical Engineering, Faculty of Engineering, University of Jos, Jos, Nigeria

Sulaiman Muhammad Adejo

Department of Electrical Engineering, Faculty of Engineering, University of Jos, Jos, Nigeria

Abubakar Sadiq Yusuf

Department of Computer Science, Ahmadu Bello University, Zaria, Nigeria

Abstract:

The escalating sophistication and frequency of cyberattacks pose a critical threat to organisations worldwide, with adversaries increasingly capable of bypassing conventional defence mechanisms. Traditional signature-based intrusion detection systems (IDS), while effective against catalogued threats, are fundamentally incapable of detecting zero-day exploits, polymorphic malware, and advanced persistent threats. Conversely, conventional anomaly-based approaches suffer from excessive false positive rates that overwhelm security operations centre (SOC) analysts, degrade operational efficiency, and erode trust in automated detection. The rapid expansion of networked infrastructure—including cloud services, software-defined networking, and Internet of Things (IoT) ecosystems—has further amplified the volume and complexity of network traffic, rendering manual analysis impractical. There is therefore a pressing need for intelligent, computationally efficient anomaly detection systems that can operate in real time, adapt to evolving network conditions, and detect novel threats without reliance on predefined attack signatures.

Keywords:

Intrusion detection system, deep learning, autoencoder, anomaly detection, network security, cybersecurity, real-time detection, CICIDS2017, unsupervised learning, denoising autoencoder, sparse autoencoder, variational autoencoder.