This abstract takes a comprehensive look at AI-enhanced intrusion detection systems in the context of today's cyber threats. In the modern landscape, where computer networks serve as the backbone of organizations, the need for effective intrusion detection is urgent. Traditional methods often struggle when faced with the complexities of contemporary cyber threats, resulting in false alarms and delayed threat identification. This article delves into the crucial role played by big data technologies like Hadoop and Spark that provide scalable and efficient solutions for managing vast data volumes, enabling thorough analysis of network activities and the discovery of hidden threat patterns. AI-enhanced intrusion detection systems, powered by machine learning algorithms, mark a transcendental shift in the field of cybersecurity. These systems continually adapt to counter emerging threats, perform real-time analysis of network traffic to detect anomalies, and refine the precision of threat detection while decreasing false alarms. As AI and big data technologies advance, AI-enhanced intrusion detection systems become crucial for protecting communication networks against unauthorized access. This emphasizes the profound importance of data integrity and network security in an era characterized by the constant evolution of cyber threats.