In today's rapidly evolving technological landscape, computer networks serve as the lifeblood of organizations, housing invaluable data and critical national defense systems. Unfortunately, this very significance makes them prime targets for relentless and sophisticated hackers who constantly seek unauthorized access to compromise databases and acquire sensitive information. This relentless onslaught of cyber threats underscores the urgent need for robust intrusion detection systems. However, these systems face an ever-increasing data deluge as networks and hosts process vast amounts of information every second, making the swift and accurate detection of intrusions a daunting challenge. To counter these evolving threats, the integration of big data techniques and artificial intelligence (AI) has become pivotal in the development of intrusion detection systems. Traditional methods, often rule-based or signature-based, struggle to keep up with the intricacies of modern cyber threats, leading to false positives and delayed threat detection. Big data technologies, such as Hadoop and Spark, have ushered in a new era for intrusion detection, offering scalable and efficient solutions for managing the vast data volumes encountered by networks, enabling comprehensive analysis of network activities, and uncovering hidden threats and patterns that elude conventional methods. AI-enhanced intrusion detection systems, powered by machine learning algorithms, represent a transformative leap in cybersecurity. They adapt and evolve to counter evolving threats, analyze network traffic in real-time for anomalies, and deliver faster, more accurate threat detection while reducing false positives. As AI and big data technologies continue to advance, these systems play an increasingly crucial role in safeguarding communication networks against unauthorized access, acknowledging the profound significance of data integrity and network security in an era where cyber threats are in constant flux.