Abstracts on Cloud Computing and Cybersecurity

Cloud Computing

Cloud computing is a transformative paradigm in information technology that enables on-demand access to a shared pool of configurable computing resources such as servers, storage, applications, and services. This model promotes scalability, flexibility, and cost-efficiency by allowing users to access and manage resources remotely over the internet. It supports multiple service models-including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)-catering to a wide range of organizational needs. Despite its benefits, cloud computing poses challenges related to data privacy, service reliability, and vendor lock-in. This paper explores the architecture, deployment models, benefits, and risks of cloud computing, with an emphasis on current trends and its role in modernizing business and IT operations.

Cybersecurity

Cybersecurity refers to the practice of protecting systems, networks, and data from digital attacks, unauthorized access, and damage. In an era where digital transformation is accelerating, the importance of cybersecurity has become paramount across all sectors. Cyber threats such as malware, phishing, ransomware, and advanced persistent threats (APTs) continue to evolve, targeting both individuals and organizations. This paper discusses the fundamental concepts, principles, and practices of cybersecurity, including encryption, firewalls, intrusion detection systems, and risk management strategies. It also examines recent developments in threat intelligence, ethical hacking, and cybersecurity frameworks, emphasizing the need for a proactive and adaptive security posture in today's interconnected digital world.