IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

Cyber Security Threats

Prof. Shradha Wankhede[1], Prof. Priyanka Choudhary[2], Mr.Vishal Balsaraf[3]
Assistant Professor, Dept. of Computer Science and Engineering[1,2]
Student, Dept. of Computer Science and Engineering[3]
Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur Maharashtra, India
shradha.cse@tgpcet.com, priyankac.cse@tgpcet.com, vishalbalsaraf8474@gmail.com

Abstract: *The relentless advancement of digital infrastructures has precipitated an era of unprecedented cyber vulnerabilities, wherein industries grapple with an ever-evolving array of sophisticated threats. Adversaries employ algorithmically enhanced offensive cyber mechanisms, leveraging artificial intelligence, adversarial machine learning, and polymorphic malware to circumvent conventional security paradigms. The advent of Ransomware-as-a-Service (RaaS) has further exacerbated the threat landscape, democratizing cybercriminal capabilities and enabling the proliferation of highly adaptive extortion campaigns. Concurrently, the integration of hyperconnected ecosystems—spanning cloud-native architectures, ubiquitous IoT deployments, and the pervasive rollout of 5G networks—has exponentially expanded the digital attack surface, rendering legacy security frameworks obsolete.*

Keywords: Ransomware-as-a-Service (RaaS), Cloud-native architectures, IoT deployments, 5G networks

DOI: 10.48175/IJARSCT-25939