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

Smart Devices, Smarter Threats: Cyber security Implications of IoT in Modern Classrooms

Dr. Pradeep Kumar Tiwari and Mr. Vivek Dhiman
Associate Professor & Head, Department of Education, Sikkim Skill University, Sikkim[1]
Head, Department of Civil Engineering , Sikkim Skill University, Sikkim[2]
drpradeeptiwarikavi@gmail.com and vivekdhiman121@gmail.com

Abstract: • *The adoption of Internet of Things (IoT) devices in modern classrooms has accelerated rapidly, transforming traditional education into an interactive, data-driven experience. Tools such as smartboards, connected tablets, wearable tech, and AI-enabled learning platforms are being widely integrated to enhance teaching efficiency and student engagement. However, as classrooms become increasingly connected, they also become more vulnerable to cyber threats. This research investigates the cyber security implications of IoT usage in educational settings, with the objective of identifying common vulnerabilities, assessing risk management practices, and exploring the preparedness of schools in protecting sensitive data. The study emphasizes the urgency of implementing tailored cyber security strategies to safeguard both institutional and student data from unauthorized access, data breaches, and exploitation.*

The research follows a qualitative, exploratory methodology. Data was collected through case study analysis, expert interviews, and review of secondary sources such as academic journals, government reports, and industry whitepapers from 2018 to 2024. Key sources include publications from the National Institute of Standards and Technology (NIST), cyber security firms like Kaspersky and Cisco, and educational technology policy documents. The findings reveal significant gaps in cyber security awareness, inadequate infrastructure, and the absence of IoT-specific security protocols in many schools. Most educational institutions still rely on generic IT policies that do not address the unique risks posed by IoT ecosystems, such as insecure default settings, lack of encryption, and weak network segmentation. The study concludes that a more robust, proactive approach is necessary—one that includes stricter procurement policies, regular risk assessments, and comprehensive training for educators and administrators. Effective cyber security in IoT-enhanced classrooms must go beyond technical solutions and involve a cultural shift towards greater digital responsibility and informed usage. The research recommends that education stakeholders develop frameworks that align with both technological innovation and cyber security resilience to ensure safe, inclusive, and future-ready learning environments...

Keywords: Internet of Things**,** cyber security resilience, National Institute of Standards and Technology, digital responsibility, AI-enabled learning platforms

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-25979