

ABSTRACT

In today's digital landscape, cybersecurity has become a dominant concern due to the increasing complexity and sophistication of cyber threats. The growing volume of information and data stored by individuals, businesses, organizations, and governments has made them prime targets for cyberattacks. In response, Artificial Intelligence (AI) has emerged as a powerful tool for strengthening cybersecurity defenses. AI plays a crucial role in identifying and mitigating threats in real time, offering detection and response capabilities at a scale that traditional security measures cannot achieve due to their reliance on rule-based systems rather than adaptive learning. One of AI's key contributions to cybersecurity is the development of automated incident response systems, which enhance security while incorporating human oversight to improve effectiveness and reliability. This seminar explores AI's capabilities, impact, and limitations in cybersecurity, highlighting its role in risk mitigation and ethical considerations. Through currently existing tools and information about them, the seminar provides valuable insights into AI's evolution and implications, paving the way for future advancements in cybersecurity.

Keywords: Artificial Intelligence (AI), Cybersecurity, Threat Detection, Real-Time Response, Automated System, Ethical AI, Machine Learning, AI Techniques.

Index

Sr. No	Topic	Page No.
1	Introduction	1-3
1.1	Scope	2
1.2	Shifting from Reactive to Proactive Security:	2-3
1.3	Real-time Threat Detection:	3
1.4	Vulnerability Management:	3
2	Objectives	4
3	AI's Role in Cybersecurity	5-6
4	Key AI Technologies and Algorithms	7-9
5	AI Applications at various systems.	10-11
6	AI Driven Tools	12-14
7	Impact & Benefits of AI in Cybersecurity	15-17
8	Challenges & Limitations of AI in Cybersecurity	18-20
9	Conclusion	21
10	References	22