**Summary of Research:**

**Research Overview**

The research focused on the increasing prevalence of cybersecurity threats in healthcare, driven by the digitization of sensitive medical records and operational systems. It emphasized the vulnerabilities specific to the healthcare sector, such as legacy systems, interconnected devices, and the critical need for operational continuity. The analysis covered:

1. **Digital Threat Landscape**:
   * Growth in cyber threats, fueled by the increasing volume, variety, and velocity of attacks.
   * Healthcare's unique risks due to reliance on legacy systems and sensitive patient data.
2. **Current Threats in Healthcare**:
   * Data breaches, ransomware, phishing, and IoT device vulnerabilities were highlighted as major concerns.
3. **Modes of Cyber Attacks**:
   * Explored attack techniques including malware, phishing, insider threats, DDoS, and supply chain compromises.
4. **Impact on Healthcare**:
   * Detailed operational, financial, and reputational consequences of cyberattacks on hospital systems.
5. **Defense Strategies**:
   * Proposed proactive measures (e.g., employee training, system upgrades), response planning, and regulatory compliance.
6. **Strategic Recommendations**:
   * Advocated for implementing Zero Trust Architecture, real-time monitoring, and collaboration with cybersecurity experts.