# Transcript

# Cybersecurity Threats in Internet of Medical Things (IoMT)

## Slide 1 – Title

Good day everyone. Today, I’ll be presenting on Cybersecurity Threats in the Internet of Medical Things (IoMT): Challenges and Responses in the Healthcare Sector. This topic explores how connected medical devices are transforming healthcare — but also how they introduce new cybersecurity risks that require urgent attention.

## Slide 2 – Introduction

The Internet of Medical Things, or IoMT, is rapidly reshaping healthcare by enabling real-time patient monitoring and personalized medical care. However, as IoMT devices become more widespread, they also expand the attack surface for cyber threats. This presentation focuses on identifying IoMT vulnerabilities and assessing how current defense mechanisms protect the CIA triad — confidentiality, integrity, and availability — which are essential for maintaining trust in healthcare systems.

## Slide 3 – Research Questions

This study aims to answer three main questions:  
1. What are the major cybersecurity threats affecting IoMT systems?  
2. How effective are current security frameworks and technologies in addressing these threats?  
3. What strategies can enhance the long-term resilience of IoMT infrastructures?

## Slide 4 – Methodology and Source Selection

The research draws on peer-reviewed journals, IEEE and MDPI publications, and recent studies from 2021 to 2025. A systematic review method was used to identify challenges, security mechanisms, and emerging technologies in IoMT cybersecurity.

## Slide 5 – IoMT in Healthcare: An Overview

IoMT integrates sensors, communication networks, cloud infrastructures, and intelligent algorithms to support telehealth and data-driven care. It enables doctors to monitor patients remotely, improving efficiency and outcomes. The IoMT market is projected to reach USD 285 billion by 2029, indicating its massive global adoption and importance.

## Slide 6 – Types of IoMT Devices and Applications

IoMT applications range from:  
- Wearable sensors that track vital signs in real time.  
- Implantable devices such as pacemakers and insulin pumps.  
- Medical imaging systems like MRI and CT scanners.  
- Hospital management networks for centralized diagnostics and resource allocation.  
Each of these introduces unique security risks.

## Slide 7 – Key Cybersecurity Threats

Major IoMT threats include:  
- Malware attacks – malicious software that disrupts or spies on device operations.  
- Denial-of-Service (DoS) – overloading servers to cause outages.  
- Supply chain attacks – exploiting vulnerabilities in third-party vendors.  
- Insider threats – employees misusing access privileges (Bughio et al., 2024).  
These threats can compromise patient safety and data integrity.

## Slide 8 – Human Factors and Legacy Systems

Human error remains a leading cause of security breaches. Many healthcare systems rely on outdated legacy infrastructure that lacks modern protection protocols. Limited awareness and training among healthcare professionals further increase vulnerability.

## Slide 9 – Compliance and Regulatory Challenges

Different regions have inconsistent regulatory frameworks for IoMT cybersecurity. While standards like HIPAA and GDPR exist, their enforcement and interpretation vary. This leads to uneven data protection and compliance issues across healthcare systems.

## Slide 10 – Security Solutions and AI Innovations

Technologies such as AI, blockchain, and federated learning are emerging as strong defense mechanisms. AI can detect anomalies in real time, while blockchain ensures data integrity and traceability. Federated learning enables decentralized model training without exposing raw patient data.

## Slide 11 – AI and Federated Learning

AI-based threat detection systems require minimal human input but face challenges such as limited transparency and heavy computational costs (Shree et al., 2024). Future improvements must focus on explainable AI and energy-efficient models to enhance trust and scalability.

## Slide 12 – Implementation Challenges

Implementing IoMT cybersecurity measures is complex due to high costs, interoperability issues, and a shortage of cybersecurity professionals in healthcare. Collaboration between IT teams, clinicians, and policymakers is often weak, resulting in delayed responses to cyber incidents.

## Slide 13 – Critical Evaluation of Current Research

While research has advanced rapidly, most studies remain theoretical or lab-based. There is limited validation of these models in real clinical environments, which raises questions about their real-world reliability.

## Slide 14 – Research Gaps and Future Directions

Future studies should explore long-term security impacts, ethical implications, and scalable frameworks for IoMT protection. They should also investigate secure-by-design principles for medical devices and ensure continuous cybersecurity training for healthcare professionals.

## Slide 15 – Strategic Recommendations

Key recommendations include:  
- Enforcing secure-by-design practices for all IoMT devices.  
- Providing ongoing cybersecurity training for medical staff.  
- Encouraging cross-industry collaboration among regulators, hospitals, and manufacturers.  
- Developing AI-driven monitoring systems that are transparent and auditable.

## Slide 16 – Conclusion

IoMT has the power to revolutionize healthcare delivery but also introduces complex cybersecurity risks. Technologies like AI and blockchain hold promise, yet they face ethical and technical challenges. A collaborative, multi-stakeholder approach is essential to ensure that IoMT remains safe, secure, and trustworthy.

.