# Privacy and Security Issue in Healthcare

TEAM MEMBERS

ATHARVA PAWAR

ADITYA VYAS

HARSHVARDHAN TRIVEDI

# Index

- Introduction
- IOMT Based Health Care
- Security & Privacy Challenges
- Add your third bullet point here
- State of Art Security Research
- Future Research
- Conclusion

# Introduction

Healthcare is a critical sector that deals with sensitive personal information, making it a prime target for cyberattacks. This presentation will discuss the privacy and security issues in healthcare, with a focus on the Internet of Medical Things (IoMT).

Importance of privacy and security in healthcare: Privacy and security are essential for protecting patients' personal health information, ensuring the integrity of medical devices and systems, and maintaining trust in the healthcare system.

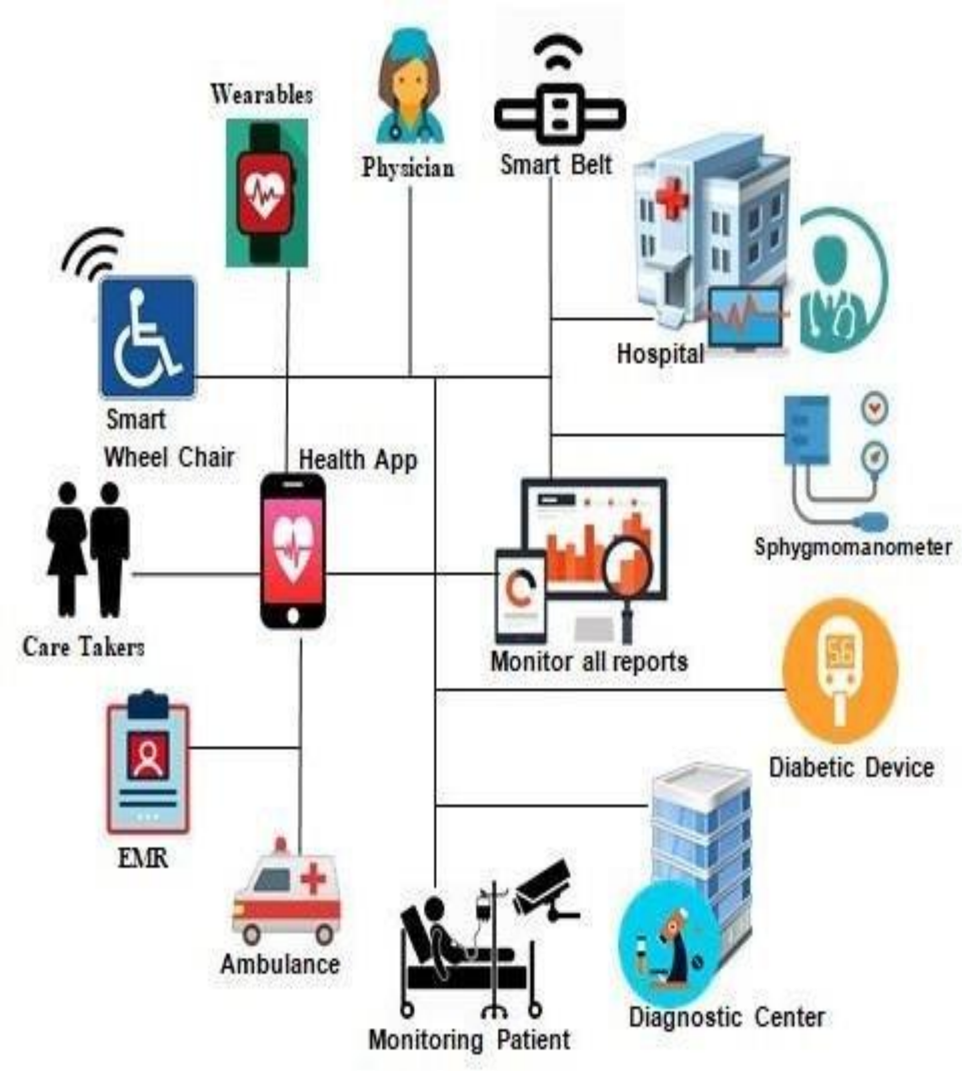
The purpose of this presentation is to raise awareness of the privacy and security challenges in healthcare, provide an overview of the IoMT-based healthcare systems, and discuss the state-of-the-art security research and future research directions.

# IOMT Based Healthcare

The Internet of Medical Things (IoMT) refers to the network of medical devices, wearables, and sensors that are connected to the internet and can collect, store, and transmit health data.

IoMT-based healthcare systems enable remote patient monitoring, real-time health data analysis, and personalized healthcare services. They can improve the quality of care, reduce healthcare costs, and enhance patient outcomes.

IoMT-based healthcare systems offer many benefits, such as improved patient engagement, better disease management, and more efficient healthcare delivery. However, they also pose several challenges, such as data privacy and security risks, interoperability issues, and regulatory compliance.



# Security & Privacy Challenges

# Challenges in IOMT

IoMT-based healthcare systems face various security and privacy challenges, such as unauthorized access, data breaches, malware attacks, and data leakage

The threats to IoMT-based healthcare systems include cybercriminals, hacktivists, insiders, and nation-state actors. They can exploit vulnerabilities in medical devices, networks, and applications to steal sensitive health data, disrupt healthcare services, or cause physical harm to patients.-

Some example include some real-life examples of security breaches in healthcare, such as the WannaCry ransomware attack on the UK's National Health Service (NHS) in 2017, which affected over 200,000 computers and disrupted patient care, or the data breach at Anthem Inc. in 2015, which exposed the personal information of 78.8 million individuals.

# Requirements for IOMT

To address the security and privacy challenges in IoMT-based healthcare systems, several security and privacy requirements need to be met. These requirements can be classified into data-level, network-level, and medical server-level requirements

Data-level security and privacy requirements include data encryption, access control, data integrity, and data anonymization.

Network-level security and privacy requirements include secure communication protocols, network segmentation, intrusion detection and prevention, and network monitoring.

Medical server-level security and privacy requirements include secure authentication and authorization, secure storage and backup, and disaster recovery.

# State of the Art Security Research

Machine learning and deep learning can be used to detect anomalies in medical data, identify potential security threats, and predict security breaches.

Biometric authentication can be used to enhance the security of medical devices and systems by using unique physiological or behavioral characteristics of individuals, such as fingerprints, iris scans, or voice recognition.

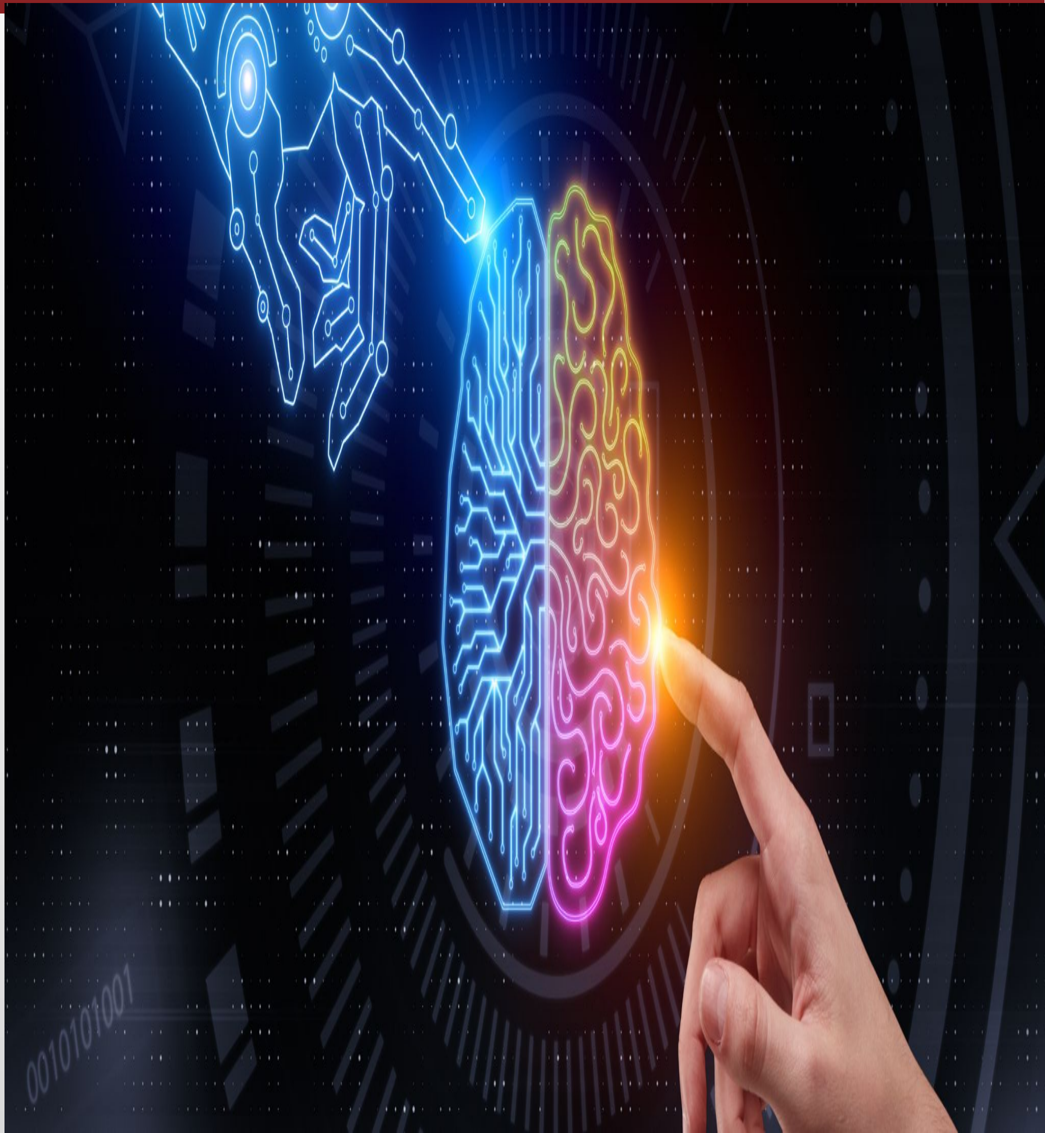
Implantable security schemes can be used to secure medical devices that are implanted in the human body, such as pacemakers or insulin pumps.

# Future Research

The emerging technologies and future research directions are in IoMT security and privacy, such as blockchain, edge computing, and privacy-preserving machine learning.-

Emerging technologies such as blockchain can be used to secure medical data and transactions, while edge computing can be used to process medical data closer to the source and reduce latency and bandwidth requirements.

The challenges and opportunities for future research in IoMT security and privacy, such as the need for interoperability standards, the trade-off between security and usability, and the ethical and legal implications of using personal health data.



# Conclusion

This Topic summarizes the main points discussed in the previous slides, such as the security and privacy challenges in IoMT-based healthcare systems, the security and privacy requirements for IoMT, the state-of-the-art security research, and the future research directions.-

The importance of privacy and security in healthcare and the need for healthcare providers and policymakers to prioritize at the earliest

This topic also discusses the potential of biometrics and its applications for securing IoMT healthcare systems, as well as the security schemes for implantable IoMT devices.

# THANK YOU