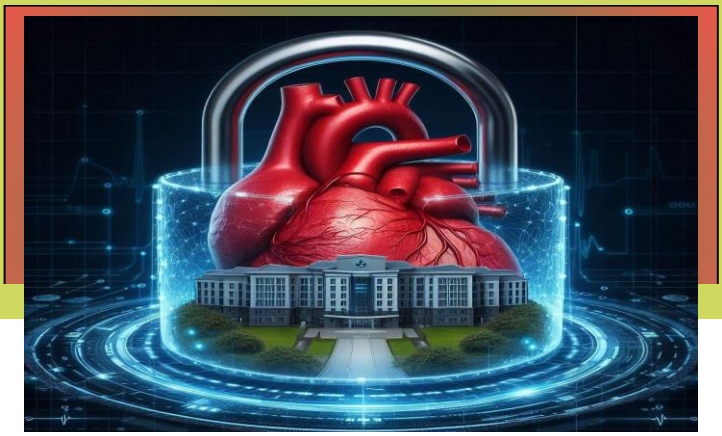
iNTELEGRID Newsletter

January, 2024



AI HOSPITALS

How to innovate cardiology department with AI: from diagnosis to treatment and beyond

Today, a wide range of AI systems are available for the diagnosis and treatment of cardiology, including:

1. AI algorithms for coronary calcium detection and quantification: These are AI systems that can automatically measure the amount of calcium in the coronary arteries from CT scans, which is a marker of atherosclerosis and cardiovascular risk. An example of this is via VB50 Siemens Healthineers.
2. AI systems for automated plaque detection and stenosis severity quantification: These are AI systems that can identify and measure the degree of narrowing or blockage of the coronary arteries from angiogram videos, which can help diagnose coronary artery disease (CAD) and guide treatment decisions. An example of this is AI-Heart, Siemens Healthineers.
3. AI systems for coronary ML CT-FFR assessment: These are AI systems that can estimate the blood pressure and flow across the coronary arteries from CT scans, which can help assess the functional significance of coronary lesions and the need for revascularization. An example of this is the CT-FFR prototype, Siemens Healthineers.
4. AI systems for cardiac image interpretation and diagnosis: These are AI systems that can analyze various types of cardiac images, such as echocardiograms, MRI, and PET, and provide diagnostic information, such as cardiac function, structure, perfusion, and metabolism. An example of this is Mayo Clinic AI Cardiology.
5. AI systems for cardiovascular risk prediction and prognosis: These are AI systems that can use various types of data, such as clinical, genetic, and lifestyle factors, to predict the likelihood of developing or worsening cardiovascular diseases, such as heart failure, arrhythmias, and stroke. An example of this is Frontiers in Cardiovascular Medicine.
6. AI systems for cardiac arrhythmia detection and management: These are AI systems that can monitor and analyze the heart rhythm from wearable devices, such as smartwatches and patches, and detect and alert the presence of abnormal or dangerous arrhythmias, such as atrial fibrillation, ventricular tachycardia, and cardiac arrest. An example of this is the Apple Watch.
7. AI systems for heart failure diagnosis and treatment: These are AI systems that can help diagnose and treat heart failure, a condition where the heart cannot pump enough blood to meet the body's needs, by using data from sensors, biomarkers, and medical records and providing personalized recommendations, such as medication, diet, and exercise. An example of this is artificial intelligence in coronary computed tomography and angiography.

In fact, artificial intelligence (AI) is a potent and exciting weapon that has the potential to improve and revolutionize cardiology in a number of domains, including diagnosis, therapy, and beyond. AI can assist cardiologists in customizing and optimizing patient treatment and

CYBER INSURANCE IN HEALTHCARE

K S Jayamohan,
Cyber Insurance Consultant

Cyber insurance covers losses and damages from security incidents affecting an organization's network or data. Healthcare businesses can use it to cover costs like legal fees, data recovery, reputational harm, and service interruption. However, it is not a replacement for investing in cybersecurity measures. Cyber insurance only partially offsets financial losses, not reducing damage to patients, employees, or business operations. To protect data and systems, healthcare companies should develop strong cybersecurity policies. Factors to consider when selecting a policy include coverage scope, premiums and deductibles, and security best practices and standards. HDFC Bank, a leading private sector bank in India, offers customizable Cyber Sachet Insurance, available online or through the HDFC Bank mobile app, with instant policy issuance and 24x7 cyber assistance.

discoveries and advancements. However, there are also serious hazards and obstacles associated with AI that must be addressed. These include problems with data integration, quality, validation, and ethics as well as legal and ethical concerns. Therefore, the future of cardiology with AI requires a human-centered approach that balances the needs and expectations of all stakeholders, as well as the technical and ethical aspects of AI. By doing so, AI can become a valuable and trusted ally for cardiologists and patients, and pave the way for a smarter and healthier future.

HOSPITALS MUST HAVE CYBERSECURITY; IT IS A MUST, NOT OPTIONAL. IT MUST BE INTEGRATED AS SECURITY DURING THE HDO DESIGN PHASE, ADHERING TO THE PRINCIPLES OF CYBER-INFORMED ENGINEERING (CIE) AND SEAMLESSLY MAINTAINED. IN ORDER TO PREVENT HARM TO PATIENTS AND A LOSS IN PATIENT TRUST, HOSPITALS NEED TO ACT SWIFTLY.

AI HOSPITALS: FUTURE CYBERSECURITY CHALLENGES FOR A CLINICAL ENGINEER

Cybersecurity is a crucial aspect of healthcare, especially in the context of artificial intelligence (AI) and medical devices. Clinical engineers, who are responsible for testing, and maintaining medical devices and systems, face various cybersecurity challenges in an AI hospital. Some of these challenges are:

1. *Ensuring the safety and reliability of AI-based medical devices, such as pacemakers, insulin pumps, or radiology systems, that may be vulnerable to cyberattacks or malfunction due to algorithmic errors or data quality issues.*
2. *Protecting the privacy and security of patient data, which is often used to train and improve AI models, from unauthorized access, misuse, or breach by hackers or malicious actors.*
3. *Complying with the regulatory and ethical standards for AI in healthcare, which may vary across different jurisdictions and domains and may not be fully aligned with the existing legislation for medical devices.*
4. *Keeping up with the rapid pace of innovation and evolution of AI technologies may require constant updating, testing, and monitoring of medical devices and systems, as well as continuous learning and adaptation by clinical engineers.*

These are some of the upcoming cybersecurity challenges that clinical engineers may face in an AI hospital. To address these challenges, clinical engineers need to collaborate with other stakeholders, such as AI developers, healthcare providers, regulators, and patients, and adopt a holistic and proactive approach to cybersecurity in healthcare.

AIIMS CYBERATTACK 2022

THE INVESTIGATING TEAM DISCOVERED THAT SERVERS AT AIIMS DELHI WERE THE FOCUS OF A CYBERATTACK WITH ORIGINS ABROAD. THE IP ADDRESSES OF TWO EMAILS ORIGINATED IN THE CHINESE PROVINCE OF HENAN AND IN HONG KONG. THESE EMAIL EXCHANGES WERE EASIER TO IDENTIFY THANKS TO THE HEADERS OF THE FILES THAT THE HACKERS ENCRYPTED. THE IDENTITY OF THE INDIVIDUAL, GROUP, AND EXACT LOCATION OF INDIVIDUALS INVOLVED IN THE CYBERATTACK IS STILL UNKNOWN. EVEN WITH THE INDIAN GOVERNMENT'S RECENT EFFORTS TO DIGITIZE HEALTHCARE, THE AIIMS CYBERATTACK POST-MORTEM PRIMARILY REVEALED A TALE OF MEDICAL ADMINISTRATION INCOMPETENCE. THE MAIN EXAMPLES OF NEGLIGENCE THAT WERE NOTABLE WERE:

DESPITE THE NATIONAL INFORMATICS CENTRE'S (NIC) RECOMMENDATION, THE AIIMS DEPARTMENT IN CHARGE OF IT INFRASTRUCTURE DID NOT HAVE ACCESS TO DATABASE, SECURITY, AND SYSTEM ADMINISTRATORS.

THERE WAS NO DISASTER BACKUP SYSTEM TO PROVIDE BUSINESS CONTINUITY IN THE CASE OF A PRIMARY SITE FAILURE, WHICH WOULD HAVE DEMONSTRATED CYBER-RESILIENCE.

BETWEEN AIIMS AND THE NIC, THERE WAS NO SERVICE-LEVEL AGREEMENT THAT WOULD HAVE HELD THE LATTER RESPONSIBLE FOR ANY SERVICE BREAKDOWNS. ALTHOUGH IN PRACTISE NO SUCH CHANGES WERE MADE OVER TIME, AIIMS MANAGED ITS OWN SERVERS AND WAS IN CHARGE OF UPDATING SERVER OPERATING SYSTEMS AND SECURITY SOFTWARE.

AIIMS NEVER PRIORITIZED CYBER-SAFETY AND RESILIENCE, DEMONSTRATING THE ABSENCE OF A CYBER-SECURITY CULTURE. THIS CLAIM IS SUPPORTED BY THE FOLLOWING FACTS: (A) NO WORKSHOPS OR SEMINARS WERE HELD TO TEACH MEDICAL IT WORKERS AND DOCTORS ABOUT CYBER HYGIENE; (B) NO NIC-RECOMMENDED SECURITY AUDITS WERE CONDUCTED; AND (C) NUMEROUS MEDICAL STAFF MEMBERS USED PERSONAL GMAIL ACCOUNTS RATHER THAN THEIR OFFICIAL AIIMS EMAILS FOR WORK-RELATED PURPOSES.

Using human heart cells produced from stem cells and micro-scale 3D printed acrylic components, researchers at Boston University have built the miniPUMP, a spontaneously beating 3D printed miniature human heart. Without using human subjects, researchers may examine how diseases affect the human body, how drugs interact with it, and how the heart chamber copy performs. Without involving human subjects in research, the miniPUMP can monitor heart growth, the impact of diseases, and the efficacy of novel treatments. The tool makes significant advancements in cardiac tissue engineering and regenerative medicine conceivable by enabling researchers to track the course of a disease in a manner not previously achievable.

PRACTICING PHYSICIANS AND CYBER SECURITY

Hospital cyber-security is a shared responsibility of all the stakeholders, including the practicing physicians and surgeons. In a major hospital that uses PACS, IoMT, robotic surgery, telemedicine, etc., practicing physicians and surgeons should take the following measures in ensuring hospital cyber-security without fail.

Adopt the hospital's security guidelines approved by the director board, which include creating strong passwords, securing their devices, and reporting any occurrences or behaviors that seem suspicious. Avoid clicking on any dangerous links or attachments and being alert to potential cyber threats and attacks that could impact the hospital, such as ransomware, phishing, and denial-of-service attacks. Utilize techniques like encryption, access control, firewalls, and other security measures to protect the privacy, availability, and integrity of patient data and medical device data. Regularly update and backing up these systems is also important. Request advice and assistance from the CISO, and hospital's security officers and specialists, as well as educating and training themselves and their colleagues on the value of and best practices for cyber-security. Participate and collaborate in the security initiatives and projects of the hospital, such as conducting risk assessment, implementing security by design, cyber informed engineering and developing security awareness and culture.

According to some studies and experts, the interaction and coordination gap between the doctors community and the CISO (Chief Information Security Officer) is one of the factors that can contribute to the vulnerability and risk of cyberattacks in hospitals. Hospital cyber-security can also be impacted by other factors, including the lack of knowledge and training among doctors, nurses, and paramedical staff, the complexity and diversity of ICT systems and devices, financial and regulatory constraints, and the sophisticated and ever-evolving nature of cyber threats and attacks. Therefore, it is important to address all these factors and to adopt a holistic and collaborative approach to enhance the hospital cyber-security. There are some specific cyber-security standards or declarations that are relevant for doctors to adopt cyber-security practices in hospitals. Some of them are:

1The Digital Personal Data Protection Act, 2023 regulates the processing of digital personal data in India, including health data. It requires data fiduciaries to obtain consent, provide access rights, ensure data security, and report breaches to the Data Protection Authority of India. The ISO/IEC 27001 Standard outlines information security management systems for organizations, protecting sensitive data from cyber threats. The Declaration of Helsinki, adopted by the World Medical Association, upholds privacy and confidentiality in medical research.

Hospitals should invest in tailored cybersecurity training programs for doctors and nurses to address their specific needs and challenges. These programs should cover secure access to ICT systems, protecting patient data, preventing cyber threats, and following security regulations. The CISO should provide training in various formats, including online courses, webinars, workshops, and simulations. Regular updates are necessary to ensure the training remains relevant and effective in protecting the hospital and patients from cyber threats.

WHY MEDJACKING IS MORE THAN JUST A SCARY WORD

Hackers have found another way to extort the medical community and their patients called medjacking or medical device highjacking. A disturbing trend of cybercriminals targeting medical devices in doctors' offices and hospitals. Medjacking, the practise of hacking a medical device with the intent to harm or threaten a patient, has been called a ticking time bomb. Cyber-attacks on life-saving medical devices such as heart pacemakers present a very real threat and could come from terrorist groups or even nation states, according to a new World Economic Forum report on cyber risk. Medjacking has been reported in media and research, including a 2015 security flaw in an infusion pump that allowed hackers to remotely control the pump, alter dosage, or stop infusions. In 2016, The Shadow Brokers leaked hacking tools, including ETERNALBLUE, which were used in ransomware attacks like WannaCry and NotPetya, disrupting healthcare services and putting patients at risk. In 2017, researchers demonstrated how to hack into pacemakers, causing fatal shocks and extracting sensitive information, affecting over 8,000 different types.

Medjacking is alarming. Hacking of medical devices, such as X-ray systems, CT scanners, implantable defibrillators, and insulin pumps, with the intent to harm the patient or steal their data. Medjacking poses a serious threat to the health and privacy of patients, as well as the security and reputation of health care systems. Medjacking can be prevented by using devices with high cybersecurity standards, encrypting data transmissions, and separating the networks of different devices.

> **“The hospitals are in desperate need of a cyber-hygiene injection.”**
>
> — Dr. James Scott, Institute for Critical Infrastructure Technology.

Designing Modern Hospitals in the IoMT Era: Challenges and Solutions

K S Manoj & Renjith R

(Biomedical Engineering Consultants)

Designing modern hospitals in the IoMT era is a complex and challenging task that requires addressing various aspects such as security, interoperability, data management, and sustainability. Some of the challenges and solutions are:

- Security: IoMT devices are vulnerable to cyberattacks that can compromise the confidentiality, integrity, and availability of sensitive medical data and devices. Some of the potential solutions are encryption, authentication, access control, intrusion detection, and blockchain.
- Interoperability: IoMT devices and systems need to communicate and exchange data with each other and with other healthcare systems, such as electronic health records, cloud services, and telemedicine platforms. Some of the potential solutions are standardization, integration, middleware, and application programming interfaces.
- Data management: IoMT devices and systems generate large amounts of data that need to be stored, processed, analyzed, and visualized in an efficient and effective way. Some of the potential solutions are big data analytics, machine learning, artificial intelligence, and edge computing.
- Sustainability: IoMT devices and systems need to be designed and deployed in a way that minimizes the environmental impact, maximizes the social benefit, and ensures the economic viability of the healthcare system. Some of the potential solutions are energy efficiency, renewable energy, green computing, and the circular economy. [45]

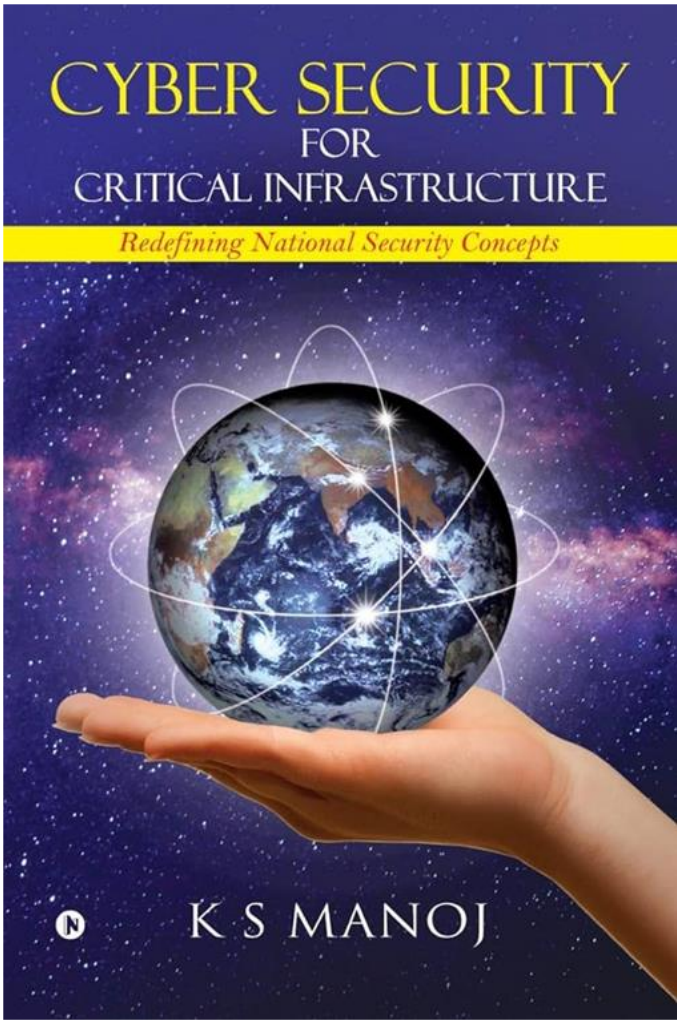
Designing modern hospitals in the IoMT era is not only a technical challenge but also a social, ethical, and legal challenge that requires the involvement and collaboration of various stakeholders, such as healthcare providers, patients, regulators, manufacturers, and researchers.

IoMT

IoMT stands for Internet of Medical Things, which is a network of internet-connected medical devices, software applications, and healthcare systems and services that transmit real-time data via networking technologies. IoMT devices can be used for various purposes, such as remote patient monitoring, diagnosis, treatment, prevention, and education. IoMT can also enable telehealth and telemedicine, which are forms of healthcare delivery that use digital technologies to provide care remotely. IoMT can improve the quality, efficiency, and accessibility of healthcare, as well as reduce costs and risks. However, IoMT also faces some challenges, such as security, interoperability, data management, and sustainability.

Designing modern hospitals in the IoMT era is not only a technical challenge but also a social, ethical, and legal challenge that requires the involvement and collaboration of various stakeholders, such as healthcare providers, patients, regulators, manufacturers, and researchers.

Today, cyberspace has emerged as a domain of its own in many ways, like land, sea, and air. Even if a nation is small in land area, low in GDP per capita, low in resources, less important in geopolitics, or weak in the strength of its armed forces, it can become a military superpower if it is capable of launching a cyberattack on critical infrastructure of any other nation, including superpowers, and crumbling that nation. In fact, cyberspace is redefining our security assumptions and defense strategies. This book explains the current cyber threat landscape and discusses the strategies being used by governments and corporate sectors to protect critical infrastructure (CI) against these threats.



Available in Amazon, Flipkart, Kobo, Etc.

Published by Intelegrid ECC(P) Ltd. TF3, Galaxy Delight, Kesari Lane, Trivandrum-12, INDIA.

Point of Contacts:*ksjayamohank@gmail.com, 8547611741, 8547018797, 0471 3577774.*

iNTELEGRID

ENGINEERING & CYBERSECURITY CONSULTING (P) Ltd

Protect Your Digital Future

A Platform for Research, Design, Build and Maintain Cybersecurity-Capable Health Delivery Organizations(HDO), Operational Technology(OT) and Critical Infrastructure(CI) with Visibility and Security.

LACK A CYBERSECURITY ENGINEER IN YOUR ORGANISATION?

Intelegrid Virtual CISO consultancy acts as your own Security Engineer

Intelegrid offer personalized and managed security services, security architecture and policy development, security maturity, risk and cyber vulnerability assessment, IT-OT segregation and integration consulting, and implementation.