PETRAS

Industry Briefing

Cybersecurity for the Internet of Things and Artificial Intelligence in the Healthcare Sector

Dr Monica Racovita

About PETRAS

The PETRAS National Centre of Excellence exists to ensure that technological advances in the Internet of Things (IoT) are developed and applied in consumer and business contexts, safely and securely. This is done by considering social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

The Centre is a consortium of 16 research institutions and the world's largest socio-technical research centre focused on the future implementation of the Internet of Things. The research institutions are: UCL, Imperial College London, University of Bristol, Cardiff University, Coventry University, University of Edinburgh, University of Glasgow, Lancaster University, Newcastle University, Northumbria University, University of Nottingham, University of Oxford, University of Southampton, University of Surrey, Tate and the University of Warwick.

As part of UKRI's Security of Digital Technologies at the Periphery (SDTaP) programme, PETRAS runs open, national level funding calls which enable us to undertake cutting edge basic and applied research. We also support the early adoption of new technologies through close work with other members of the SDTaP programme, such as InnovateUK, supporting demonstrations of new technology and commercialisation processes.

The wider PETRAS community has played a role in creating this report - in particular Professor Rachel Cooper OBE from Lancaster University for her critical role in review, and Caroline Wijnbladh and Emilie Didier from the PETRAS Business Development Team for their editorial overview.

Design work by Dr Catherine Wheller is based on original work by Dr Michael Stead.

This report should be referenced as follows:

Racovita, M. 2020. *Industry Briefing: Cybersecurity for the Internet of Things and Artificial Intelligence in the Healthcare Sector,* PETRAS National Centre of Excellence for IoT Systems Cybersecurity, London, UK

DOI: 10.14324/000.rp.10112770

From the Director

It is my pleasure to present this Industry Briefing on Cybersecurity for the Internet of Things and Artificial Intelligence in the Healthcare Sector. This is the first in a series of Industry Briefings, intended to link with and inform the six PETRAS Sectors: Ambient Environment, Supply Chains and Control Systems, Infrastructure, Agritech, Health and Wellbeing, and Transport and Mobility.

PETRAS has a large network of industry partners and expert academics, and works directly in collaboration with these and government partners to ensure that research can be directly applied to benefit society, business and the economy. I am delighted to see that as a Centre dedicated to identifying and addressing some of the needs within IoT, PETRAS has managed to connect industry with social and physical scientists to work towards some of the major challenges and questions around the cybersecurity of the Internet of Things. As IoT technology develops at speed and embraces AI and machine learning 'at the Edge', so do the challenges around cybersecurity and systems, and it is critical that these are addressed by industry, government and academia.

We hope that these Industry Briefings, which have highlighted insights into the challenges of deploying IoT systems, provide a fresh perspective on the existing and emerging opportunities for industry and those working within the Healthcare sector. With exciting innovative ideas, we are positive that PETRAS will be able to encourage collaboration between academia and industry, supporting the opportunities these challenges present, and we look forward to opening these discussions.

I hope this Industry Briefing will catalyse further debate and collaboration between researchers and users, making the use of the IoT safe and trustworthy, and maximising its social and economic value to the UK.

Professor Jeremy Watson CBE FREng
Director of the PETRAS National Centre of Excellence

UKRI Engineering and Physical Sciences Research Council

Contents

Executive Summary 4

Introduction 6
- Scope of this brief 6
- Sector background 7

Internet of Things and AI Cybersecurity 8
- Security vulnerabilities for IoT 9
- Threats and attack scenarios in smart hospitals 10
- Approaches and good practices for IoT cybersecurity 12
- Cybersecurity issues for AI 13

Policy and Regulations 14
- Current initiatives 14

Challenges and Opportunities 16
- Research challenges 16
- New developments in the field 16

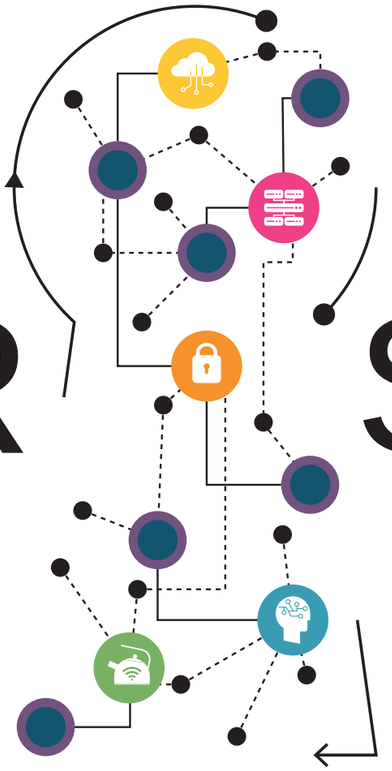
PETRAS in the UK Research Landscape 17

Glossary 19

End Notes 20

PETRAS

THE PETRAS NATIONAL CENTRE OF EXCELLENCE FOR IoT SYSTEMS CYBERSECURITY



Executive Summary

The PETRAS National Centre of Excellence aims to ensure that technological advances in the Internet of Things (IoT) and Artificial Intelligence (AI) are developed and applied safely, and securely by considering social and technical issues in a variety of sectors.

Healthcare is a sector highly vulnerable to cyber-attacks.

Security vulnerabilities affecting Internet of Things (IoT) devices have more than doubled since 2013[1], and are easy to exploit[2].

The number of IoT devices is continuously increasing, due to technological advancements in healthcare and policies promoting the uptake of such new technologies[3]. Personal medical information is very valuable, some argue, even more valuable than financial information[3] as it can be used to commit medical fraud, obtain controlled substances or steal identities.

Based on research that began in early 2020, this brief offers insights into general trends and challenges in cybersecurity research and policy for IoT devices and AI in healthcare in the UK, EU and at the global level.

Security vulnerabilities

- **IoT device limitations:** such as small size, limited processing power and memory;
- **Interaction with infrastructure:** legacy systems; increased use of IoT; need for data confidentiality; vulnerabilities of IT infrastructure (such as outdated systems, no authentication or authorisation of medical devices);
- **Users (e.g. clinical staff, IT staff and patients):** with low knowledge of cybersecurity or internal functioning of devices; not following security measures due to time pressure or interference with the quality of care.

Factors to consider for IoT cybersecurity in healthcare

- **A need to acknowledge that "safety" has different understandings in healthcare:** care for information (IT staff) and care for patients (health practitioners);
- **Understanding the main approaches for cybersecurity include standards, cyber labels, risk-based approaches and security by design;**
- **Good practices for cybersecurity:** Technical: network segmentation, asset and configuration management, network monitoring and intrusion detection; Organisational: risk management, security governance, training and awareness raising.

AI cybersecurity presents particular challenges, especially for neural networks. But AI can also be used in cybersecurity to protect healthcare data or predict attack patterns.

Policy

With regard to policy, the UK has adopted a minimum intervention approach to IoT, leading to an absence of security standards.

While the EU does not have specific references to cybersecurity for medical devices, it has a strong privacy law, and medical data is not allowed to cross international borders. In contrast, the US has more guidance on cybersecurity, but its privacy law is less robust.

For AI, several international bodies and organisations have begun work on standardisation measures.

Research

In terms of cybersecurity research for IoT and AI in healthcare, a few high-level research challenges include:

- Balancing the specifications of the IoT devices (size, memory, energy, power) with the requirements for increased security;
- Establishing a secure connectivity of new IoT devices with legacy systems;
- Increasing resilience of IoT devices in case of attacks;
- Designing security protocols that would take into consideration user behaviour;
- Having a security by design approach at all layers of IoT systems (of which the first layer includes medical devices);
- Improving the security of training datasets for machine learning;
- Employing AI and ML to help detect threats and provide recommendations to cyber analysts.

Research opportunities can emerge from addressing policy gaps, such as the lack of unified security standards and protocols, and research challenges, such as device or system limitations or user behaviour.

These gaps and challenges can be tackled either at company or institutional level for simpler issues with a narrower scope, or through partnerships for more complex, wide-encompassing issues.

The PETRAS National Centre of Excellence has a wealth of expertise in cybersecurity research. Although its foray into healthcare applications is relatively new, PETRAS has thus far completed 4 projects that focus on cybersecurity for healthcare IoT while one project is ongoing.

Introduction

Scope of this brief

This brief offers a summary of general trends and challenges in cybersecurity research and policy for IoT (Internet of Things) devices and AI (Artificial Intelligence) in healthcare in the UK, EU and at the global level based on research collected in early 2020. In addition, the document will offer insights into PETRAS activities focused on IoT and AI in healthcare.

The intended audience is primarily external industry and government organisations, including small, medium and large companies working around IoT, AI, and cybersecurity in healthcare, who would like to gain insights into PETRAS's work and collaboration offers.

For the scope of this document, IoT devices are seen as a component of an 'ecosystem' together with data communication, data aggregation and processing, data analytics and inference and data visualisation. This brief focuses on medical-grade devices used in a clinical or home based setting. In addition, the interest in the use of health IoT devices goes beyond the clinical environment of hospitals or clinics, in a recognition that the management of chronic diseases is increasingly relocated to home or homecare facilities.

Sector background

A June 2020 market research report from MarketsandMarkets predicts that the IoT in healthcare market size will increase from $US 72.5 billion in 2020 to $US 188.2 billion by 2025[4]. Based on components, the largest market size belongs to medical devices, while by application, inpatient monitoring applications are predicted to have the highest growth rate. By geographical region, the most promising growth in the IoT in healthcare market is expected to come from the Asia-Pacific, although the majority of the key market players are based in the US.

The main drivers of the market were identified in the MarketsandMarkets report as "rising focus on active patient engagement and patient-centric care, growing need for adoption of cost-control measures in the healthcare sector, and growth of high-speed network technologies for IoT connectivity, and increasing focus on patient-centric service delivery through various channels". In addition, the COVID-19 pandemic is thought to be a driver for healthcare IoT development through its increase in demand for wearable devices. Opportunities for IoT development are further provided by governments around the world increasingly promoting digital health, by restructuring health services, setting up necessary infrastructure and implementing regulations for electronic health records[4].

A main impediment for the healthcare IoT market development is the presence of old healthcare IT infrastructures, while the main challenge to overcome is cybersecurity due an increase in attack surfaces brought by a rise in IoT device use[4].

Technological advancements in healthcare, of which IoT devices are an important part, and policies promoting the uptake of such new technologies are the drivers increasing the exposure to cyber threats[3]. According to researchers, personal medical information can even be more valuable than financial information, as cybercriminals can use the first to commit medical fraud, obtain controlled substances or steal identities[3].

Security and privacy were overlooked at the beginning of IoT development in favour of usage objectives. But with a higher incidence of cyberattacks that target multiple security flaws, affecting a patient's privacy and endangering their health, security and privacy measures are currently a major focus of research[5].

Key market players identified by MarketsandMarkets: Medtronic (Ireland), Cisco Systems (US), IBM Corporation (US), GE Healthcare (US), Resideo Technologies (US), Agamatrix (US), Armis (US), Bosch (Germany), Capsule Technologies (US), Comarch SA (Poland), HQSoftware (Estonia), Huawei (China), Intel (US), KORE Wireless (US), Microsoft Corporation (US), Oracle (US), OSP Labs (US), Oxagile (US), PTC (US), Royal Philips (Netherlands), R-Style Labs (US), SAP SE (Germany), Sciencesoft (US), Siemens (Germany), Softweb Solutions (US), STANLEY Healthcare (US), Telit (UK), and Welch Allyn (US)

Internet of Things and AI Cybersecurity

The number of security vulnerabilities affecting IoT devices has more than doubled since 2013[1]. The healthcare sector is among those most affected by critical vulnerabilities, with potential hackers able to gain control of the devices and the networks to which they are connected[2]. This section presents a few main enablers of security vulnerabilities, together with threats and attack scenarios in smart hospitals and a few examples of good practices.

Security vulnerabilities for IoT

DEVICE LIMITATIONS

- **Computational:** small size and limited processing power can inhibit robust security measures (such as encryption). Reconfiguring or upgrading devices is also very difficult if not impossible[6].
- **Memory:** device memory may not be sufficient to execute complicated security protocols[6]
- **Energy:** IoT devices have limited battery power.
- **Life span:** While some sensors could be low cost and in theory could be replaced every couple of years, it is more challenging for more expensive devices[7].

IOT INTERACTION WITH SMART HOSPITALS/SMART HOME INFRASTRUCTURE

- **Security vulnerabilities due to legacy systems:** Some medical devices were not designed to be connected to a network, but the need appeared later so connectivity was added on. The communication between smart devices and older systems can create gaps and thus allow attackers to gain access to systems and data[7].
- **Security vulnerabilities due to increased use of IoT:** With an increase in the number of IoT devices, designing a scalable security scheme without compromising security requirements becomes challenging[6].
- Devices vary highly in terms of computation, power, memory, and embedded software. Therefore, designing a security scheme that can accommodate even simple devices becomes difficult[6].
- An increase in use of IoT also means integrating multiple local network protocols[6].
- **Security vulnerabilities due to the need for data confidentiality:** Need to build a stream access control or identity management system[6].
- **Smart hospital IT infrastructure security vulnerabilities:** Due to the wider dispersion of IoT devices in the hospital, physical security becomes practically impossible for all components[7].
- Usually IoT components are built on top of the already existing infrastructure, which could be outdated itself[7].
- For devices with low security and no security breach alert, compromised devices can act as bridgeheads for further malware proliferation in hospitals[7].
- Medical devices often do not require authentication or authorisation when used by staff, allowing unauthorised users to gain access through an end device to a critical system[7].
- Some systems or devices that do not meet organisational or industry standards or lack proper configuration could be used because of clinical needs. The number of such devices can exceed the IT department's capacity to follow appropriate security checks of new systems/devices[7].

USERS AS CYBERSECURITY WEAK LINKS

- Most security breaches in hospitals happen because members of staff access malicious files, which IT systems are not prepared to stop[3].
- Users have little or no knowledge of the internal functioning of the devices or the exact data streams they produce, especially in terms of the risk decisions made by the manufacturer. Poor communication from manufacturers and limited knowledge from users leads to a poor understanding of potential threats and less than adequate reaction in case of an incident[7].
- Even if security measures are in place, clinical staff may circumvent them because of time pressure or because of conflicts with other care objectives like efficient healthcare/patient flow, pleasant patient experience or patient/employee privacy[7].
- Sometimes physicians or patients use personal devices (mobile, wearables, etc.) which can automatically connect with the hospital system. These personal devices, of which the IT department is not even aware, can be a source of great vulnerability[7].

Threats and attack scenarios in smart hospitals

Attack scenarios are important to test the system's response to potential threats and allow developers to realistically check how the system will react to possible security breaches. For example, a social engineering type of attack is presented in Figure 1 and Table 1. In addition, Box 1 presents the example of the biggest cyber attack that affected the NHS, the WannaCry ransomware attack. One of the lessons learned was that there was a need for a cybersecurity response plan.

- **Threat actors** in hospitals can include insiders (hospital staff with malicious intent), patients and guests, remote attackers or other (environmental accidental equipment/software failure)[7].
- **Attack vectors** can include physical interaction with IT assets, wired or wireless communication with IT assets, or interaction with staff[7].
- The highest likelihood of threats is perceived to come from **human errors**, followed by malicious actions and system failures[7].
- The greatest impacts are considered to result from **malicious acts and human errors**[7].

Figure 1. A typical social engineering attack in a smart hospital (adapted from ENISA, 2016)[7]

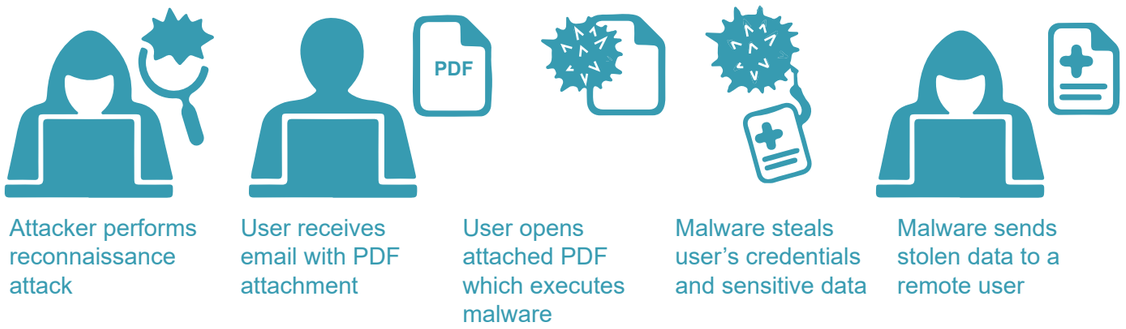


Table 1. Characteristics of social engineering attacks (summarised from ENISA, 2016)[7]

Criticality	• Highly critical, because of the broad range of follow-up attacks that could follow it
Likelihood	• High, because people are considered a particularly weak link in the hospital security chain
Effects	• Patient data and health records as well as financial information can become the target of follow-up attacks
Recovery times and efforts	• Depend on the extent of the attack and reaction time
Good practices	• Frequent training of staff • Clear policies for the use of social media and the reporting of suspicious people or situations • Clear roles and responsibilities to avoid and quickly respond to attacks • Frequent audits

Box 1. The WannaCry Ransomware Cyber Attack

In May 2017 a worldwide cyber attack targeted computers running the Microsoft Windows operating system, encrypting files and demanding a ransom in Bitcoin currency to release them. The attack exploited a Microsoft Windows vulnerability, previously identified and fixed by Microsoft through a security update. The computers infected either did not install the update (the majority) or were running unsupported software (the minority)[26]. It affected more than 230,000 computers in 150 countries causing loses of approximately $USD 4 billion[27].

Although the attack did not specifically target the healthcare sector, in the UK it affected the NHS provision of medical services for 80 out of 236 hospital trusts and 595 out of 7,454 GP practices[26].

A National Office Audit report on the impact summarised the lessons learned[28]:

- The need to have a response plan for a cybersecurity attack with clear roles and responsibilities for both local and national bodies;
- The need to implement critical CareCERT alerts (emails providing information or requiring actions, such as security and anti-virus updates);
- The need to ensure that in the case of future attacks essential communications are getting through;
- The need to increase awareness, at the level of organisations, boards and their staff, for cyber threats and their impact, and maximise resilience.

Approaches and good practices for IoT cybersecurity

According to cybersecurity analysts[8] the objective of safety differs between an IT specialist and a health practitioner. If for the first, 'safety' refers to information, for the second, it refers to health outcomes. Bringing the two together often requires a shared understanding of two domains.

Main approaches for cybersecurity:

- Standards and policies for IoT devices (summarised in the policy section in this document);
- Cyber labels, similar to energy efficiency labels, could be make it easier for end users to understand cybersecurity challenges for medical IoT devices[9];
- Risk based approaches to focus on how much risk could occur and with what likelihood. This approach could be more appropriate for the wide variety of medical IoT devices[9].

For good practices, "**security by design**" are a set of principles meant to increase the cybersecurity of IoT devices. The five principles for the design of cyber secure systems, as recommended by the National Cyber Security Centre[10] are:

1 Establish context before designing a system
2 Make compromise difficult
3 Make disruption difficult
4 Make compromise detection easier
5 Reduce the impact of compromise

In addition, Table 2 summarises proposed measures for security and privacy by design for different layers of IoT systems.

Yet adhering to security by design measures is not enough. Holistic testing to validate security is also needed and especially for IoT platforms a "real-world" testing, by monitoring the initial use, can uncover hidden or unknown vulnerabilities[11]. Figure 2 presents organisational and technical good practice measures.

Table 2. Security and privacy by design (summarized from Habibzadeh et al., 2020)[5]

Layer	Security and privacy measure
Data acquisition and sensing	• Lightweight cryptography • Platform integrity attestation mechanisms for protection against hardware/software tampering attacks
Communications	• Cryptography • Constrained application method (CoAP)
Cloud storage and processing	• Authentification mechanisms e.g. two-factor authentification • During processing advanced encryption schemes

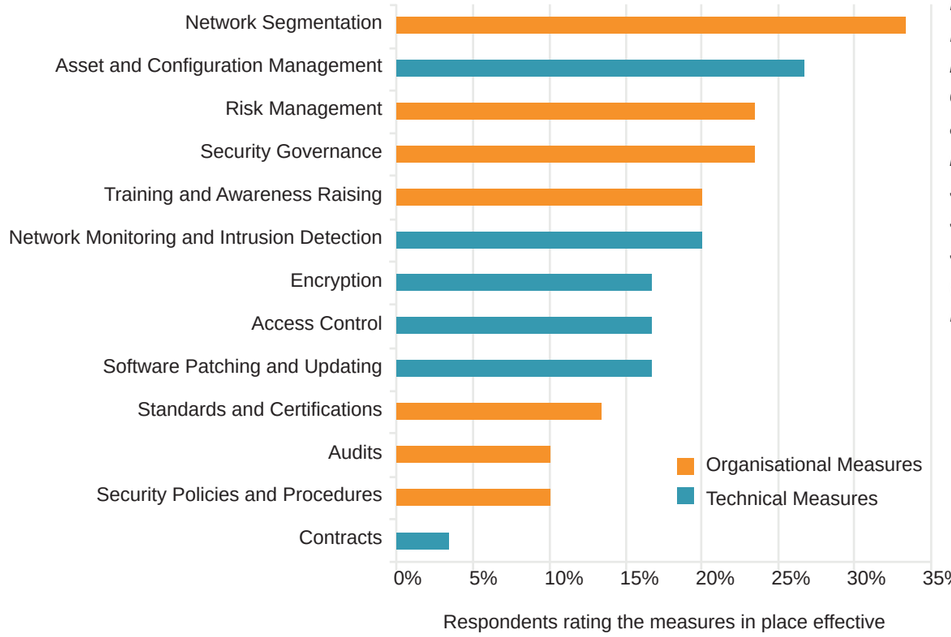


Figure 2. Ranking by respondents of organisational and technical measures to safeguard security in smart hospitals (adapted from ENISA, 2016)[7]

Cybersecurity issues for AI

Cybersecurity challenges for AI and big data could foster a closer synergy between individual privacy and public security, and encourage privacy by design[12].

The security of deep learning models presents particular challenges, as neural networks are sensitive to attacks. Attackers can impact the training process by injecting fake training datasets which can lower the accuracy and affect the network performance. Research in the security of deep learning or machine learning remains at an early stage[13]. However, early commercial initiatives of employing AI to strengthen healthcare cybersecurity have been signalled and a few are presented in Box 2.

AI and ML have been proposed to help detect threats and provide recommendations to cyber analysts, by for example automating mundane tasks, thus enabling analysts to respond more quickly to attacks[14].

Box 2. AI in healthcare cybersecurity (Joy, 2019)[25]

Protecting healthcare data

- Halifax Health enrols AI to help a firewall detect attacks by identifying the wrapper around malware payload.
- Cisco Systems employs AI for several security tools: firewalls, Cloudlock cloud access security, cognitive threat analytics and Cisco Advanced Malware Protection.
- IBM's Watson is used for security assessments, reducing times for analysis and response and reducing false positives.

Predicting attack patterns

- Boston Children's Hospital is employing AI to predict unusual behaviour (for example, 500 doctors attempting to see one patient record in the same time).

Policy and Regulations

For IoT in healthcare, a lack of unified security standards across healthcare organisations is an already well-known cybersecurity challenge. **Consistent use of data standards and protocols are urgently needed to address interoperability** (connectivity and secure data communication between multiple IT systems)[15]. The UK has adopted a minimum intervention approach to IoT in general, leading to an absence of universally agreed and enforced security standards[16].

Current initiatives

Despite this, there have been some notable initiatives. These include[16]:

- October 2018, DCMS (Digital, Culture, Media, and Sport)'s "Secure by Design" guidance, the UK government's Code of Practice for industry actors developing, operating, and selling consumer IoT services and solutions;
- February 2017, National Cyber Security Centre (NCSC) unites previous independent cybersecurity attempts of individual departments;
- Privacy and Electronic Communications Regulations (PECR 2003), providers of public electronic communication services are required to keep communications secure.

The EU and the US are de facto world leaders in harmonised regulatory frameworks for medical devices, and they also have the biggest share of health device markets[9]. The EU does not have specific references to cybersecurity but has strong privacy law and medical data is not allowed to cross international borders. In contrast, the US has more guidance on cybersecurity, but its privacy law is less robust[9].

In 2017 the EU passed new regulation on medical devices and in vitro medical devices, 2017/745 (MDR) and 2017/746 (IVDs) respectively[17]. According to the new regulation manufacturers need to:

- remove or reduce risk associated with negative interaction between software and IT environment (Art 14(2));
- ensure protection against "unauthorised access" (Art 17(4));
- protect the confidentiality of personal data (Art 109).

…cont

… A notable absence in the new EU regulation for medical devices is an explicit reference to cybersecurity. The protection against "unauthorised access" in Art 17 remains more within safety risk assessment rather than cybersecurity as an Atkins consultancy white paper indicates[8]. Two existing European ISO standards for medical devices BS EN ISO 62304 and BS EN ISO 14971:2012 refer to cybersecurity, the first including security provisions and the second indicating that it would be difficult to estimate probabilities for software failure, sabotage or tampering[8].

The EU Cybersecurity Directive (Directive on security of network and information systems), that came into force in August 2016, refers specifically to 'cybersecurity'. According to it, market operators would need to "comply with mandatory security breach and incident notification requirements to competent authorities, i.e. regulators, and will be required to implement appropriate organisational risk management, technical and security measures. The Directive duplicates some of the provisions in the EU General Data Protection Regulation (GDPR) on personal and sensitive information and the requirement to notify regulators of security breaches"[8].

On post-market management of cybersecurity and interoperability for medical devices, the US Food and Drug Administration (FDA) has issued varied guidance documents[8]. The "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" guidance stipulates that cybersecurity should be included in the design of medical devices. FDA also recommends for manufacturers the use of the NIST (National Institute of Standards and Technology) Framework for Improving Critical Infrastructure Cybersecurity[8].

For AI, several international bodies and organisations, such as the International Organisation for Standardisation (ISO), the Institute of Electrical and Electronics Engineers (IEEE), the US Consumer Technology Association (CTA), and the Chinese Electronics Standards Institute have begun work on standardisation measures for AI[18].

Challenges and Opportunities

Maintaining cybersecurity for IoT and AI in healthcare is a monumental task for researchers and practitioners with new threats increasing exponentially.

Research challenges

High-level research challenges include:

- Balancing the specifications of the IoT devices (size, memory, energy, power) with the requirements for increased security;
- Establishing a secure connectivity of new IoT devices with legacy systems;
- Setting up scalable security schemes that would accommodate an increasing number of devices, with variable properties and multiple local network protocols;
- Needing to build a stream access control or identity management system for data confidentiality;
- Integrating IoT devices with smart homes/hospitals IT infrastructure;
- Increasing resilience of IoT devices in case of attacks;
- Designing security protocols that would take into consideration user behaviour;
- Designing better approaches for standards, cyber labels or risk-based approaches;
- Having a security by design approach at all layers of IoT systems (of which the first layer includes medical devices);
- Improving the security of training datasets for machine learning;
- Employing AI and ML to help detect threats and provide recommendations to cyber analysts.

Research opportunities in the field of cybersecurity for healthcare IoT and AI can emerge from addressing policy gaps, such as the lack of unified security standards and protocols, and research challenges, such as device or system limitations or user behaviour.

These gaps and challenges can be tackled either at company or institutional level, for simpler issues with a narrower scope, or through partnerships, for more complex, wide-encompassing issues.

New developments in the field

Examples of notable new developments in the field include:

- **Policy and regulation:** use of cyber labels or risk-based approaches[9] or security by design[5];
- **Uncovering vulnerabilities:** AI fuzzing (utilising AI to find vulnerabilities in a system by attempting to crash it)[19].

PETRAS in the UK Research Landscape

PETRAS has a wealth of expertise in cybersecurity research. Although its foray into the healthcare applications is relatively new, PETRAS has thus far completed 4 projects that focus on cybersecurity for healthcare IoT (Table 3).

For AI, no PETRAS project had a specific focus on healthcare, but the results from projects in other sectors could be relevant for the healthcare sector as well (see Table 4).

Outside of PETRAS, other research hubs working on healthcare cybersecurity are Imperial College London's Institute of Global Health Innovation[20], and the Institute for Security Science and Technology[21].

For the private sector, some producers of medical equipment, like Baxter, which operates in the UK as well, have started offering cybersecurity by design for their products[22]. Other companies, like CyberSmart, offer assistance for standards of cyber hygiene, as covered in UK government's Cyber Essentials certification scheme[23].

PETRAS has a dedicated Business Development team who connect the public and private sectors with a network of transdisciplinary academic experts, to enable research collaborations that address social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

If you are a research institution, private or public sector organisation interested in collaborating with PETRAS, please contact petras@ucl.ac.uk.

Table 3. PETRAS projects on the cybersecurity of IoT in healthcare

Project	Partners	Description	Industrial relevance
Security and New Threats in Healthcare (SeNTH, SeNTH+)	• Intel Health and Life Sciences	• To investigate the security of IoT devices, in the context of implantable and wearable sensors.	• Biosensors, nano and microtechnologies • Biomedical engineering • Diagnostic and therapeutic systems
Privacy-Enhancing and Identification Enabling of IoT Solutions (PEIESI)	• CISCO • Eurofins Digital Testing • EE • MEVALUATE • SOGETI • ZTE Corporation	• To find solutions that make a balance between identifiability and privacy, for businesses that identify and re-identify customers.	• Any industry with concerns for privacy policies, like health or finance
Authentication and Access Control with Multiple IoT Devices (AACIoT)	• L3-TRL • Callsign	• To develop new approaches to ensure the resilience of IoT systems registering multiple enterings and leavings, each with rigorous authentication.	• Wearable health devices • Smart homes

Table 4. PETRAS projects on AI cybersecurity

Project	Partners	Description	Industrial relevance
Impact of Cyber Risk at the Edge: Cyber Risk Analytics and Artificial Intelligence (CRatE) (ongoing)	• CISCO • The FAIR Institute • AppDynamics	• To research the role of artificial intelligence and machine learning to design a self-adapting system for predictive cyber risk analytics that can form an automatic anomaly detection system.	• Any domain with cybersecurity challenges

Glossary

HEALTHCARE includes the prevention, diagnosis, treatment, recovery, or cure from disease and injury, being either physical or mental.

A **SMART HOSPITAL** makes use of sensors and medical devices that connect with clinical information systems.

AI (Artificial Intelligence) "A branch of computer science that attempts to both understand and build intelligent entities, often instantiated as software programs"[24].

ML (Machine Learning) "A field of computer science that uses algorithms to identify patterns in data"[24].

DEEP LEARNING involves training an artificial neural network with many layers on big datasets[24].

ARTIFICIAL NEURAL NETWORKS are computing systems inspired by biological neural networks.

CYBER LABELS similar to energy efficiency labels, could make it easier for end users to understand cybersecurity challenges for medical IoT devices[9].

RISK BASED APPROACHES focus on how much risk could occur and with what likelihood[9].

SECURITY BY DESIGN are a set of principles meant to increase the cybersecurity of IoT devices[10].

End Notes

1. Mirani S, Meyer J, Ramgattie R, Sindermann J (2019) SOHOpelessly Broken 2.0. Security Vulnerabilities in Network Accessible Services. Independent Security Evaluators (ISE)

2. Davis J (2020) Impact of Ripple20 Vulnerabilities on Healthcare IoT, Connected Devices. In: HealthITSecurity. https://healthitsecurity.com/news/impact-of-ripple20-vulnerabilities-on-healthcare-iot-connected-devices. Accessed 14 Aug 2020

3. Kruse CS, Frederick B, Jacobson T, Monticone DK (2017) Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care 25:1–10. https://doi.org/10.3233/THC-161263

4. MarketsandMarkets (2020) IoT Healthcare Market Size, Share and Global Market Forecast to 2025 | COVID-19 Impact Analysis | MarketsandMarkets. https://www.marketsandmarkets.com/Market-Reports/iot-healthcare-market-160082804.html. Accessed 8 Oct 2020

5. Habibzadeh H, Dinesh K, Rajabi Shishvan O, et al (2020) A Survey of Healthcare Internet of Things (HIoT): A Clinical Perspective. IEEE Internet of Things Journal 7:53–71. https://doi.org/10.1109/JIOT.2019.2946359

6. Nogueira V, Carnaz G (2016) An Overview of IoT and Healthcare. In: In Salvador Abreu and Vitor Beires Nogueira, editors, Actas das 6as Jornadas de Informática de Universidade de Évora. Escola de Ciências e Tecnologia da Universidade de Évora, Evora, Portugal

7. European Union Agency for Network and Information Security (ENISA) (2016) Cyber security and resilience for Smart Hospitals. ENISA, Heraklion, Greece

8. Piggin R (2017) Cybersecurity of medical devices. Addressing patient safety and the security of patient health information. BSI, BSI Group Macquarie Park UK

9. Royal Academy of Engineering (2018) Cyber safety and resilience strengthening the digital systems that support the modern economy. Royal Academy of Engineering, London, UK

10. National Cyber Security Centre (2019) Cyber security design principles. https://www.ncsc.gov.uk/collection/cyber-security-design-principles/cyber-security-design-principles. Accessed 31 Jul 2020

11. Peasley S, Lewis T, Wolfe B, et al (2018) IoT Platform Security by Design. Cybersecurity capabilities to look for when choosing an IoT platform. Deloitte

12. Jay J (2020) Rise of AI and Big Data could introduce fresh cyber security challenges. In: teiss. https://www.teiss.co.uk/ai-and-big-data-cyber-security/. Accessed 26 Apr 2020

13. Arjoune Y, Faruque S (2020) Artificial Intelligence for 5G Wireless Systems: Opportunities, Challenges, and Future Research Direction. In: 2020 10th Annual Computing and Communication Workshop and Conference (CCWC). pp 1023–1028

14. Bresniker K, Gavrilovska A, Holt J, et al (2019) Grand Challenge: Applying Artificial Intelligence and Machine Learning to Cybersecurity. Computer 52:45–52. https://doi.org/10.1109/MC.2019.2942584

15. Allen S (2020) 2020 Global Health Care Outlook Laying a foundation for the future. Deloitte

16. Tanczer L, Brass I, Elsden M, et al (2019) The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. Social Science Research Network, Rochester, NY

17. Medicines and Healthcare products Regulatory Agency (2020) Medical devices: EU regulations for MDR and IVDR. In: GOV.UK. https://www.gov.uk/guidance/medical-devices-eu-regulations-for-mdr-and-ivdr. Accessed 28 Jul 2020

18. Wenzel MA, Wiegand T (2019) Towards International Standards for the Evaluation of Artificial Intelligence for Health. In: 2019 ITU Kaleidoscope: ICT for Health: Networks, Standards and Innovation (ITU K). pp 1–10

19. Korolov M (2019) What is AI fuzzing? And why it may be the next big cybersecurity threat. In: CSO Online. https://www.csoonline.com/article/3375203/what-is-ai-fuzzing-and-why-it-may-be-the-next-big-cybersecurity-threat.html. Accessed 27 Aug 2020

20. Institute of Global Health Innovation. In: Imperial College London. http://www.imperial.ac.uk/global-health-innovation/. Accessed 28 Aug 2020

21. Institute for Security Science and Technology. In: Imperial College London. http://www.imperial.ac.uk/security-institute/. Accessed 28 Aug 2020

22. Product Security. In: Baxter. https://www.baxterhealthcare.co.uk/product-security. Accessed 28 Aug 2020

23. Cybersecurity for Healthcare. In: CyberSmart. https://cybersmart.co.uk/cybersecurity-for-healthcare/. Accessed 28 Aug 2020

24. Yu K-H, Beam AL, Kohane IS (2018) Artificial intelligence in healthcare. Nature Biomedical Engineering 2:719–731. https://doi.org/10.1038/s41551-018-0305-z

25. Joy K (2019) How Healthcare Organizations Use AI to Boost and Simplify Security. In: Technology Solutions That Drive Healthcare. https://healthtechmagazine.net/article/2019/11/how-healthcare-organizations-use-ai-boost-and-simplify-security-perfcon. Accessed 27 Aug 2020

26. Smart W (2018) Lessons learned review of the WannaCry Ransomware Cyber Attack. Department of Health and Social Care, NHS Improvement, NHS England, London, UK

27. Cooper C (2018) WannaCry: Lessons Learned 1 Year Later. In: Symantec Enterprise Blogs. https://symantec-enterprise-blogs.security.com/blogs/feature-stories/wannacry-lessons-learned-1-year-later?utm_content=71750833&utm_medium=social&utm_source=twitter. Accessed 15 Oct 2020

28. Comptroller and Auditor General (2018) Investigation: WannaCry cyber attack and the NHS. National Audit Office, London,UK