Cyber-risks from using IoT devices for managing Covid-19

Petar Radanliev, David De Roure, Max Van Kleek

Scientific research is increasingly focused on Covid-19 management with IoT technologies and artificial intelligence (AI). Autonomous connected devices, performing medical tasks without physical human interaction, is certainly beneficial for treating deadly infectious pandemics.

Read More

Some examples of medical IoT solutions include thermal camera detection monitoring for Covid-19[1], connected thermometers, smart wearables, and even IoT buttons for Covid-19 emergencies[2]. Although the current focus is predominated with Covid-19 mobile tracing apps[3], the IoT technologies are currently tested for advanced long-term healthcare solutions. Some of the current applications include patients desk sensors in field hospitals built for Covid-19, remote temperature monitoring of medical units, and open/close sensors for monitoring for restricted areas[4]. Long-term solutions are crucial for preventing and managing future pandemics, and for post-Covid-19 strategic digital transformations, in anticipation of 'Covid-21'[5]. However, Covid-19 has already exposed significant cyber-risks on medical IoT systems, and two US hospitals have been attacked, exploiting vulnerabilities in medical IoT devices[6]. Such cyber-attacks could hinder the adoption of IoT solutions for long term pandemic management planning. Since IoT can provide unique solutions for Covid-19 management, its safe adoption in long term solutions seems of utmost importance. In the following, we review how cyber-risk from medical IoT solutions could be assessed, in a fast-changing global pandemic.

Cyber-risk and its associated cyber-risks are growing with the integration of artificial intelligence (AI) in Covid-19 human-computer interactions. Some examples include connected devices into more aspects of modern life, including banking, finance, insurance, and more recently, in Covid-19 pandemic management. Cyber-attacks are increasing in frequency across all IoT smart systems, and the severity of future attacks could be much greater than what has been observed to date, triggering questions on our cyber risk preparedness. This is especially concerning in life-or-death situations, which brings into focus the new Covid-19 healthcare IoT systems.

The growth of artificial intelligence in human-computer interactions can also expose risks and vulnerabilities at the edge (IoT) of the network, where most of the Covid-19 IoT systems are based (e.g. thermal cameras, IoT emergency buttons, remote temperature monitoring). A new risk assessment is required for detecting and reducing the new types of cybersecurity threats and simplifying compliance with existing internal, industry, and government regulations. One solution for

---

[1] https://www.cio.com/article/3544913/iot-trojectory-podcast-thermal-detection-monitoring-for-covid-19.html

[2] https://www.geospatialworld.net/blogs/how-iot-can-help-fight-covid-19-battle/

[3] https://www.nhsx.nhs.uk/covid-19-response/nhs-covid-19-app/

[4] https://www.alliot.co.uk/covid-19-iot-solutions/

[5] https://www.crn.com/news/internet-of-things/intel-iot-programs-key-for-post-covid-19-digital-transformation

[6] https://www.networkworld.com/article/3545368/covid-19-pandemic-ratchets-up-threats-to-medical-iot.html

protecting the edge is to integrate AI in the Covid-19 data collection and analytics of risk through fog computing for predictive outputs. While new cybersecurity is constantly been developed, probabilistic data for Covid-19 risk analytics is not collected at the edge. Calculating cyber-risks at the edge creates a new role of AI in Covid-19 cyber-risk analytics with confidence intervals and time-bound ranges. This would protect the patient's data integrity while securing predictive analytic outputs and integrating solutions in these new types of fog computing cybersecurity.

What makes it difficult to quantify risk from the IoT in Covid-19 management?

The challenge in quantifying cyber-risk from the IoT systems used for Covid-19 management emerges with the pervasiveness and automation of IoT technology [1]. Existing risk quantification approaches are not designed to calculate such high-connectivity healthcare systems. This categorizes many IoT cyber-risks as invisible in the medical and healthcare risk assessment process. Adding to this, IoT devices often do not have a mechanism for reporting attempted hacks. Systems such as connected remote temperature monitoring or open/close sensors as room systems for monitoring for restricted areas are increasingly at risk, because of the new connected devices (e.g. smart camera or smart locks). Such risk can be reduced by connecting and authenticating the devices through the cloud, but that would trigger additional costs for the healthcare providers. Without quantification of the potential impact on patient's data, healthcare providers could be reluctant to invest in additional costs (e.g. cloud connection and authentication). This creates a direct link in the digitalization of Covid-19 management, between quantification of risk impact and willingness for cybersecurity investment. There are existing methods for cyber-risk assessment[7], and IoT cyber-risk analytics [2], but there are no cyber-risk models for assessment or analytics, specific for Covid-19 medical and healthcare systems. Given the speed of Covid-19, such a risk model would need to use networks as sensors for real-time intelligence for predictive analytic outputs. Integrating real-time dynamic probabilistic data in Covid-19 risk analytics could enable predictive intelligence. But this would require a new AI-enhanced method for cyber-risk analytics in medical and healthcare systems, integrated into the Covid-19 data collection. AI could enable dynamic risk assessment of the new Covid-19 management systems, while the probabilistic data of risk frequency and magnitude would enable understanding of risk exposure. Understanding of risk exposure by connection or device type and associated with low/high cost of the device and installation, is crucial for making decisions on using new IoT technologies, in medical and healthcare systems for Covid-19 management.

Cyber-risk quantification and Covid-19 management?

With the current lack of standards and regulations to govern the use of IoT in Covid-19 management, with a privacy-preserving compliance process, the risk from IoT devices is becoming a liability. Speaking in legal terms, medical and healthcare providers are required to take reasonable precautions to protect the patient's data and information. With the increasing volume of IoT devices due to Covid-19, it could become difficult to be compliant with this legal requirement. Hence, with the increasing rate of infections, the definition of what can be considered reasonable becomes blurred. Government legislations are in the process of being created, but it is unlikely that such legislation will come soon for Covid-19, and even more unlikely that the legislation would be unified and global, which is crucial for global pandemic management.
It is more likely that IoT legislations for Covid-19 management, will emerge on a case-by-case basis,

[7] https://www.fairinstitute.org/

and judging from the media coverage on the ease of virtual care systems hacking[8], this would start with network segmentation, awareness, and visibility of IoT devices, and organizational awareness. It is also possible that such new legislation on IoT systems for Covid-19 would create more damage than good. For example, if new legislations criminalize all hacking, including regular schedules of ethical and white hat, to protect patient's data, it would be even more challenging for healthcare providers to identify vulnerabilities. This leaves only Fog computing as the available option for fast IoT legislation that could be used in time for Covid-19 management. Fog computing is currently used primarily as an enforcer to limit damage from rogue devices. Fog computing also provides sufficient memory for the gradual integration of AI alternatives, that we discussed for automated risk surveillance. Fog computing enhanced with AI would also improve information knowledge management on future pandemics, through predictive analytics, supported with real-time dynamic intelligence. Such Covid-19 information knowledge management enables measuring the IoT device cost and cyber-attack probabilities from human-computer interactions in pandemic management. The main obstacle in assessing the impact of cyber-risk from IoT technologies in Covid-19 management is the lack of probabilistic data. This is partially caused by the fast spread of Covid-19, but the real cause is the lack of appropriate data collection strategies in past pandemics. As a result, the growth of cyber-risk during the Covid-19 pandemics, combined with the lack of empirical data from past pandemics, leads to difficulties in understanding cyber-risk from IoT technologies in Covid-19 management. Even more concerning, with the lack of probabilistic data on the impact of cyber-risks during fast-spreading global pandemics, the loss of life estimates from unpredictable 'black swan' cyber-attacks can be entirely speculative. However, if these concerns are considered during Covid-19, for designing automated risk surveillance, with real-time intelligence for predictive risk intelligence, this could prove very valuable in preventing and managing future pandemics.

How can IoT risk be quantified?

Traditional risk assessments could help in conducting an initial risk assessment for IoT technologies used in Covid-19 management. One example is comparing the Covid-19 management benefits with risks on individual IoT device-by-device. However, the IoT enables many entry points, each entry point creating a security issue. Hence, new automated DevSecOps approaches that anticipate the uniqueness of connected technologies are required for calculating the IoT risks in Covid-19 management systems. Connecting the cyber-risk of human-computer interactions in different medical and healthcare systems, with Covid-19 data records, can provide feedback for managing future pandemics. Dynamic real-time data mechanisms, designed for Covid-19 management, would also assist and enable a better understanding of the problems before pandemics occurring. The reliability of such assessments could increase significantly if decision-makers have a dynamic and self-adapting AI-enhanced methodology to assess, predict, analyze, and address future pandemics. However, the volume of data generated from IoT medical and healthcare systems, combined with the need for patient privacy, creates diverse ethical challenges. Simultaneously, the design of cybersecurity architecture for IoT technologies in complex coupled medical and healthcare systems, while understanding the need for fast and changing requirements of Covid-19 management, demands bold new solutions for data visualization, optimization, and decision making. Much of that is application-oriented and by default interdisciplinary, requiring hybrid researchers, with experiences in the areas of medicine, healthcare, cybersecurity, and risk assessment. Also, the design of Covid-19 management cybersecurity architecture must meet public acceptability, security standards, and legal scrutiny. With consideration of the above, the integration of areas such as cybersecurity, risk modelling, policy, and governance will contribute to knowledge by integrating risk

[8] https://www.networkworld.com/article/3545368/covid-19-pandemic-ratchets-up-threats-to-medical-iot.html

assessment models with pandemic management.

Quantifying the impact of IoT risk in Covid-19 management

How can the risk from IoT in Covid-19 management be quantified?

New approaches for cyber-risk quantification: one technique the could be used to assess the values vs risks from IoT technologies in Covid-19 management, is the Cyber Value at Risk framework[9]. The framework is generally applied to estimate cyber-risk losses over a given period, but in Covid-19 management, it could be applied to answer the question of how much would the risk be reduced if we invest a given amount, in more secured IoT systems. The components of the framework consist of analyzing the dependencies between vulnerabilities, assets, and the profile of attackers. The rationale is that the number of attacks would depend on the value of the healthcare assets, and the trends in the attacking community during Covid-19. However, the lack of probabilistic data on cyber-attacks in IoT solutions specific to Covid-19 management could lead to qualitative cyber-risk assessment. There is an emerging trend in similar quantitative models that are effectively designed with ranges and confidence intervals based on expert opinions and not probabilistic data. For example, the majority of the cybersecurity frameworks today apply qualitative methods, [e.g. OCTAVE [3]; TARA [4]; CMMI [5]; CMM [6]], that advocate reaching the required cybersecurity maturity level. The issue is that the current cyber state of the Covid-19 management needs to be transformed into a given target cyber state fast. But the implementation guidance [8], for reaching a target state without being able to quantitatively assess the outcome, represents a speculative assumption. Even the biggest supporters of qualitative approaches agree that assessments are resources intensive and often unreliable. Since qualitative approaches are often based on experts' opinions, they are prone to different interpretation, and are influenced by political and cultural forces. Such assumption cannot be considered acceptable for Covid-19 systems that effectively decide on life or death of patients. The problem is that qualitative approaches are predominating the risk assessment process at present.
There are a few quantitative cyber-risk models, (e.g. FAIR [9]), that are complementing the work of NIST and the International Organisation for Standardisation (ISO) [11], e.g. ISO 27032 and ISO 27001. A similar quantitative approach is needed for estimating the risk from IoT systems used in Covid-19 management but adapted for assessing a fast-changing rate of infection and other conditions of the pandemic. The argument is that without a fast and dynamic approach, changing with the rate of infection in real-time applying AI for fast data analytics, the risk estimations can be outdated and imprecise. What is currently needed for assessing the risks of IoT solutions in digital pandemic management, is predictive cyber-risk analytics based on confidence intervals and time-bound ranges. Given the requirement of this being operational during Covid-19, such an approach would almost certainly need to be based on the already established cyber-risk approaches discussed above.

Recommendations on quantitative assessment of medical and healthcare IoT solutions used for Covid-19 management: the Cyber Value at Risk approach could estimate the maximum loss of life that can occur in a worst-case rate of infection scenario. Such scenarios include a larger loss of life and rate of infection than estimated with other methods. The analytical benefit from applying the Cyber Value at Risk is that understanding the maximum loss of life, which is different than the expected loss of life and enables a better understanding of the infection uncertainty. This quantification offers a better understanding of opportunities and the risk from IoT solutions in pandemic management. However, given the lack of probabilistic data on IoT risks in pandemic management, this could also lead to a design that aims to present statistical results without

[9] https://www2.deloitte.com/lu/en/pages/risk/articles/benefits-limits-cyber-value-at-risk.html

statistical data.
It is more likely that a completely new quantitative approach needs to be developed for assessing the risks from medical and healthcare IoT solutions used in pandemic management. This new quantitative approach needs to be developed as a forward-facing predictive model, supported with mathematical and statistical methods, including dependency modeling, probability, linear regression, decision trees, clustering, and Bayesian inference. Such an approach would undoubtedly require collecting probabilistic data on the risks from medical and healthcare IoT solutions used in pandemic management.
Given that these solutions are applied at the edge, and increasingly are enhanced with AI, it would mean that critical medical domains need to extract value from centralized and edge analytics. This will likely further increase the attack surface for adversaries to poison or trick machine learning models to undermine their integrity or availability.

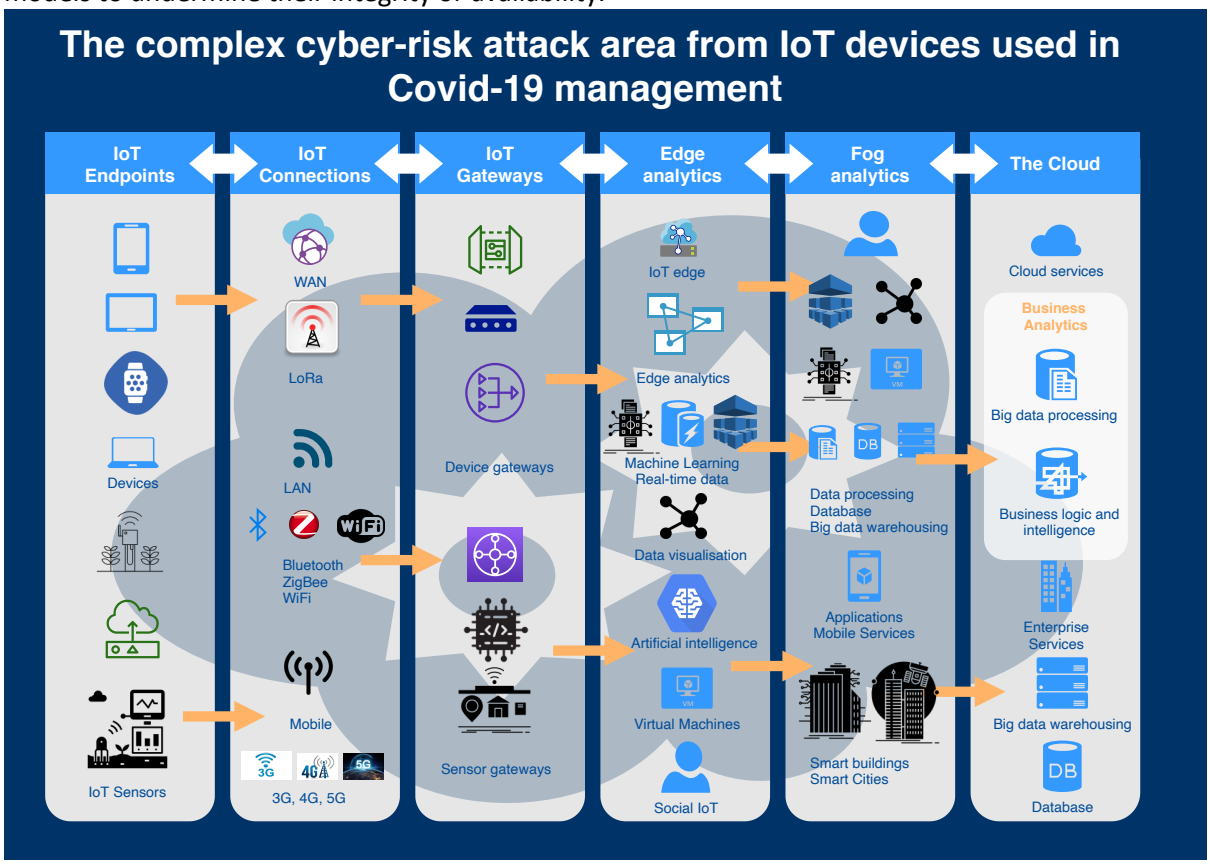

Figure 1: Taxonomy of potential risk areas - connecting points for IoT devices in Covid-19 digital management

Furthermore, this complexity is compounded by the sectors and applications, that risk analytics can be applied to, e.g. many changing requirements, while data and conditions are not fully understood. Therefore, some form of validation is required before medical and healthcare IoT solutions can be used in practice for pandemic management safely.

Elements that will enable cyber-risk quantification: the most valuable element for quantification is the availability of risk metrics. Currently, there is a lack of risk metrics on many aspects of Covid-19. To address this, governments need to work with the private sector, to identify and develop appropriate standards and processes, for the collection, distribution, and availability of risk metrics, from the digital solutions used in Covid-19 management. This could be achieved with a national information-sharing platform, strengthening the supervision of critical digital medical and healthcare infrastructure, and sectors that are elevating the cyber-risks (e.g. medical IoT device producers). The

medical cybersecurity companies have also not matured and evolved as fast as the Covid-19 cyber-risks have. Medical cybersecurity providers could expand operations into performing quantitative cyber-risk assessment before offering IoT solutions and products for pandemic management. But manipulating patient's medical data in real-time can be controversial. Hence, the threat event frequency should be developed along with an assessment of how imposter devices (e.g. vulnerable or hacked IoT devices) might compromise edge computing systems. This assessment should adapt for real-time data collection, with AI analytics for predictive intelligence on threat event frequency and the magnitude loss.

Final remarks

The findings up-to-date indicate that medical IoT solutions are frequently not adequately assessed for cyber-risks, and with the increased use of such solutions in Covid-19 management, more focus needs to be placed on the risk assessment concern. Large healthcare providers on the other hand could be inadequately protected from third-party medical IoT solutions, operating in the Covid-19 monitoring. This, combined with the increasing sophistication of cyber-attacks on medical IoT solutions, amplifies the maximum loss of life scenario. Simultaneously, the returns from IoT cybersecurity investments are invisible without appropriate risk assessment. While new cybersecurity is constantly been developed, probabilistic data for risk analytics of medical IoT solutions are not collected. Hence, the Covid-19 could be an opportunity for integrating AI in cyber-risk analytics of medical IoT solutions and related to confidence intervals and time-bound ranges. The objective of such an approach would be to protect the patient's medical data integrity while securing predictive analytic outputs and integrating such solutions in fog computing security. In fog computing, the medical IoT solutions are open to adversarial behaviors that are yet uncharted and poorly understood, especially with the fast-changing conditions of Covid-19.
By integrating AI in the risk analytics of medical IoT solutions, a new approach can be devised, creating a stronger resilience of systems through cognition in their physical and digital dimensions. Such an approach would revolve around understanding how and when compromises happen, to enable Covid-19 systems to adapt and continue to operate safely and securely when they have been compromised. AI could enable medical IoT systems to recover and become more robust. Since some companies[10] are already using AI[11] to defend, adapt and recover systems in response to adverse events, medical IoT solutions for Covid-19 should be built upon that knowledge, to design a similar model for Covid-19 and future pandemic management. The crucial factor is assuring that medical IoT systems can continuously adapt and employ AI techniques to understand and mitigate the vulnerabilities of adverse events.

References

[1] Radanliev, Petar., De Roure, David., and Van Kleek, Max, "Digitalization of COVID-19 Pandemic Management and Cyber-risk from Connected Systems - IEEE Internet of Things," *IEEE Internet of Things Newsletter*, 14-May-2020.
[2] Radanliev, Petar., De Roure, David., Nicolescu, Razvan., Huth, Michael., Montalvo, Rafael Mantilla., Cannady, Stacy., and Burnap, Peter, "Future developments in cyber-risk assessment for the internet of things," *Comput. Ind.*, vol. 102, pp. 14–22, Nov. 2018.
[3] Caralli, Richard A., Stevens, James F., Young, Lisa R., and Wilson, William R, "Introducing OCTAVE

[10] https://www.appdynamics.com/

[11] https://www.appdynamics.com/cognition-engine/

Allegro: Improving the Information Security Risk Assessment Process," Hansom AFB, MA, 2007.
[4] Wynn, Joseph., Whitmore, Geoff., Upton, Lindsay., Spriggs, Dan., McKinnon, Richard., McInnes, Richard., Graubart, Lauren., and Clausen, Jackson, "Threat Assessment & Remediation Analysis (TARA) Methodology Description Version 1.0," Bedford, MA, 2011.
[5] CMMI, "What Is Capability Maturity Model Integration (CMMI)®? | CMMI Institute," *CMMI Institute*, 2017. [Online]. Available: http://cmmiinstitute.com/capability-maturity-model-integration. [Accessed: 26-Dec-2017].
[6] U.S. Department of Energy, "Cybersecurity Capability Maturity Model (C2M2) | Department of Energy," Washington, DC, 2014.
[7] NIST, Cybersecurity_Framework, *Cybersecurity Framework | NIST*. 2016.
[8] Barrett, Matt., Marron, Jeff., Yan Pillitteri, Victoria., Boyens, Jon., Witte, Greg., and Feldman, Larry, "Draft NISTIR 8170, The Cybersecurity Framework: Implementation Guidance for Federal Agencies," Maryland, 2017.
[9] FAIR, "Quantitative Information Risk Management | The FAIR Institute," *Factor Analysis of Information Risk* , 2017. [Online]. Available: http://www.fairinstitute.org/. [Accessed: 26-Dec-2017].
[10] FAIR, "What is a Cyber Value-at-Risk Model?," 2017. [Online]. Available: http://www.fairinstitute.org/blog/what-is-a-cyber-value-at-risk-model. [Accessed: 26-Dec-2017].
[11] ISO, "ISO - International Organization for Standardization," 2017. [Online]. Available: https://www.iso.org/home.html. [Accessed: 26-Dec-2017].
[12] Öğüt, Hulisi., Raghunathan, Srinivasan., and Menon, Nirup, "Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection," *Risk Anal.*, vol. 31, no. 3, pp. 497–512, Mar. 2011.

Keywords: cyber risk quantification, IoT risk assessment, Covid-19 management, medical IoT solutions

BIOS & Photo:

Petar Radanliev is a Post-Doctoral Research Associate at the University of Oxford. He obtained his Ph.D. at the University of Wales in 2014 and continued with postdoctoral research at Imperial College London, Massachusetts Institute of Technology, and the University of Oxford. His current research focuses on artificial intelligence, the Internet of things, and cyber risk analytics.

David De Roure is a Professor of e-Research at the University of Oxford. He obtained his Ph.D. at the University of Southampton in 1990 and went on to hold the post of Professor of Computer Science, later directing the UK Digital Social Research programme. His current research focuses on social machines, the Internet of Things, and cybersecurity. He is a Fellow of the British Computer Society and the Institute of Mathematics and its Applications.

Max Van Kleek is an Associate Professor of Human-Computer Interaction with the Department of Computer Science, at the University of Oxford. He works in the Software Engineering Programme, to deliver course material related to interaction design, the design of secure systems, and usability. His current project is designing new Web-architectures to help people re-gain control of information held about them "in the cloud", from fitness to medical records. He received his Ph.D. from MIT CSAIL in 2011.