Cybersecurity Business Models for IoT-Mobile Device Management Services in Futures Digital Hospitals

Julius Francis Gomes[1], Marika Iivari[1], Petri Ahokangas[1], Lauri Isotalo[2] and Riikka Niemelä[3]

- [1]*Martti Ahtisaari Institute of Global Business & Economics, Oulu Business School, University of Oulu, Finland*
- [2]*Elisa Corporation, Finland*
- [3]*MedicalMountains AG, Tuttlingen, Germany*

E-mail: julius.francisgomes@oulu.fi; marika.iivari@oulu.fi; petri.ahokangas@oulu.fi; lauri.isotalo@elisa.fi; niemelri@gmail.com

Received 8 September 2017;
Accepted 7 November 2017

Abstract

Hospitals as critical infrastructures has been historically dependent on various types of devices and equipment that are being revolutionized with digitalized solutions. The digitalization of conventional healthcare equipment is added with the new inclusion of numerous new devices for data collection, analysis, communication, and so on. All in all, the futures digital hospitals in 5G will be exponentially more data-dependent and digital-intensive. For that, this paper looks to theorize how the security scenario in a futures digital hospital would look like, and what relevant business possibilities could emerge for cybersecurity providers in the healthcare context. In this paper, we open up discussions on business possibilities relevant to Internet of Things-mobile device management for critical infrastructures such as future digital hospital. We apply business models as a conceptual lens to analyze how cybersecurity business could evolve for 5G enabled IoT-Mobile device management providers as a cybersecurity vendor.

Keywords

- Internet of Things
- Mobile Device Management
- Business Model
- Digital Hospital
- 5G Security
- Cybersecurity

1 Introduction

The healthcare sector has progressed significantly since the introduction of Internet and proliferation of network technologies [1]. Among many issues, the use of data, availability of data, data mass, and access control of data in healthcare remain are critical for keeping healthcare services trustworthy and secure for the end users, both hospital staff and the patients.

Disruptions in healthcare services would have severe effects on people's lives. However, as hospital managers and professionals need to design their data-dependent and digital-intensive networks in a manner, which is highly secure, they also should provide the basis for uninterrupted service for business sustainability. Security is often observed as a tradeoff between risk and business gains [2]. Investing in security is important in order to secure business-critical systems and data for meeting business goals and eventually for creating competitive advantage [3, 4].

Innovative technologies have the power to disrupt industries and prompt business transformation [5]. The coming of fifth generation (5G) of telecommunications networks is seen to result in this kind of disruption. As we are gradually moving towards 5G, it is worthwhile to theorize how the security scenario in a futures digital hospital would look like, and what relevant business possibilities could emerge from cybersecurity in the healthcare context. From this perspective, in this paper, we open up discussions on business possibilities relevant to Internet of Things mobile device management for critical infrastructures such as future digital hospital. We apply business models as a conceptual lens to analyze how cybersecurity business could evolve for 5G enabled IoT device management providers as a cybersecurity vendor.

A futures digital hospital facility is envisioned to consist tech-aided advanced critical medical devices, intelligent information systems, digital communication tools, hundreds of handheld mobile devices (smartphones, tablets), wireless clinical wearables, in addition to thousands of smart IoT nodes [6, 7]. These devices should be fully integrated to improve staff productivity, hospital functions, patient safety and privacy, and, overall improve patient experience through secure and reliable healthcare services. However, inclusion of these various kinds of digital devices to the hospital context make the overall device network quite complex and heterogeneous [7]. Thus, from a critical infrastructures view point, to manage, configure, update and secure the immense fleet of digital devices besides all the high-tech medical equipment, the futures digital hospital will need to redefine device management policy and services [3].

Mobile device management (MDM) systems are usually referred to "support centralized control of an entire fleet of mobile devices (smartphones and tablets) and mobile applications by applying and ensuring pre-defined configuration settings" [8, 9]. In the scope of this paper, we broadly use the term IoT-MDM to refer to a device management system that is capable of managing, configuring and updating both handheld mobile devices and IoT devices in combination in a centralized manner. We will briefly open up the concept of MDM and IoT-MDM.

The purpose of this study is to identify business potential for IoT-MDM service providers as cybersecurity vendor in the context of the future digital hospital. In doing so, we apply the concept of business model in order to make sense of a ICT-oriented business environment [10]. Among various available conceptualizations, business model is considered as a boundary-spanning unit of analysis that explain the underlying business logic and the value creation and value capturing logic of an organization [11–15].

2 IoT Device Management and Mobile Device Management

Traditionally, device management has been associated with management and configuration of handheld mobile devices [16], thus, mobile device management (MDM). Gartner [17] perceives MDM software to be a policy tool to configure and manage mobile handheld devices. They also mark that MDM services need to ensure security in reference to connectivity and content that is being transmitted. Along with surge of smart mobile devices, the Internet of Things (IoT) is growing large during the last few years and promises to flood the market with billions of devices in the coming years too [18]. Zhang et al. [19] states scalability, transparency and reliability as important issues that differentiates IoT from the conventional Internet. To that end, there are several IoT platforms available currently in the market for managing, updating and configuring IoT nodes, e.g. IBM Bluemix, Cumulocity, ARM mbed OS, etc. [20]. However, the transition raises the question about the differences and similarities between MDM and IoT device management as approaches.

Takalo [16] marks MDM and IoT device management to be quite close on a conceptual level: both need solution for automated management of large device fleets consisting different form factors, device models, and operating system. Additionally, such systems conceptually needs to support various communication channels like: WiFi, cellular network and Ethernet. However, on practical level, MDM is more strictly controlled by operating systems and device vendors. IoT device management, on the other hand, is characterized by multiple operating systems, multiple hardware platform variations, non-complete standards, multiple communication methods and protocols. This agile approach allows the coexistence of various types of devices and nodes in the same environment. Recently, services are appearing where MDM and IoT device management are brought together under the same platform, which in a way reduces the complexity in device management and also improves the overall security of the system.

While we are still in early phase of mass IoT deployment and 5G deployment is approaching, it is important to revisit some of the key security threats that has been identified in recent literature relevant mainly to IoT. Zhang et al. [19, 21] identified privacy preservation as a critical issue for information security in IoT ecosystems. They further state that conventional naming, identification and authentication policies need to be improved and rather needs approaching differently. Farooq et al. [22] look at the four layer generic IoT architecture consisting perception layer, network layer, middle-ware layer & application layer. Additionally, they offer a list of security challenges for each layer. Some of the key challenges are: unauthorized access, tag cloning, eavesdropping, spoofing, RF jamming, sinkhole attack, sleep deprivation attack, denial of service attack, malicious code injection, man-in-the-middle attack, spear-phishing attack, sniffing attack. Backman et al. [23] state, a comprehensive security solution needs to address endpoint security, management and monitoring security, and secure data distribution and storage.

Ortbach et al. [9] enumerate the drivers for adoption of MDM in organization through a quantitative analysis, reflecting three broad drivers: organization, environment, and technology. From organizational perspective, the company size, mobile IT usage, employee innovativeness with IT and BYOD (bring your own device) culture were identified as important drivers. From environmental viewpoint, regulations and other business partner influence are significant drivers for MDM adoption. Finally, from technology point of view, perceived security benefits and perceived cost of the service seems to affect the managerial attitude towards MDM adoption.

MDM systems are today a very common tool to manage users' devices. With MDM, all mobile device types, tablets and PCs with typical operating systems can be controlled centrally [9]. It is often thought that MDM can manage only mobile phones, but actually the MDM framework includes also users' identities and profiles. This makes MDM a viable tool for organizations to manage their employees identities, user profiles, all devices, all applications and security controls under same system.

From an emerging technology perspective, SDN (software-defined network)/NFV (network functions virtualization) based 5G Slicing will challenge some of the traditional MDM features [24]. Especially end-to-end security from device to IT cloud is difficult to realize with MDM. Of course, it is possible to force the use of VPN in mobile device with MDM, but many aspects of communications security will be still unsolved. Thus, 5G slicing provides new tools to control and manage the end-to-end communications flow with network functions (VNFs). In the advent of IoT, this is particularly important since the billions of IoT devices of the 2020s will have only a minimal processing power and memory compared to the smart phones of today. These IoT devices may connect to network only once a month and communicate only with network edge cloud servers. Therefore, managing these new IoT devices cannot be done with conventional MDM systems of today.

Fortunately, many features of MDM can be provided by dedicated 5G slices and their VNFs. If e.g. a IoT device does not have the latest anti-virus updates, the network slice may still provide the isolation and security controls so that the IoT device can send the metering data. Moreover, if the IP flow from the IoT device includes other than actual metering data, eg. due to malware in IoT device, this IP flow can be analyzed and filtered by slice specific VNFs before passing it to IoT could.

As a summary, it can be argued that SDN/NFV based 5G Slicing will provide new tools for security management, and, when combined with IoT-MDM system functionalities, together these can deliver a better device management framework for different kinds of user devices of the 2020s.

3 Futures Digital Hospital

Hospital organizations are considered as critical infrastructure (CI) to nation states [3, 25]. As a critical infrastructure, hospital organizations are prone to security threats that can affect health policies, public health, healthcare services, surgical procedures, electronic patient records, patient privacy, doctor-patient communication, etc. Lehto and Ahokangas [3] notes, new technology (e.g. next generation mobile networks, smart data storage, IoT) adoption of CIs increases the cybersecurity touchpoints and hence making the CIs more vulnerable. Broadly, from cybersecurity perspective, the hospital organizations in future will be vulnerable from management perspective (e.g. organizing healthcare services, managing huge amount of patient data, clinical data, medication data, communication between health professional and patients etc.), healthcare service delivery perspective (e.g. in an unwelcoming case of denial of service attacks in hospital context: like wannacry), network perspective (e.g. security of the overall hospital network), and last but not the least from an individual privacy perspective (e.g. individual patient records, healthcare professional logs, etc.).

A futures digital hospital will consist various advanced technologies, such as critical medical devices, intelligent information systems and digital communication tools, which are fully integrated to improve staff productivity, hospital operations, patient safety, and the overall patient experience. Among them, many will be wireless mobile devices, wireless wearables and thousands of smart IoT devices for various kinds of measurements [6].

Innovations help transform healthcare in forms of advanced telecommunications techonology, new drugs and treatments like biological sensor pills or implants, new medical devices, social media interation, etc. [1, 6, 7]. In future, hospitals and surgical tools will be revolutionized with intelligence and connectivity i.e. providing more assistive functions by sensors, processors, data collection, software algorithms and interfaces which are, for example, embedded in the tools that will support surgeon's decision-making in action [6]. Robotic-assisted Surgery (RAS) can be considered as a good example of such transformation. The rapid adoption of Minimally Invasive Surgery (MIS) and today's information revolution not only improves the surgical outcomes and patient's life but also changes the patient-physician relationship.

'Smart' i.e. IoT-based technologies are going to intellectualize medical devices and service systems into Smart Hospitals. Smart hospitals extrapolate from totally digitalized and automated data collection, tracking and delivery between systems, devices, patients, and health professionals and organization [26]. In future, it is also envisioned that virtual hospitals and personalized medication will become part of patient care. Patients will be able to visit virtual hospitals or e-clinincs for clinical purposes without the presence of health professionals, but procedures and communication are managed via remote management and telemedicine solutions [27].

Other features that futures digital hospitals will include: use of different AR (augmented reality) and VR (virtual reality) applications for healthcare related purposes. While VR applications are quickly evolving in the gaming industry, some applications are deemed suitable in hospital environment too. Patients can be introduced to hospital environment through VR solutions, which can reduce patient stress prior to surgical procedures [28]. Another application of VR in healthcare has been identified as rehabilitation support for temporary physical disabilities and mental trauma. Further, AR solutions can help patients navigate within a large hospital complex.

4 Business Model Approaches

The term, Business model, has had its root in information systems (IS) and information communication technology (ICT) since the late 1970s originating from business informatics. However, it came into management and strategic management literature as a research interest from the mid-1990s [29, 30]. Although business model had its roots in IS and ICT, the amount of research work on cyber security as a context is still quite negligible harnessing the potential of business model concept.

The concept of business models lies at the intersection of entrepreneurship and strategy, it can be observed as a bridge between abstract strategies and the practical implementation of strategic decisions and actions amidst the uncertainties of the modern business context [11–14, 31]. For instance, Zott and Amit [15] conceptualize business model as a 'boundary-spanning' set of

activities aimed at creating and appropriating value. Morris et al. [32] viewed the concept of the business model as a set of decisions related to the venture strategy, architecture, and economics of firm (value creation and capture) that need addressing to create sustainable competitive advantage in the chosen markets and specific contexts.

As a boundary-spanning unit of analysis, business models [33], connects an organization with its business environment, other organizations, customers, individuals and society as well; with the overall ecosystem at large [34, 35]. Trying to bridge business models and cyber security under current context, there are two core issues. First, as almost all of the entities operating within the digital sphere face multifaceted cyber threats, how can business model approach help organizations to respond to such situations? Second, how can business model approach help to identify opportunities and monetize security in future 5G? In the next two sub-chapters, we present two business model approaches that are suitable for ICT contexts, and, can help find answers to the above mentioned questions.

4.1 The 4C ICT Business Model Archetypes

As the mobile telecommunications industry advanced, so did business model related discussions in the literature about extending organizational boundaries through vertical and horizontal integration in industries [36]. Around this, Wirtz et al. [10] offered four mutually exclusive business models classifying Internet based business models to be precise. According to Wirtz et al. [10], these business models present in Web 2.0 are related to connection, content, context, and commerce. Building further, Yrjölä et al. [37] interpreted these business models as chronological layers, where “lower” layer business models are pre-requisites for the “higher” layer business models to exist.

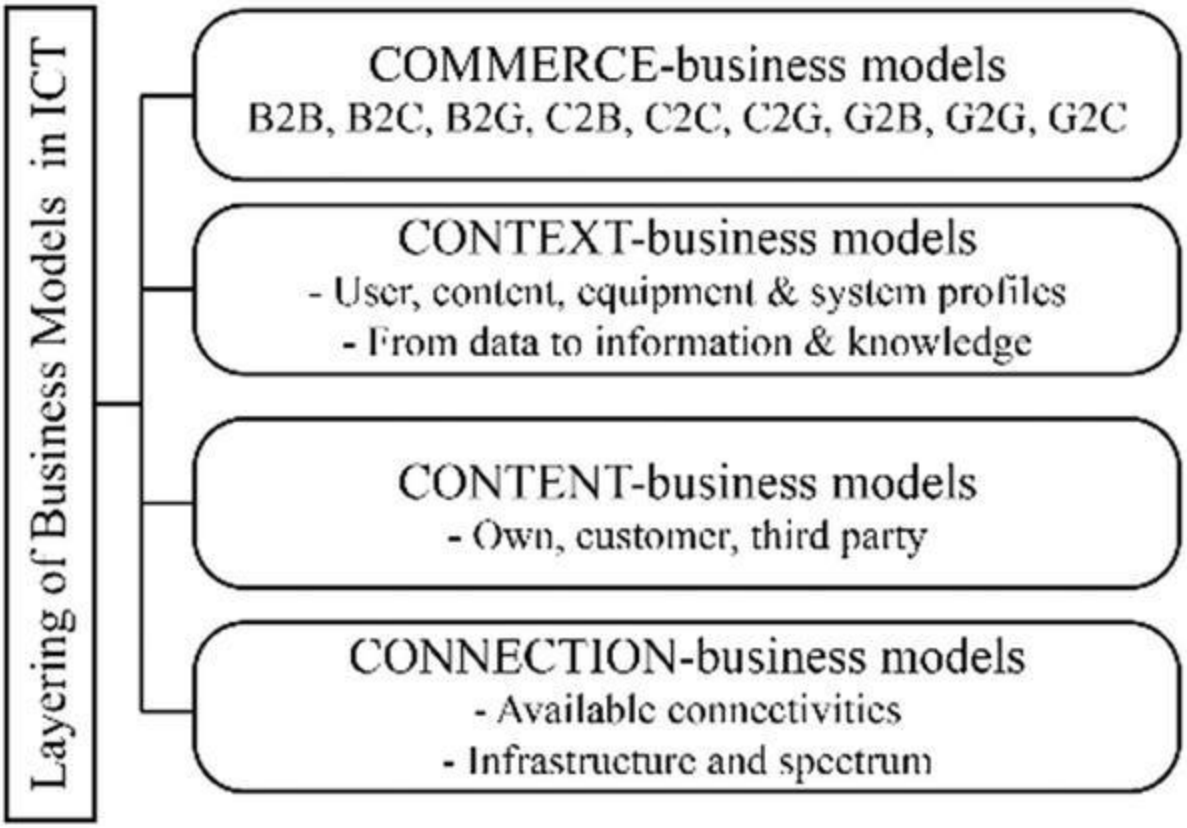

Figure 1 The layered 4C ICT business models archetypes [Adapted from 35, 37, 38].

The first layer is concerned with *connection*-related business model where a stakeholder provides connection services [38]. Connection- related business models are relevant to connectivity for all sorts of devices and nodes through various communication channels, e.g. PCs, smartphones, tablets, IoT devices, etc. The second layer is the business model focusing on monetizing *content*. At the content layer, all sorts of online content services (e.g. mobile video streaming) are classified (i.e. relevant, up-to-date and interesting) and are accessible conveniently for the end user. The content might be peer-to-peer/user-oriented contents (i.e. exchange of personal content), and web browsing content (audio, video, text etc.).

The third, *context*, layer concerns the ability to create and monetize user, content, equipment/user device and system profiles and turn (big) data into meaningful information and knowledge through systemic virtual contextualization. The fourth layer concerns *commerce*, the ability to monetize any or all of the connection, content, or context specific resources, actors or activities related to the ongoing communications. At this layer, we identify business, consumer and public/government types of communications [39]. Thus, B2B (business-to-business), B2C and B2G communications as well as C2B, C2C and C2G or G2B, G2C and G2G communications may be monetized at this layer.

4.2 Mixed-Source Business Model Approach

Casdesus-Masanell and Llanes's [40] offers different software business models based on the openness of core software and extension software offering. According to the mixed source software business model approach, services can be: open source (open core- open extension), open core (open core- closed extension), open extensions (closed core- open extension) and proprietary (closed core- closed extension). Although this model was offered specifically suiting the software industry, we argue that similar approach can be useful in other ICT contexts to scale up value offering by adjusting cooperation and industrial partnering model.

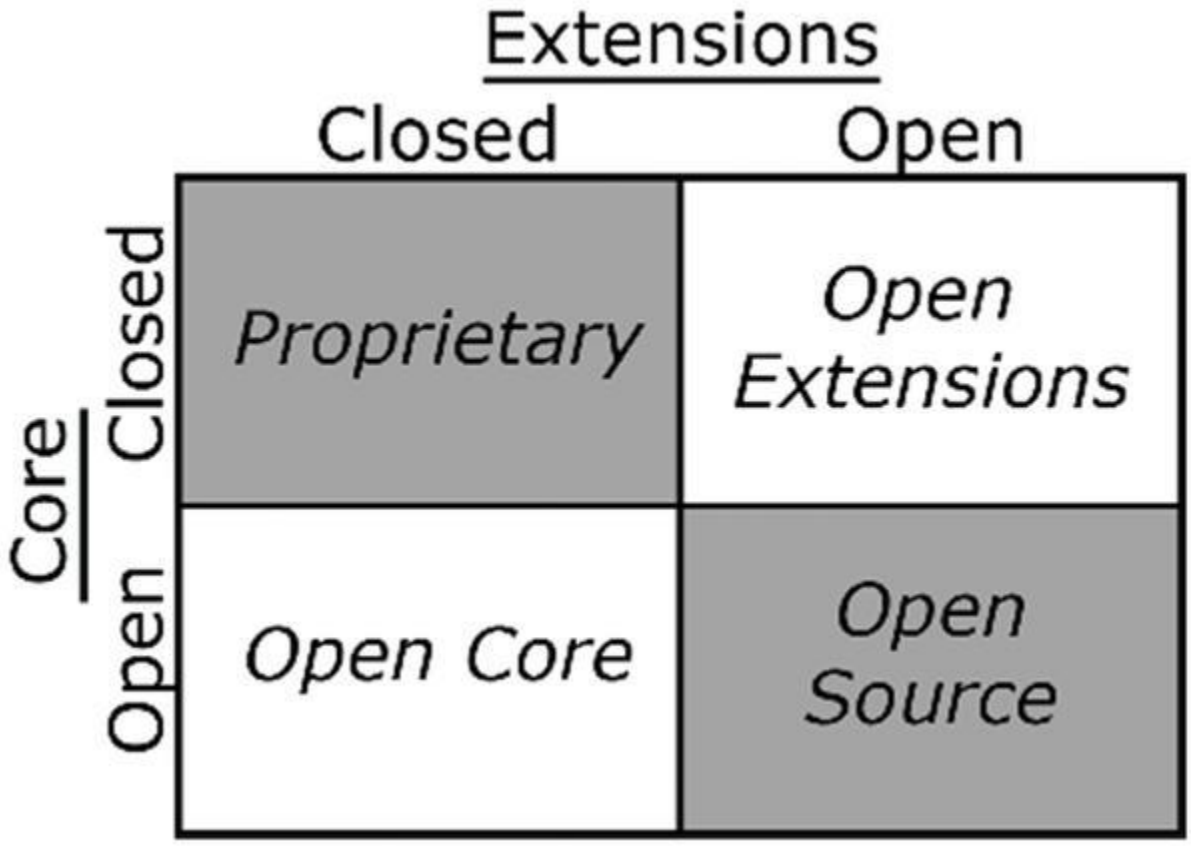

Figure 2 Mixed source business model approach [Adapted form 40].

Depending on individual organization's choice of mixed source options, it should eventually translate the value creation and value capture logic of the firm. Casadesus-Masanell & Llanes [40] argues that purely proprietary models results in higher captured value for organizations but lessens the scope of value creation for users. In contrast, purely open source models can deliver the maximum value to customers but reduce captured value. The key for organizations is to locate the best mix of openness-closeness for an optimum level of value capture and creation. From the business model elements collection, the mixed source approach explain key partners, key activities, key resources and technologies used. From a strategic perspective, this approach to business modeling helps an organization to find a way to scale up or down its business activities.

5 Methodology

This study concerns business possibilities of IoT and mobile device management in the context of futures digital hospital. Since future is elusive and the speed of technology advancements has been rapid during recent decades, we consider the most suitable method for conducting this research to be through qualitative approach. Qualitative methods helps with flexibility and sensitivity to the context that is less explored, and it can facilitate understanding of how things work in a particularly complex setting [41]. We adopt a single qualitative case study approach for this research to explain underlying business potential of a scantly explored industrial context within the existing literature [42].

Table 1 Summary of data used for this research

Data Collection Method	Specialty	Viewpoints	Focus
Interview 1	Pediatric Surgery	Administration, teaching, hospital development, technology and innovations	Pediatric surgery patient journey, concept development of futures digital hospital, digitalization in healthcare.
Interview 2	Anesthesia nurse	New hospital development, hospital ICT inclusion	Same as above
Interview 3	General practice	Secondary-primary healthcare, care process design	Same as above
Interview 4	Pediatric Surgery	General surgery	Same as above
Interview 5	Pediatric Surgery	Specializing, own research	Same as above
Workshop 1	Network specialists, operator service provider, cybersecurity expert	Business opportunity creation, new market exploration, security aspects	Digitalization in healthcare, security business opportunities in health domain, business modeling.
Workshop 2	Operator service provider, cybersecurity expert	Business opportunity creation, new market exploration, security aspects	Digitalization in healthcare, security business opportunities in health domain, business modeling.

Table 1 summarizes the data used for this research. The empirical data used for this study was collected through two streams. First, in order to build the conceptual case of future digital hospitals, five interviews were conducted with pediatric surgery specialists, a nurse, and a

general physician from two hospital districts in Finland. These semi-structured interviews were organized between April and May 2016. These interviews also focused on understanding the journey path in a pediatrics surgery case to clarify suitability of digitalization in the future. However, in the scope of this paper, we do not discuss the patient journey pediatrics surgery in detail. Second, we explored the cybersecurity and business perspectives in two workshops that were organized with telecommunications and cybersecurity experts from the industry. One of the workshops were organized in November 2016. The other workshop took place in August 2017. While the futures digital hospital context from a security perspective relates more towards hospital management and network functionality, the IoT devices and mobile devices perspective is closer to end user security needs. This paper focuses on the cyber security related business opportunities through IoT-MDM systems/services that broadly covers the above mentioned domains. Findings and analysis from the interviews and workshops are presented next.

6 Discussion

In this section, we present our analysis in four steps. First, we briefly discuss the relevance of Internet business models (4C) [10] to the context of the study, addressing how this approach can help cybersecurity providers identify business opportunities in IoT-MDM. Second, we present a 4-quadrant matrix reflecting four different 5G security-provisioning scenarios, which are also relevant to IoT-MDM. Then, we connect each scenario back to business models by applying a mixed-source business model approach [40] and identify different possible business models for each kind of cybersecurity provider. Finally, we connect the overall discussion back to the case of future digital hospital.

6.1 The 4C ICT Business Model Archetypes as an Analytical Tool for Cybersecurity Vendors

The 4C business model archetypes helps decoding the boundaries between multiple business models operating either in the same verticals of the ecosystem or in the same horizontals. These archetypes can provide with a basis to classify and analyze business models of suppliers, competitors, and, at the same time, business models of customers. For this case, the 4C business model archetypes are mostly relevant for cybersecurity providers and IoT-MDM system/service providers as a tool to analyze customer business models and identify customer needs, the hospital management style. These customer needs can eventually be turned around as business opportunities. While IoT-MDM systems and services are not only concerned about cybersecurity, there is room for service providers to customize and tailor services based on customer needs. These service providers either can target customers from one layer (connection/content/context/commerce) across multiple industries, or, they can also target a specific industry (e.g. healthcare) create customized services for all the layers in that industry.

6.2 Generic Cybersecurity Provisioning and Alternative Scenarios

To make sense of the overall cybersecurity provisioning for future 5G, we created the 4-quadrant matrix (Figure 3) by identifying major security drivers for new business creation in future 5G. These scenarios were created in workshops with telecommunication & cybersecurity experts

from the industry. While these service provisioning scenarios are relevant to overall 5G, they are also significantly related to the case of IoT-MDM system/services.

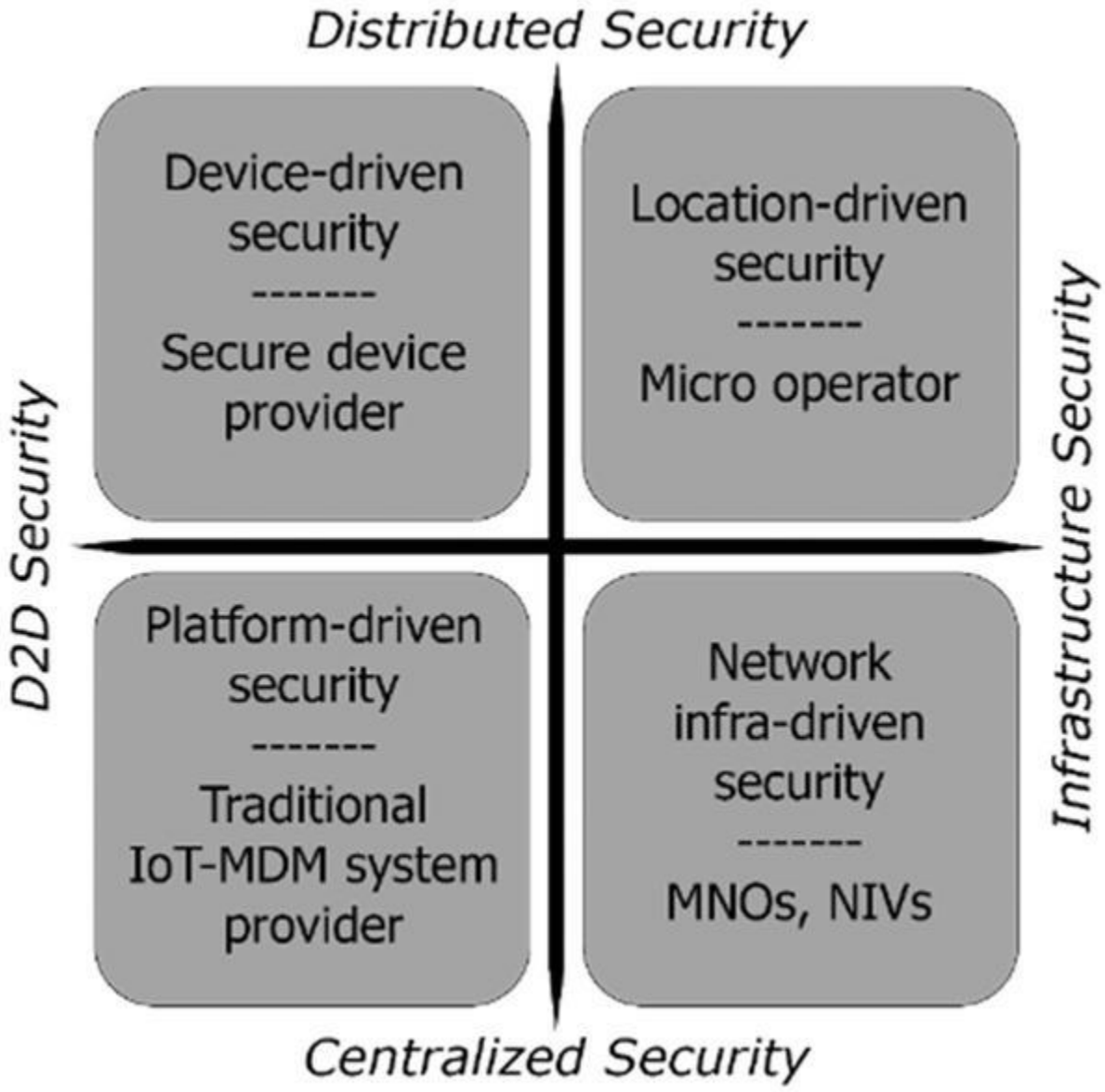

Figure 3 Scenarios for 5G cybersecurity provisioning [Adapted from 35].

As a result, we find four major drivers of security, which potentially will come with new business opportunities in the 5G era. Device driven security comprises distributed and D2D security techniques. Platform driven security will focus on centralized and D2D security techniques. Whereas, network infrastructure driven security should focus on centralized and infrastructure security methods. Lastly, location driven security should harness distributed and infrastructure security techniques.

In a quest to identify potential business entities operating in each of the quadrants relevant to device management, we recognize a ‘secure device manufacturer/provider’ focuses on device-driven security. Currently, multiple device manufacturers are developing devices where security features are built-in, regardless of which network or websites the users are accessing. This built-in security can be offered to multiple kinds of devices including smartphones, tablets, pcs, wearables, and even to IoT devices with communication and computation capability. These secure devices are built in a way that it will control access to potentially harmful networks, websites, and content; even without any commercially available security applications installed. However, when a customer enterprise (e.g. the future digital hospital) is buying a fleet of hundreds of such secure devices, the question raises how to manage and configure all these devices from time-to-time. In such a case, even the secure devices will need IoT-MDM services for proper management and seamless upgrading when needed.

For the platform-driven security, we observe a ‘traditional IoT-MDM system provider’ can be a good example. In many cases, IoT-MDM system providers are selling there device management systems to enterprises directly. And, in other cases, they are selling the service through MNO’s bundled with connectivity and/or infrastructure. While as network infrastructure-driven security, a ‘mobile network operator/carrier’ or a ‘network infrastructure vendor’ can build own IoT-MDM system to offer their clients as well. And, finally, a location-specific micro operator can offer location-driven security. Micro operators offer mobile connectivity combined with specific, local services. The operation of a micro operator is spatially confined to either its premises or to a defined area of operation. As a part of the location-specific services, these micro operators can also offer IoT-MDM services for the users through outsourcing.

6.3 Mixed-Source Business Model Options for Cybersecurity Vendors

Further, we attempt to connect the aforementioned classification and examples of different players offering IoT-MDM services with the mixed source business model approach. Table 2 summarizes our understanding on how each kind of cybersecurity provider can open and mix the core value creation logic for end users. As mentioned previously, the mixed-source business model options are: open source (open core, open extensions), open core (open core, closed extensions), open extensions (closed core, open extensions), and proprietary (closed core, closed extensions). In relation to these mixed-source options, we analyze the plausible options for each of the four distinct cybersecurity providers in the context of this study.

Table 2 Viable mixed-source business model options for IoT-MDM service providers

Cybersecurity Provider	Core Business	Viable Mixed-Source BusinessModel Options
Secure device manufacturer/provider	Secure devices	Proprietary (own device, own IoT-MDM platform), Open extensions (own device, outsourced IoT-MDM service).
Micro operator	Location specific network access	Open source (Users device/ outsourced device, outsourced IoT-MDM service)

Cybersecurity Provider	Core Business	Viable Mixed-Source BusinessModel Options
Traditional IoT-MDM system provider	IoT-MDM systems	Direct open extensions (IoT-MDM systems directly provided to end user enterprise), Indirect open extensions (IoT-MDM service provided through MNOs being outsourced)
MNOs, NIVs	Connectivity, Network infrastructure	Proprietary (own network infrastructure and connectivity, own IoT-MDM system), Open extensions (own network infrastructures and connectivity, outsourced IoT-MDM services)

From a secure device manufacturer perspective, device business can be considered as the core operation whereas IoT-MDM services would be extended solution. A secure device manufacturer/provider can have either a proprietary model or an open extensions model. In the proprietary model, the secure device manufacturer will offer their own devices alongwith their own IoT-MDM system/service. This is a viable case in a sense that customers who are purchasing the fleet of secure devices might prefer the IoT-MDM service from the same vendor, which is ideally less risk prone. Generally, when a customer organization buys a fleet of secure devices, they would expect the device management functions to be offered by the same service provider since integration of multiple systems/interfaces might increase vulnerability and reduce the customer's confidence on the system. However, in practice, not all secure device manufacturer will specialize in automated device management solutions, and new R&D expenses to develop the IoT-MDM systems could result to be financially unfeasible. So, the second option for a secure device manufacturer is to have an open extensions model, where they will still offer the secure devices but outsource the IoT-MDM services to other vendors.

A micro operator's core business relates to location specific network, while they are offering additional location specific services as extensions. Ideally, a micro operator's business model in this case can be considered to be open source. At one hand micro operators are dependent on appropriate available spectrum resources on carriers and NIVs, and on the other hand, outsourcing the IoT-MDM services to other vendors seems more economically feasible than building own system. In contrast, a traditional IoT-MDM system/ service provider can have either a direct-open extensions business model or an indirect-open extensions business model. Unlike the other three archetypes in this discussion, IoT-MDM system/services are the core business for this kind of actor, as device and network related issues can be considered as extensions. An IoT-MDM system/service provider is characteristically dependent on connectivity providers, i.e. MNOs, NIVs. In a direct-open extensions business model, while they are selling the IoT-MDM service directly to the end users, they are using the operator connectivity, but delivering their core value directly. Alternatively, in an indirect-open extensions business model, these IoT-MDM vendors can sell the services through MNOs/NIVs/device vendors to the end users.

Finally, a mobile network operator can either have an open extensions business model, or less likely a proprietary business model for IoT-MDM services. In an open extensions business model, operators will offer own connectivity to end users while outsourcing the IoT-MDM

service to vendors. In very few cases though, operators might have their own IoT-MDM system on offering and thus they can sell both connectivity and IoT-MDM service as a proprietary bundle.

6.4 Summary

Looking back at the case of futures digital hospital, it is deemed to comprise various advanced technology-aided devices, let it be for clinical purposes or communications purpose that support healthcare. With the presence of devices like smartphones, tablets, wearables, connected TVs, VR touchpoints, AR touchpoints, robotic assistance for surgeries, thousands of smart IoT devices, makes the overall device network of the digital hospital complex and need automated centralized management. This centralized management of numerous IoT and mobile devices can be delivered through IoT-MDM system/services. Using the IoT-MDM system/service, the hospital organization can configure, secure, and time-to-time update their device network.

While procuring IoT-MDM services, the above analysis shows that futures digital hospitals can source it either directly from IoT-MDM service providers or through MNOs. Alternatively, if a digital hospital also plays the role of a micro operator, besides offering other location-specific services, the micro operator can also offer device management services by sourcing it from other vendors. In other cases, the future digital hospital can procure fleet of secure devices for the hospital from whom they can also source the device management service as a bundle. From the 4C business models perspective, the hospital organization seems to be a single organizational entity where different activities can be categorized in the 4C layers. Cybersecurity providers can specify and address such issues to highlight and customize their service offering for the future digital hospital.

7 Conclusions

In this article, we have looked at the futures digital hospital context from a device management perspective, and attempted to portray business model options based on how to create and capture economic value from cybersecurity business. Though in this research, we adopt a high-level stance on cybersecurity from a technical perspective, the overall discussions on business potential are relevant to issues like information security, communication security, storage security, security at vulnerable touchpoints in hospital context (end user interface layer, IoT nodes, system layer, network layer).

Futures digital hospitals will be vulnerable to cybersecurity threats because of its data-dependency and digital-intensive device network. Thus, the business opportunity for cybersecurity providers in this case can be considered as the need for automated and centralized IoT-MDM service. To that end, this paper presents four distinct players who can provide such service to a critical infrastructure like a digital hospital. The mixed-source business model options further open up multiple alternatives that each type of vendor can consider while tailoring services for the future digital hospital [40]. This paper also connects the 4C ICT business model archetypes to cybersecurity business context which can be used as an analytical tool to identify customer needs and scope for value creation [10].

Academically, this work contributes by filling up the void in discussing business models for cybersecurity as an industry. In addition, in the existing literature the hospital context has also been less discussed from a cybersecurity business perspective. From an industrial point of view, the business model options discussed in this research are timely and relevant to the market context and need. As mentioned, the mixed source business model options show how cybersecurity providers can extend their offering for different kinds of need for the hospital context based on their core businesses. This study can prove to be helpful for cybersecurity business entities and at the same time hospital managers. The scope of this paper explains business potential of cybersecurity vendors to an emerging industry from a higher level. In this paper, authors do not attempt to analyze the technical aspect of cyber security provisioning in healthcare context, however that is a forthcoming research possibility of this study. Also, since this research is based on a conceptual phenomenon, thus its empirical validation, both qualitatively and quantitatively is still yet to come, which can be considered as a limitation of the study.

All in all, we consider that applying a business perspective to IoT-MDM systems can solve many challenges of a modern mobile IT environment, not only in healthcare but also in other kinds of critical infrastructures [25]. These IoT-MDM systems can be provided by various kind of vendors through a balanced and timely business model.

Acknowledgment

This study has been supported by the DIMECC Cyber Trust – Digital cyber security program.

References

[1] Gomes, J. F., Pikkarainen, M., Ahokangas, P., and Niemelä, R. (2017). Towards business ecosystems for connected health. *Finnish Journal of EHealth and EWelfare*, 9, 95–111. doi:10.23996/fjhw.61004

[2] PWC. (2017). Strategically managing emerging cyber risks. Accessed on: 1 September, 2017. Available at: https://www.pwc.com/us/en/cybersecurity/broader-perspectives/ransomware-global-outbreak.html

[3] Lehto, I., and Ahokangas, P. (2017). "Mobile Security Business Models for Critical Infrastructures – An Ecosystemic Approach", in *Proceedings of the 24th Nordic Academy of Management Conference 2017, Bodo, Norway.*

[4] Pinto, Z. (2013). Cyber security – product of service? Accessed on: 29 August, 2017 Available at: http://www.automationworld.com/security/cyber-security-product-or-service

[5] Loebbecke, C., and Picot, A. (2015). Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. *The Journal of Strategic Information Systems*, 24, 149–157.

[6] Himidan, S., and Kim, P. (2015). The evolving identity, capacity, and capability of the future surgeon. In *Seminars in pediatric surgery*, 24, 145–149, WB Saunders.

[7] Thimbleby, H. (2013). Technology and the future of healthcare. *J. Public Health Res. 2.* doi:10.4081/jphr.2013.e28

[8] Beimborn, D., and Palitza, M. (2013). "Enterprise app stores for mobile applications-development of a benefits framework", in *Proceedings of the Nineteenth Americas Conference on Information Systems,* Chicago, Illinois.

[9] Ortbach, K., Brockmann, T., and Stieglitz, S. (2014). "Drivers for the adoption of mobile device management in organizations", in *proceedings of the Twenty Second European Conference on Information Systems, Tel Aviv 2014.*

[10] Wirtz, B. W., Schilke, O., and Ullrich, S. (2010). Strategic development of business models: implications of the Web 2.0 for creating value on the internet. *Long range planning*, 43, 272–290.

[11] Afuah, A. (2004). *Business Models: A Strategic Management Approach*. McGraw-Hill/Irwin.

[12] Alt, R., and Zimmermann, H. D. (2001). Preface: introduction to special section–business models. *Electronic markets*, 11, 3–9.

[13] Chesbrough, H., and Rosenbloom, R. S. (2002). The role of the business model in capturing value from innovation: evidence from Xerox Corporation's technology spin-off companies. *Industrial and corporate change*, 11, 529–555.

[14] Shafer, S. M., Smith, H. J., and Linder, J. C. (2005). The power of business models. *Business horizons*, 48, 199–207.

[15] Zott, C., and Amit, R. (2010). Business model design: an activity system perspective. *Long range planning*, 43, 216–226.

[16] Takalo, T. (2016). IoT vs. Mobile Device Management. Accessed on: 25 August, 2017. Available at: http://www.capricode.com/iot-vs-mobile/

[17] Gartner. (2011). Magic quadrant for mobile device management software. Available at: http://www.knet.com.au/uploads/5/7/1/8/57184575/magic_quadrant_gartner.pdf

[18] Xu, T., Wendt, J. B., and Potkonjak, M. (2014). Security of IoT systems: Design challenges and opportunities. In *Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design*, 417–423. IEEE Press.

[19] Zhang, Z. K., Cho, M. C. Y., and Shieh, S. (2015). Emerging security threats and countermeasures in IoT. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, 1–6. ACM.

[20] Takalo, T. (2016). Should IoT Device Management be automated? Accessed on: 25 August, 2017. Available at: http://www.capricode.com/automatic-iot-device-management/

[21] Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., and Shieh, S. (2014). IoT security: ongoing challenges and research opportunities. In *Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference*, 230–234. IEEE.

[22] Farooq, M. U., Waseem, M., Khairi, A., and Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *Int. J. Computer Appl.* 111.

[23] Backman, J., Väre, J., Främling, K., Madhikermi, M., and Nykänen, O. (2016). IoT-based interoperability framework for asset and fleet management. In *Emerging Technologies and Factory Automation (ETFA), 2016 IEEE 21st International Conference*, 1–4. IEEE.

[24] Isotalo, L. (2017). "5G Slicing as a Tool to Test User Equipment Against Advanced Persistent Threats", in *International Conference on Network and System Security*, 595–603. Springer, Cham.

[25] Alcaraz, C., and Zeadally, S. (2015). "Critical infrastructure protection: requirements and challenges for the 21st century", in *International Journal of Critical Infrastructure Protection*, *8*, 53–66.

[26] Sutherland, J., and van den Heuvel, W. J. A. M. (2006). Towards an intelligent hospital environment: adaptive workflow in the OR of the future. In *System Sciences, 2006. HICSS'06,* in *Proceedings of the 39th Annual Hawaii International Conference*, 5, 100b–100b. IEEE.

[27] Haq, M. M. (2008). *U.S. Patent No. 7,412,396*. Washington, DC: U.S. Patent and Trademark Office.

[28] Spector, N. D., Cull, W., Daniels, S. R., Gilhooly, J., Hall, J., Horn, I., and Stanton, B. F. (2014). Gender and generational influences on the pediatric workforce and practice. *Pediatrics*, 133, 1112–1121.

[29] Wirtz, B. W. (2011). Business model management. *Design–Instrumente–Erfolgsfaktoren von Geschäftsmodellen*, *2*.

[30] Gomes, J. F., Ahokangas, P., and Owusu, K. A. (2016). Business modeling facilitated cyber preparedness. *Int. J. Business & Cyber Security*, 1, 54–67.

[31] Richardson, J. (2008). The business model: an integrative framework for strategy execution. *Strategic change*, 17, 133–144.

[32] Morris, M., Schindehutte, M., and Allen, J. (2005). The entrepreneur's business model: toward a unified perspective. *J. Business Res.* 58, 726–735.

[33] Zott, C., Amit, R., and Massa, L. (2011). The business model: recent developments and future research. *J. Manage.* 37, 1019–1042.

[34] Teece, D. J. (2010). Business models, business strategy and innovation. *Long range planning*, 43, 172–194.

[35] Gomes, J.F., Iivari, M., Ahokangas, P., Isotalo, L., Sahlin, B., and Melen, J. (Forthcoming, in press), Cyber security business models in 5G. Comprehensive guide to 5G security, Wiley Publishers, London.

[36] Ballon, P. (2007). Business modelling revisited: the configuration of control and value. *info*, 9, 6–19.

[37] Yrjölä, S., Ahokangas, P., and Matinmikko, M. (2015). Evaluation of recent spectrum sharing concepts from business model scalability point of view. In *Dynamic Spectrum Access Networks (DySPAN,* in *2015 IEEE International Symposiu,* 241–250. IEEE.

[38] Ahokangas, P., Moqaddamerad, S., Matinmikko, M., Abouzeid, A., Atkova, I., Gomes, J. F., and Iivari, M. (2016). Future micro operators business models in 5G. *The Business & Management Review*, 7, 143.

[39] Mitola, J., Guerci, J., Reed, J., Yao, Y. D., Chen, Y., Clancy, T., and Guo, Y. (2014). Accelerating 5G QoE via public-private spectrum sharing. *IEEE Communications Magazine*, 52, 77–85.

[40] Casadesus-Masanell, R., and Llanes, G. (2011). Mixed source. *Manage. Sci*. 57, 1212–1230.

[41] Mason, J. (2002). *Qualitative researching*. Sage.

[42] Miles, M. B., and Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.

Biographies

Julius Francis Gomes is pursuing his Ph.D. in international business from the University of Oulu. He currently works at the Oulu Business School as a Doctoral Student to research the futuristic business models for digital intensive industries. His research focuses on using business models as a mean to look in to future industries. He is interested to research business ecosystems in different contexts like cyber security, healthcare, future's network etc. with a business model perspective. He received his M.Sc. (2015) in international business from the University of Oulu. Prior to that he acquired MBA (2011) specializing in managing information systems in business applications. Previously, he has also enjoyed about three years in a top tier bank in Bangladesh as a channel innovator.

Marika Iivari is a postdoctoral researcher at the Martti Ahtisaari Institute within Oulu Business School. She defended her doctoral dissertation on business models in ecosystemic contexts. She holds M.Sc. in International Business from the Ulster University, Northern Ireland. Her research interests are in the areas of open innovation, business models and strategy in the context of innovation ecosystems and smart cities, digital and ICT business ecosystems. She has been involved in several research projects around 5G and the Internet of Things, most recently in the health care sector. She is also an active member of the Business Model Community, the Open Innovation Community and the Society for Collaborative Networks.

Petri Ahokangas received his M.Sc. (1992) and D.Sc. (1998) degrees from the University Vaasa, Finland. He is currently Adjunct Professor (International software entrepreneurship) and Senior research fellow at Martti Ahtisaari Institute, Oulu Business School, University of Oulu, Finland. His research interests are in how innovation and technological change affect international business creation, transformation, and strategies in highly technology – intensive or software – intensive business domains. He has over 100 publications in scientific journals, books, conference proceedings, and other reports. He is actively working in several ICT-focused research consortia leading the business-related research streams.

Lauri Isotalo has received his M.Sc. from Helsinki University of Technology (currently Aalto University) in 1992. He has also a postgraduate Diploma in Business Administration. At first Lauri worked in Nokia Corp. in Mobile Technology & System Marketing unit specializing in Intelligent Networks. In 1992 he joined Elisa Corp. where he has held several managerial positions in value added services business, system and process security and mobile network development. Since 2005 Lauri has also led Elisa SME teams in various international collaboration projects and acquired a deep knowledge of the cyber security of legacy telecommunication networks, ip core, access networks, user terminals and modern virtualized data center IT platforms/cloud systems. From 2014 Lauri has headed SDN&NFV development in Elisa.

Riikka Niemelä, M.Sc., MHSc., is a cross-disciplinary health-tech professional who obtained her degrees in Electrical Engineering (Master of Science) and Medical technology (Master of Health Sciences) from the University of Oulu, Finland. After R&D engineering, she worked as a research assistant to research the national eHealth development of the Finnish healthcare. Thereafter, she has been researching and promoting the adaptation of connected health technologies in surgical processes of a Nordic future hospital, resulting in scientific publications. Currently, she works as a project manager in Tuttlingen, Germany – the world center of Medical Technology – to generate R&D and innovation projects in cooperation with the ICT and LifeScience companies from Oulu, Finland. Her aim is to promote the digitalization and internationalization of the both high-tech regions and to generate innovations serving the increasing demands for healthcare.

Journal of ICT, Vol. 5_1, 107–128.
doi: 10.13052/jicts2245-800X.516