IT Security of Cloud Services and IoT Devices in Healthcare

Michael Gleißner[1,2], Johannes Dotzler[1], Juliana Hartig[1], Andreas Aßmuth[2], Clemens Bulitta[1] and Steffen Hamm[1]

Technical University of Applied Sciences OTH Amberg-Weiden
[1] Hetzenrichter Weg 15, 92637 Weiden, Germany
[2] Kaiser-Wilhelm-Ring 23, 92224 Amberg, Germany

email: {m.gleissner | jo.dotzler | j.hartig | a.assmuth | c.bulitta | s.hamm}@oth-aw.de

***Abstract*—The continuous evolution of new technologies is going to rapidly transform several sectors. A widespread hypothesis claims that especially the healthcare sector will undergo a drastic transformation with the integration of medical Internet of Things (IoT) devices. The use of medical IoT devices results in the implementation of necessary medically approved hardware, software and attached cloud services. This leads to new Information Technology (IT) security challenges and demands for new IT security concepts. This paper aims to identify upcoming security challenges by researching existing IT security guidelines targeting network-connected medical IoT devices, their users and the attached cloud services in homecare and integrated care.**

***Keywords*—Internet of Things; healthcare; medical IoT; cloud services.**

I. Introduction

According to the Check Point Software Technologies Ltd. Security Report from 2020, more than 90 percent of companies use cloud services, with 67 percent of security departments complaining about a lack of transparency in their cloud infrastructure and compliance. The number of attacks on cloud services has increased in 2019 and is expected to continue rising in the following years. Above all, the incorrect configuration of cloud systems is identified to be a major problem [1]. Additionally, the number of active connections to the Internet of Things (IoT) will grow worldwide from 8.74 million in 2020 to 25.44 million in 2030 [2].

The benefits of more devices and cloud services will ensure a high potential for innovation especially in the healthcare sector. However, this also increases the risk of attacks. The healthcare sector is an area where particularly sensitive information is stored and processed. In this field, digitization is seen as a key factor for growth and the opportunity for modernization. Although Germany only ranks second to last when it comes to digitization in the healthcare system compared to other European countries, there is a noticeable change in the market [3]. Further digitization in the health sector will lead to more extensive exchange of sensitive patient data. Since the data requires special protection, the IT security has to be a major focus point.

This paper will describe some of the specific security considerations that need to be made in the healthcare branch when using IoT devices and cloud services. There are some specifics that need to be highlighted in this industry. In Section II, an overview of the status quo concerning IT security for medical applications is provided. Initial analysis of IoT devices and cloud services are presented in Sections III and IV, respectively. Both sections go into more detail specifically for the use cases homecare and integrated care. It shows the different special conditions of the environment from the IT security perspective. This can be used as a blueprint for dealing with cloud services and IoT devices in the healthcare sector.

II. Recent Work in Medical IT Security

With the current Covid-19 pandemic, it is obvious that the healthcare sector is forced to transform itself and adopt new telecommunication technologies more quickly. Therefore, medical IoT device manufacturers are eager to evolve their current hardware and develop additional cloud services, which can already be seen in the rapid digitization of the industrial sector. This trend raises several IT security challenges. Firstly, as mentioned with the development of medical IoT devices, manufacturers are trying to enlarge their business offerings by developing digital services. Secondly, it is obvious that due to financial restrictions medical healthcare facilities are going to integrate their out-of-date medical inventory into their existing IT infrastructure. It is obligatory to note that such devices were never designed to operate in an IoT network, therefore, lacking the required security design to operate in this environment. Additionally, for most older medical devices the original manufacturers either never intended to provide updates from the beginning or stopped doing so. The previously mentioned thoughts clearly illustrate upcoming vulnerabilities. As a consequence, several institutes and enclosed working groups are aiming to guide and regulate medical device manufacturers. An example for a guiding group is the Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745. They published the “Guidance on Cybersecurity for medical devices” [4]. This Medical Device Directive represents a first basis of the ongoing research when it comes to implementing IT security in the field of network-connected medical devices. Also, the International Medical Device Regulators Forum (IMDRF) is investigating cyber threats and is aiming to "promote a globally harmonized approach to medical device cybersecurity that at a fundamental level ensures the safety and performance of medical devices and encouraging information" in their current work item "Medical Device Cybersecurity Guide" [5]. From a national perspective, the German Federal Office For Information Security (BSI) recently published the reports of

 ISBN: 978-1-61208-845-7

their research projects “Manipulation in Medical Products” (ManiMed) and “Digitization in Care” (eCare). These documents contain recommendations for good IT security practices for medical manufacturers. The publication “Cyber Security Requirements for Network-Connected Medical Devices” [6] provides detailed assistance to manufacturers in how identified security threats can be reduced. Even if those concepts are developed, approved and implemented it is still vital to consider how they are embedded into their specific environment. In detail, it is important to differentiate the surroundings (e.g., private home, clinic, elderly home) into which medical IoT devices will be integrated, the technical capabilities of the targeted user and the individual IT landscape into which the devices are integrated.

III. Medical IoT

The Internet of Things is widely known as a landscape of interconnected devices that collect, send and store data over a network. After an initial setup, mostly no human-to-human or human-to-computer interaction is required. In contrast to classic devices, most IoT devices have features known as smart functions, which means that they can access information on the internet, as well as be accessed from outside their local network. In general, two types of IoT devices can be distinguished. While there are IoT devices that require another device (such as a smartphone) in order to establish a connection with the network indirectly, others are connected directly. In order to use IoT devices, connections between the devices are required. These connections can be wired, such as Ethernet, or wireless, e.g., USB, Bluetooth, 5G networks, WiFi and Zigbee, that should be considered in an IT security strategy. Especially in the field of healthcare, specific requirements for certain devices are needed, e.g., connectors for an ECG have standard requirements regarding safety (ANSI/AAMI EC53) [7]. A review of several guidelines and standard literature reveals that the recommendations and specifications are similar to each other and show almost no contradiction. In this respect, different sources of information are being used in this paper, which all have the same direction in approaching the desired security level. The productive usage of IoT devices has a variety of benefits. In relation to the health sector, IoT devices can proactively foresee health conditions and patients can be diagnosed, treated and monitored automatically. IoT devices increase the transparency in tracking of medical objects. Central management enables better visibility for a large number of devices at the same time. This offers an opportunity to relieve medical staff and let them focus on their actual work on patients. As a consequence, hospital stays can be reduced and re-admissions avoided [8]. However, these interconnections represent potential security weaknesses. In the following section potential threats concerning medical IoT devices are discussed. The focus is on general advice influenced by the top-level use cases homecare and integrated care, which are explained in detail in Section III-A and III-B, respectively.

First, a holistic security strategy must be created. This strategy needs to include the overarching infrastructure of the surrounding environment. It is crucial to distinguish whether the environment is safe and controllable (e.g., hospital network) or an unprotected area (e.g., in a patient’s home). In any case, fine-grained access control mechanism and multi-level user administration have to be part of the deployment strategy. Otherwise, especially in unprotected surroundings, this could be an easy gateway for data theft or data manipulation [6]. An investigation by the BSI of six medical products (e.g., senior tablet, emergency watch with fall detection, etc.) shows that this has not been sufficiently taken into account so far. These devices were examined for security vulnerabilities. The bottom line remains: The IT security level of all devices is critical, as moderate to severe weaknesses were identified, which concludes that none of the devices were previously subjected to an IT security test. None of the devices met the requirements of ISO 27001 [9]. Since it is mostly sensitive patient data, encrypted data transmission is essential. The technical guideline TR-02102 of the BSI on cryptographic procedures should be included in the strategy [6].

If the configuration is adapted to the environment, it must be ensured that the specifications for secure implementation are adhered to before commissioning. In concrete terms, this means a separation of software units and the use of already certified and, therefore, approved implementations instead of in-house development of services or protocols. Before medical IoT devices are put into operation, it has to be ensured that the assignment of permissions is restricted by default. Only the privileges necessary for operation should be allowed at its lowest level.

After the devices have been configured and implemented, an automated, auditable and controllable update function must be offered in order to be able to close known vulnerabilities as quickly as possible. Patches and updates for medical IoT devices in Germany have to come from known and trustworthy sources [10].

A. Medical IoT in Homecare

The term homecare describes the treatment of patients with medical aids, dressings and medical diets at home or in nursing homes [11]. In the context of this research, the focus is solely on the applications at home. Products that are being used in nursing homes will be addressed in the Section “Integrated Care" below. In the homecare sector, various applications (e.g., wearables) can support the health system, such as remote monitoring of health progress, improving self-management of chronic conditions, early detection of anomalies, quick identification of symptoms or compliance with medication intake. However, the use of IoT equipment in a remote environment requires a well thought out strategy to allow reaping said benefits whilst neither compromising confidentiality nor integrity.

First, the characteristics of the environment in which an IoT device is to be deployed must be identified. This is necessary in order to derive the precautions, which are needed for secure

 ISBN: 978-1-61208-845-7

operation. The home networks of patients differ vastly in size, complexity and given security. Devices of a home network are unknown and can change at any time. Additionally, it cannot be guaranteed that all network components within the network are state-of-the-art and that their software is being updated regularly. Therefore, the assumption of the worst case scenario has to be made and a generic home network has to be classified as a hostile environment. This requires thorough security hardening of the used IoT devices. A certain security level can be ensured by requiring relevant certifications from the manufacturer, but there are still no specific medical technical certifications, which completely fulfill the conditions of medical surroundings. Another option would be to request a penetration testing report from a well-known cyber security company, but for most applications this is not a suitable option. In practice this could lead to additional time and money, which needs to be spent by the customer if the IoT manufacturer cannot provide such a report by default. This can be justified if the product is used in critical applications. It is therefore highly dependent on the circumstances and the amount of risk that needs to be mitigated. The customers themselves can also proactively increase the network security independently of the manufacturer. A safeguard is network segmentation, where the goal is to completely separate the communication channels of the IoT device from the traffic of the remaining home network. The IoT device is then only able to communicate with its intended communication partners and it cannot be accessed from any other non-trusted network member.

Second, the consumer has to specify the expected benefits and features the product of the manufacturer is supposed to provide. The patients' IT skills have to be taken into consideration. Because a homecare provider has to provide their services to the entire demographic and all social classes, IT knowledge cannot be expected (e.g., elders). Therefore, the set up and maintenance needs to be done by an expert and it should not be possible for a patient to change any security parameters. The specifications also allow identification of communication interfaces which should be enabled or disabled. Reducing the amount of possible communication paths minimizes the attack surface. In the context of homecare this is even more important because of the unsecured and unprotected environment.

B. Medical IoT in Integrated Care

Integrated care is not a well defined term [12]. In this paper integrated care will be referred to as the aspiration to optimize workflows within medical facilities with the help of digitization and IoT. Such facilities could be hospitals, nursing homes, medical offices or any other institutions in the healthcare sector.

Deployment of an IoT device in an integrated care facility needs to be well thought out. The IT security of the IoT device itself must be guaranteed and a secure infrastructure must be available. As with the homecare use case, the first step is to determine how to integrate an IoT product into the network. It is an advantage that the infrastructure, into which a product is deployed, is completely under the customer's control. The customer might provide their patients with WiFi access, for example, so these connections can be seen as unknown members within the network. As a consequence, the patients' connection can be potential threats. But most of the time network segmentation is in place to strongly separate this kind of traffic from the internal communications of the facility. Thus, the focus will only be on integrating IoT devices into the closed off environment of the customer. From the perspective of the IoT device the network can be seen as a trusted environment. However, IoT devices themselves can only be trusted to a certain degree. According to Check Point Software Technologies Ltd. the risk of a data breach through IoT is substantial. It is advisable to the customer to deploy network segmentation in a way that the IoT device only has access to the endpoints, which are needed for it to operate [13].

Again, the specification of all needed features is the foundation that allows for the derivation of the customer's needed IT know-how, as well as the product's communication interfaces required. The customer needs to determine if it is within the capabilities of their staff to set up and maintain the IoT product in question. This depends on the amount of work force and knowledge available, as well as the complexity and number of the products. Additionally, it needs to be ensured that only system administrators are allowed to configure IT security parameters. The staff which is responsible for handling the device in operation then only requires the permission to configure and start the product on a medical level. This is particularly a problem in nursing homes, where there is often neither the required IT knowledge nor enough staff.

IV. Cloud Services

In Section III, the focus was on the security of the IoT device. In the following sections, the chain of communication from an IoT device to its respective cloud services is going to be analyzed. Hereby, a distinction between different types of cloud services is going to be made. At last, the specifics of integrated care as well as homecare are going to be discussed as well.

When it comes to deploying IoT in any environment, considering the device itself as part of the respective network is necessary, but any relationships to the cloud services it is connected to in order to provide either its intended functions or additional features are also relevant. Similarities can be drawn to the Industrial Internet of Things (IIoT). In the IIoT, connections to different services are needed in order provide firmware updates, receive sensor data, achieve remote maintenance, perform analytics and other services [14]. Each cloud service needs to fulfill specific tasks which can differ vastly in complexity and the amount of data which is sent or received over a certain period of time. Therefore, different interfaces, protocols and connection types are needed in order to ensure the desired functionality.

In the health sector an IoT device might be responsible for monitoring vital data of a patient (e.g., heart rate and blood pressure). The manufacturer might require a connection

 ISBN: 978-1-61208-845-7

to their company servers in order to provide security and feature updates on the fly. A second connection might go to the infrastructure of the doctor or health personnel in charge in order to receive the measurements of the sensor for evaluation. Even more connections might be possible for remote maintenance and other services. The work in [15] goes into further detail on which applications might be possible and how such a cloud platform might be implemented. It can be seen that knowledge from industrial applications can be used as a foundation to build on for healthcare use cases. The main difference is that the handled information is far more sensitive and the requirements for availability and stability are far higher. In a worst case scenario a malfunction of the IoT device might decide over life and death.

Three entry points can be identified where a malicious actor might compromise security. The first being the connection itself from a client to the cloud service. In the following paragraph it is assumed that the way a connection is established and maintained from the client to the cloud is secure. This is justified because using common state of the art technology, such as Transport Layer Security (TLS) or a Virtual Private Networks (VPN), already ensures a high level of security. Furthermore, it is not the objective of this paper to evaluate common protocols or standards (e.g., Bluetooth). What is left is the possibility for an attacker to disrupt the connection, for example, with a Denial of Service (DOS) attack. An interruption of communication does not necessarily mean that a malicious actor is present. Other reasons might be technical difficulties of the provider or power outages. It is important for the customer to develop a process in which it is defined how an unexpected interruption is supposed to be handled. The maximum reaction time should be specified. The reaction time is defined as the time difference between the incident happening and the execution of the reaction. Both the steps necessary to handle a security incident and the maximum reaction time are highly dependent on the products and services used as well as the severity of a potential malfunction.

A second entry point might be the device itself. The ability to compromise an IoT device has security implications on the cloud services. Taking control of a device, which is connected to a cloud service, must not lead to a security breach of the cloud service. This can be achieved by minimizing the permissions an IoT device has within the corresponding cloud infrastructure. The provider of the cloud service is responsible for these security measures. Taking a look at the example of monitoring vital data mentioned above the device should only be able to receive updates and send sensor data. When receiving updates the only thing being sent by the device should be the credentials to gain access to said updates. When sending sensor data, only valid data sets are supposed to be accepted by the cloud service. Should the cloud service accept any malformed data sets or instructions, then security might be at risk. Malicious instructions might be sent which were not intended to be executed by design. Then the doors are potentially open for privilege escalation attacks and much more.

The last entry point is the cloud service itself for the IoT devices. This is the most crucial component. A breach of security in the cloud service not only puts at risk the availability or confidentiality of a single device but of all devices using that service. Additionally, other cloud services, which are connected to the compromised instance, in order to further process data, might be affected, too. Depending on the use case the cloud service may require extensive hardening. Guidelines and certifications help ensure the desired level of security. Again, the number of measures that need to be taken depends on the intended use cases and the requirements on the different security goals.

A. Cloud Services in Homecare

As previously established in Section III-A a home network is an inherently hostile environment, therefore, any connection to it must be verified as thoroughly as possible. As a result, each type of application that is supposed to be used in a homecare scenario has to be set up with certain precautions in order to provide a high level of security.

Three major homecare application types have been identified. First, there are management applications for staff in the field. These services help nurses, doctors and other personnel to manage and document every day tasks, patients' health records, schedule appointments and meetings as well as allow them to use the available work force as efficiently as possible. The second category is cloud applications that provide status updates to the patients. Here patients get access to all information related to their treatment. Additional features might be the ability to request appointments or ask questions related to the treatment directly online. The last and most important category for this paper are cloud services, which are connected to the medical IoT devices in the field. These services are responsible for receiving the data that is being collected as well as managing the devices by providing updates or doing remote management tasks.

Management platforms for the nursing staff are very potent tools when it comes to improving the quality of service. Because a staff member has access to the data of various patients the attack surface needs to be as small as possible. This can be done by only allowing managed work devices. These are then able to establish a secure connection to the respective cloud service. A secure connection might be realized with a VPN tunnel. VPNs require competent IT staff in order to operate securely. This has to be kept in mind when considering VPNs as an option because if the required work force and know-how is not present, such a solution will not be implemented properly, leaving the connections vulnerable again.

Patients can be given online access to updates of their treatments or the possibility to request appointments. In most cases these services will be provided over a web interface. Securing it can be a complex task because in the end it is a website with access to patient data. It is important that the provider follows good practices in web development in order to prevent vulnerabilities such as the Open Web Application Security

 ISBN: 978-1-61208-845-7

Project's (OWASP) "Top 10 Web Application Security Risks" [16]. Additionally, the amount of information provided to the patient should be restricted to only what is of relevance to them to limit the amount of information leaked in case of a security breach.

When it comes to monitoring IoT devices, which might send vital parameters to the nursing staff over a cloud service, either in intervals or continuously, it is essential that the connection to their respective platform is sufficiently encrypted and that only authorized devices are allowed to send (and receive) data. VPN tunnels might be an option, which allows the connection from the medical applications to be separated from all potentially malicious network traffic in a patient's home. However, even then the risk remains that an attack consumes the complete bandwidth of the internet connection resulting in a violation of availability.

Before integrating any of the three application types into their productive IT infrastructure, the customer of the cloud service needs to find out how the provider aims to prevent attacks on their products. This is essential because then the customer can compare the measures which have already been taken to their own requirements and evaluate if the level of security is sufficient for their needs.

B. Cloud Services in Integrated Care

In Integrated Care, the network that is supported by a cloud service is completely owned and controlled by the customer. Integrating a cloud service into one's infrastructure can be done in a way that both systems are more interlinked than they would be otherwise. This allows for more possibilities to optimize the workflows within the corresponding premises. Due to the vast amount of possible applications in this context, it is not feasible for this research to cover all possibilities in a competent manner. Instead the focus is on the cloud as an intermediary between IoT devices and the infrastructure of a customer. Data is being sent by the IoT devices to the cloud, where it is being stored to enable the staff of the customer to retrieve the needed information.

In order to assess the necessary precautions that need to be taken, two parameters are to be determined. First, finding out how sensitive/valuable the data sets or assets are, which need to be protected, is necessary. Second, it is important to evaluate the amount of trust that can be given to a potential cloud service provider. Both factors dictate to what extent patient data needs to be protected. For example, if the collected data contains location information of a patient and the service provider is also known to offer commercial activity tracking and other analytics services to customers it can be expected that the service provider is interested in the data sets as well for their own commercial profit [17]. It is then necessary to encrypt the information given to the cloud service provider in order to prevent sensitive information to be leaked to unwanted third parties. An approach where this has been put into practice can be seen in [18] and [19].

Optimally, a zero trust policy is to be established, where access to patient data is only granted to staff who need insight into the data for operation. Due to resource limitations this can not always be put into practice. It is vital for the customer to build a legal framework, where the cloud service provider can be held responsible for neglecting the security of patient data. This should be done in two ways. First, it has to be ensured that the cloud service provider is a trusted and certified entity, where the required know-how exists to provide comprehensive security and service. Certifications such as ISO 27001 are good indicators as to whether the potential service provider takes their information security seriously. Additionally, the customer should not only define the measures that need to be taken by the provider to protect the data from leaks to third parties in a written agreement, but should also record what the cloud service provider is allowed or restricted to do with the stored data. This should be done to avoid any unwanted analytics done by the cloud service provider, which could potentially leak sensitive patient data unwillingly. Finally, security and privacy audits should be carried out on a regular basis.

V. 5G4HEALTHCARE

The mentioned use cases homcare and integrated care are also the main focus of the research project 5G4Healthcare funded by the German Federal Ministry of Transport and Digital Infrastructure. Its goal is to explore the effectiveness and efficiency of healthcare services to derive recommendations for scalable solutions with the help of 5G technology. IT security is a crucial workstream within the project. So far, medical technologies (e.g., mobile ultrasound devices, televisit trolleys, medical robots) have been purchased within the project and are being examined with regard to IT security. The results of the investigations are still pending. However, due to the sensitive data, the relevance of IT security is high, since simply changing medium of communication does not guarantee higher security, which could be a misconception due to the novelty of the 5G technology.

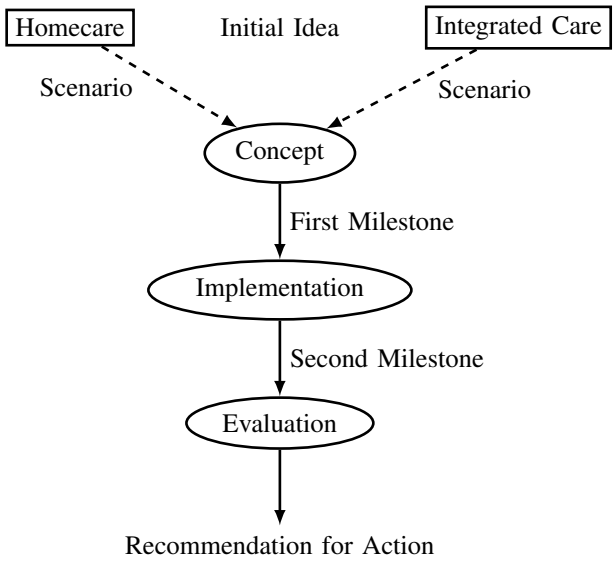

Figure 1. Workflow of a test scenario used by the 5G4Healthcare research project.

 ISBN: 978-1-61208-845-7

As can be seen in Figure 1, application scenarios are designed for the two use cases integrated care and homecare (phase 1), implemented in model form (phase 2) and tested and evaluated (phase 3). A platform based on 5G will be established, that enables testing and evaluation of digital applications in living labs (real-world environments) and test beds. So far it turned out that 5G applications in healthcare must meet essential requirements such as reliability, availability and confidentiality for rapid and high-volume data transmission. 5G enables the continuously increasing capacities of digital applications in terms of bandwidth, availability and latency, which are prioritized differently depending on the application. Most of the products used in the test scenarios are IoT devices with their associated cloud services. These scenarios demand for extensive security evaluation in parallel to the main objective of the research project. Details of the research results will be published in future.

VI. Conclusion and Outlook

This paper points out the need for common IT security guidelines and independent testing laboratories when designing and using medical IoT devices in productive environments. Institutes, regulators and others are currently focusing on developing recommendations and guidelines for IoT manufacturers but no proper entity checks on a regular basis or even worse, never, if manufactures comply with approved guidelines. Moreover, current guidelines do not take into account different environments, e.g., public hospitals or private homes, where medical IoT devices are going to be used. The authors conclude from the analysis made above, that different environments require different set-ups and different configurations. As a result different levels of certain IT-skills are needed for secure operation when embedding medical IoT devices in an existing IT infrastructure. Also, it is obvious that manufacturers are aiming to enlarge their IoT product portfolio by developing supporting cloud services and platforms. The additional cloud service offerings underpin the fact that in contrast to the fourth industrial revolution IoT devices, medical IoT devices need to comply to stricter requirements and should be required to pass recurring testing cycles by specific medical independent regulators. Doing so benefits the patient's well-being and trust. Otherwise, a wide adaptation of trustworthy medical IoT devices in the sensitive healthcare sector is doomed to fail. Mastering those upcoming challenges, which are going to exponentially grow by adopting 5G, must be unequivocally investigated from different perspectives such as environment, users and certifications to guarantee a trustworthy development and usage life cycle. First and foremost, it is obvious that a fine-grained segmentation of IoT devices based on their levels of sensitivity in usage is vital to support the administration and monitoring of sensitive IoT devices and finally ensure a secure operating environment.

VII. Acknowledgement

This research is funded as part of recently granted 5G4Healthcare project by the German Federal Ministry of Transport and Digital Infrastructure within the 5x5G Initiative.

References

[1] Check Point Software Technologies Ltd., "Cyber Security Report 2020," 2020. [Online]. Available: https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf [retrieved: 2021.03.02]

[2] Transforma Insights, "IoT Connected Devices Worldwide 2019-2030," *Statista*, 2020. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ [retrieved: 2021.03.02]

[3] T. Thranberend and T. Kostera, "Digitale Gesundheit: Deutschland hinkt hinterher [Digital Health: Germany is lagging behind]," 2018. [Online]. Available: https://www.bertelsmann-stiftung.de/de/themen/aktuelle-meldungen/2018/november/digitale-gesundheit-deutschland-hinkt-hinterher [retrieved: 2021.03.02]

[4] Medical Device Coordination Group, "MDCG 2019-16 Guidance on Cyber Security for Medical Devices," Dec. 2019. [Online]. Available: https://ec.europa.eu/docsroom/documents/41863/attachments/1/translations/en/renditions/native [retrieved: 2021.03.02]

[5] International Medical Device Regulators Forum, "Medical Device Cybersecurity Guide," 2021. [Online]. Available: http://www.imdrf.org/workitems/wi-mdc-guide.asp [retrieved: 2021.03.02]

[6] Bundesamt für Sicherheit in der Informationstechnik, "Cyber Security Requirements for Network-Connected Medical Devices," Nov. 2018. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/Medical_Devices_CS-E_132.pdf [retrieved: 2021.03.02]

[7] D. Guttadauro, "Electrical Connectors: Design Considerations for Medical Devices," 2019. [Online]. Available: https://www.medicaldesignbriefs.com/component/content/article/mdb/features/articles/33986 [retrieved: 2021.03.02]

[8] GMO GlobalSign Ltd., "Das Gesundheitswesen der Zukunft: Das IoT prägt die Branche schon jetzt [Healthcare of the Future: IoT is already shaping the industry]," Sep. 2018. [Online]. Available: https://www.globalsign.com/de-de/blog/iot-gesundheitswesen-der-zukunft [retrieved: 2021.03.02]

[9] Bundesamt für Sicherheit in der Informationstechnik, "eCare - Digitalisierung in der Pflege - eine aktuelle Marktanalyse und IT-Sicherheitsbetrachtung [eCare - Digitization in Nursing Care - A current market analysis and IT security review]," Dec. 2020. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ DigitaleGesellschaft/eCare_Abschlussbericht.pdf [retrieved: 2021.03.02]

[10] Bundesamt für Sicherheit in der Informationstechnik, "SYS.4.4 Allgemeines IoT-Gerät [SYS.4.4 General IoT Device]," 2021. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs/07_SYS_IT_Systeme/SYS_4_4_Allgemeines_IoT_Geraet_Edition_2020.pdf [retrieved: 2021.03.02]

[11] Bundesverband Medizintechnologie, "Homecare," 2021. [Online]. Available: https://www.bvmed.de/de/versorgung/homecare [retrieved: 2021.03.02]

[12] D. L. Kodner and C. Spreeuwenberg, "Integrated Care: Meaning, Logic, Applications, and Implications – a Discussion Paper," *International Journal of Integrated Care*, vol. 2, no. 4, Nov. 2002. [Online]. Available: http://www.ijic.org/article/10.5334/ijic.67/ [retrieved: 2021.03.29]

[13] Check Point Software Technologies Ltd., "Healthcare Breaches Affected Nearly One Million US Patients: The Security Risks of Medical IoT," May 2019. [Online]. Available: https://blog.checkpoint.com/2019/05/29/ultrasound-iot-hack-security-risks-healthcare-medical-device-michigan-ransomware/ [retrieved: 2021.03.02]

[14] M. Molle *et al.*, "Security of Cloud Services with Low-Performance Devices in Critical Infrastructures," in *The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization*, B. Duncan, Y. W. Lee, M. Westerlund, and A. Aßmuth, Eds., International Academy, Research, and Industry Association. International Academy, Research, and Industry Association, 2019, pp. 88–89.

[15] S. Bharati, P. Podder, M. R. H. Mondal, and P. K. Paul, *Applications and Challenges of Cloud Integrated IoMT*. Cham: Springer International Publishing, 2021, pp. 67–85.

 ISBN: 978-1-61208-845-7

[16] Open Web Application Security Project, "OWASP top ten web application security risks," 2017. [Online]. Available: https://owasp.org/www-project-top-ten/ [retrieved: 2021.03.02]

[17] S. Sharma, K. Chen, and A. Sheth, "Toward Practical Privacy-Preserving Analytics for IoT and Cloud-Based Healthcare Systems," *IEEE Internet Computing*, vol. 22, no. 2, pp. 42–51, 2018.

[18] M. Anuradha *et al.*, "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing," *Microprocessors and Microsystems*, vol. 80, p. 103301, 2021.

[19] R. Denis and P. Madhubala, "Hybrid data encryption model integrating multi-objective adaptive genetic algorithm for secure medical data communication over cloud-based healthcare systems," *Multimedia Tools and Applications*, mar 2021.

 ISBN: 978-1-61208-845-7