Engenharia Moderna: Soluções para Problemas da Sociedade e da Indústria 3

Fábio Andrijauskas
Annete Silva Faesarella
Laira Lucia Damasceno de Oliveira
(Organizadores)

Atena Editora
Ano 2022

Engenharia Moderna: Soluções para Problemas da Sociedade e da Indústria 3

Fábio Andrijauskas
Annete Silva Faesarella
Laira Lucia Damasceno de Oliveira
(Organizadores)

Atena Editora
Ano 2022

Editora chefe
Profª Drª Antonella Carvalho de Oliveira
Editora executiva
Natalia Oliveira
Assistente editorial
Flávia Roberta Barão
Bibliotecária
Janaina Ramos
Projeto gráfico
Bruno Oliveira
Camila Alves de Cremo
Daphynny Pamplona
Luiza Alves Batista
Natália Sandrini de Azevedo
Imagens da capa
iStock
Edição de arte
Luiza Alves Batista

Atena Editora
Ano 2022

Atena
Editora
Ano 2022

Engenharia moderna: soluções para problemas da sociedade e da indústria 3

Diagramação: Camila Alves de Cremo
Correção: Yaiddy Paola Martinez
Indexação: Amanda Kelly da Costa Veiga
Revisão: Os autores
Organizadores: Fábio Andrijauskas
Annete Silva Faesarella
Laira Lucia Damasceno de Oliveira

Dados Internacionais de Catalogação na Publicação (CIP)

E57 Engenharia moderna: soluções para problemas da sociedade e da indústria 3 / Organizadores Fábio Andrijauskas, Annete Silva Faesarella, Laira Lucia Damasceno de Oliveira. – Ponta Grossa - PR: Atena, 2022.

Formato: PDF
Requisitos de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia
ISBN 978-65-258-0095-0
DOI: https://doi.org/10.22533/at.ed.950221105

1. Engenharia. 2. Sociedade. 3. Indústria. I. Fábio Andrijauskas (Organizador). II. Annete Silva Faesarella (Organizadora). III. Laira Lucia Damasceno de Oliveira (Organizadora). IV. Título.

CDD 620

Elaborado por Bibliotecária Janaina Ramos – CRB-8/9166

Atena Editora
Ponta Grossa – Paraná – Brasil
Telefone: +55 (42) 3323-5493
www.atenaeditora.com.br
contato@atenaeditora.com.br

Atena Editora
Ano 2022

DECLARAÇÃO DOS AUTORES

Os autores desta obra: 1. Atestam não possuir qualquer interesse comercial que constitua um conflito de interesses em relação ao artigo científico publicado; 2. Declaram que participaram ativamente da construção dos respectivos manuscritos, preferencialmente na: a) Concepção do estudo, e/ou aquisição de dados, e/ou análise e interpretação de dados; b) Elaboração do artigo ou revisão com vistas a tornar o material intelectualmente relevante; c) Aprovação final do manuscrito para submissão.; 3. Certificam que os artigos científicos publicados estão completamente isentos de dados e/ou resultados fraudulentos; 4. Confirmam a citação e a referência correta de todos os dados e de interpretações de dados de outras pesquisas; 5. Reconhecem terem informado todas as fontes de financiamento recebidas para a consecução da pesquisa; 6. Autorizam a edição da obra, que incluem os registros de ficha catalográfica, ISBN, DOI e demais indexadores, projeto visual e criação de capa, diagramação de miolo, assim como lançamento e divulgação da mesma conforme critérios da Atena Editora.

DECLARAÇÃO DA EDITORA

A Atena Editora declara, para os devidos fins de direito, que: 1. A presente publicação constitui apenas transferência temporária dos direitos autorais, direito sobre a publicação, inclusive não constitui responsabilidade solidária na criação dos manuscritos publicados, nos termos previstos na Lei sobre direitos autorais (Lei 9610/98), no art. 184 do Código Penal e no art. 927 do Código Civil; 2. Autoriza e incentiva os autores a assinarem contratos com repositórios institucionais, com fins exclusivos de divulgação da obra, desde que com o devido reconhecimento de autoria e edição e sem qualquer finalidade comercial; 3. Todos os e-book são *open access, desta forma* não os comercializa em seu site, sites parceiros, plataformas de *e-commerce,* ou qualquer outro meio virtual ou físico, portanto, está isenta de repasses de direitos autorais aos autores; 4. Todos os membros do conselho editorial são doutores e vinculados a instituições de ensino superior públicas, conforme recomendação da CAPES para obtenção do Qualis livro; 5. Não cede, comercializa ou autoriza a utilização dos nomes e e-mails dos autores, bem como nenhum outro dado dos mesmos, para qualquer finalidade que não o escopo da divulgação desta obra.

Atena
Editora
Ano 2022

APRESENTAÇÃO

Nos anos de 2020 e 2021 tivemos a primeira e a segunda edição do livro “Engenharia Moderna: Soluções para Problemas da Sociedade e da Indústria’’ e agora, em 2022, com muito orgulho lançamos sua terceira edição. Esta edição atual provém de trabalhos desenvolvidos durante a pandemia da COVID-19, um período que nos fez refletir sobre a importância da ciência e o desenvolvimento tecnológico no mundo atual, aliados na descoberta de soluções para problemas de diferentes âmbitos, haja vista as vacinas desenvolvidas no intuito de resolver esta situação tão sensível e desafiadora. Realmente, um momento que mudou a vida de todos e que ficará para sempre em nossas lembranças.

Em tempos que, mais do que nunca, necessitam de união e paz, apresentamos este conteúdo com diversos autores, demonstrando que a diversidade de pensamento, ideias e conhecimento são pilares para o avanço da ciência. Cada capítulo foi elaborado com dedicação e comprometimento dos pesquisadores, e traz mais um resultado de sucesso para diversas áreas do conhecimento, como as Engenharias, a Saúde e o Meio Ambiente.

Mais uma vez, agradecemos à Editora Atena pela oportunidade do lançamento do nosso terceiro livro, proporcionando uma via eficaz de disseminação de conhecimento e de suas contribuições para a sociedade e para a comunidade científica.

Finalizamos com uma frase da oração de São Francisco que diz: “**Senhor, fazei de mim instrumento de vossa paz**”.

Paz e bem!

Annete Silva Faesarella

Fábio Andrijauskas

Laira Lucia Damasceno de Oliveira

SUMÁRIO

CAPÍTULO 1

A MODERN PANORAMA OF THE INTERNET OF MEDICAL THINGS DEMONSTRATING ITS APPLICATION LANDSCAPE

Reinaldo Padilha França
School of Electrical and Computer Engineering (FEEC)
State University of Campinas (UNICAMP)
Campinas – SP
orcid.org/0000-0002-7901-6691

Ana Carolina Borges Monteiro
School of Electrical and Computer Engineering (FEEC)
State University of Campinas (UNICAMP)
Campinas – SP
orcid.org/0000-0002-8631-6617

Rangel Arthur
Faculty of Technology (FT)
State University of Campinas (UNICAMP)
Campinas – SP
orcid.org/0000-0002-4138-4720

Francisco Fambrini
Faculty of Technology (FT)
State University of Campinas (UNICAMP)
Campinas – SP
orcid.org/ 0000-0002-8841-5803

Julio Cesar Pereira
Faculty of Technology (FT)
State University of Campinas (UNICAMP)
Campinas – SP
orcid.org/0000-0002-4546-3282

Vicente Idalberto Becerra Sablón
College of Electrical Engineering (EE)
São Francisco University (USF)
Campinas – SP
https://orcid.org/0000-0003-3127-1906

Yuzo Iano
School of Electrical and Computer Engineering (FEEC)
State University of Campinas (UNICAMP)
Campinas – SP
orcid.org/0000-0002-9843-9761

ABSTRACT: Internet of Medical Things is a strand of IoT within the health sector relating to patient monitoring and diagnostics; data collection, transfer, storage, and collaboration between digital systems, i.e., the adoption of technology by the various branches of activity in the medical sector. Considering since patients are connected to sensors to measure vital signs and other biometric information, problems can be quickly diagnosed, through IoMT a better quality health service can be provided, and the resources used more efficiently, as also the performance of IoMT among smart health devices and tools. Also relating that IoMT technology can be the precursor to help prevent and manage current and future pandemics, since any component of an IoMT health system must have sufficient cybersecurity against a maliciously intended digital attempt, considering that when deployed on a large scale. As also considering that it is necessary to provide high-quality health care throughout the health care cycle, health IoMT applications must be digitally secure, as patients expect private information to remain confidential by relating private health information concerning data collection by the IoMT with specific parameters, it must also at the same time guarantee privacy related to patient

privacy based on a wide spectrum of the sharing of information. Therefore, this manuscript aims to provide an updated overview of the Internet of Medical Things and your technologies, showing the fundamentals of this disruptive technology, demonstrating a landscape view to the applied aspect, as also key concerns, and challenges, with a concise bibliographic background, featuring the potential of technologies.
KEYWORDS: Analytics, Big Data, Machine Learning, IoMT, IoT, Artificial Intelligence, Smart Medical Sensors, Privacy, Security, IoMT devices, Medical Data.

1 | INTRODUCTION

Far beyond the aspects of our personal life, technology is drastically influencing all sectors of society, emphasizing all its communication aimed at the digital universe towards progress, representing that technology has become society's most powerful ally, transforming all processes in digital. Exemplifying how modern communication is based on technology as its direct channel, responsible for reading and translating the voice of a client in a business environment or even patients in health institutions, generating properties capable of connecting and satisfying clients/patients through experiences based on smart software. This represents in the modern contemporary world, the customer experience exceeds the price and the product as the key differentiator of a given brand, i.e., people tend to pay more to have a better experience, and this is also applied in the health sector (FUKUDA, 2020).

After the adoption of IoT by the various branches of society, it was natural that an adaptation movement according to the challenges faced by the health sector would occur. Analyzing that the digital technology experience provided by IoT applied in health care offers patients a dynamic and continuous posture, transforming processes into digital to move static processes, slowness, and ignorance of the patient (TARDIEU, DALY, ESTEBAN-LAUZÁN, HALL, MILLER, 2020).

When relating digital transformation to the most current and modern digital presence currently existing in society, consisting of the most expressive example is the use of smartphones. Representing devices that are easy to use and intuitive, that the common resistance to new technologies has disappeared, even considering that these devices can receive data analysis and diagnostic analysis reports on a doctor's smartphone, representing practicality combined with time savings, which are crucial in the health sector (DORSEY, MCCONNELL, SHAW, TRISTER, FRIEND, 2017).

Considering that the Internet of Things is a concept with its main characteristics in the exchange of information, being more closely linked to companies and the maximization of production together with an improvement in results and revenue, also aiming to improve the management of a given system of which the device is part, seeking to develop devices connected to the internet and with communication power. This technology also increases

the performance of this device that is part of a given system through external data, analyzed that IoT is not only used for sending messages, but also for receiving (FRANÇA, MONTEIRO, ARTHUR, IANO, 2020; ADRYAN, OBERMAIER, FREMANTLE, 2017; FRANÇA, MONTEIRO, ARTHUR, IANO, 2020).

When relating health and the application of IoT, the Internet of Medical Things emerges, treated as an evolution of IoT, focused exclusively on health. Used to achieve goals related to the provision of personalized service, through mobile devices equipped with smart applications, emergency care kits, medical equipment for home use, service applications, among others, that is, with data-driven treatment through the use of devices adapted to patients (JOYIA, LIAQAT, FAROOQ, REHMAN, 2017; SHIN, HWANG, 2017; HASSANIEN, DEY, BORRA, 2018).

IoMT corresponds to the Internet of Medical Things, a connected infrastructure that collects, groups, and transmits data with the potential to transform medical technology and the healthcare industry, automating key processes and improving diagnosis and treatment. The growth is attributed to the need to digitize health systems, as the population ages, the demand for those suffering from chronic diseases increases, requiring more efficient mobile health technologies. However, one of the main challenges is still in the education of professionals to correctly read the information generated by these devices and make their diagnoses (JOYIA, LIAQAT, FAROOQ, REHMAN, 2017; SHIN, HWANG, 2017; HASSANIEN, DEY, BORRA, 2018).

IoMT will reach the health sector in a disruptive way, with health institutions supporting this technology, depending heavily on the ability to understand the breadth of the transformation it needs and the challenge of implementing their digital strategies as quickly as possible. Considering that the essence of IoMT basically consists of digitization of processes followed by dematerialization (be it paper or other forms of registration), consequently democratization and ultimately disruption. Analyzing that IoMT technology is not just a massive adoption of new technologies and devices, but a digital revolution in the modern world related to health (JOYIA, LIAQAT, FAROOQ, REHMAN, 2017; SHEHABAT, AL-HUSSEIN, 2018; BAKER, XIANG, ATKINSON, 2017).

Analyzing that the number of elderly people worldwide increases exponentially, that is, people over 60 years of age, representing that these individuals will need more care and monitoring, from this focus is this is one of the main utilities and applicability of IoMT (SHEHABAT, AL-HUSSEIN, 2018; BAKER, XIANG, ATKINSON, 2017).

Or even relating that the real value offered by IoMT lies in the impact that can be caused by the appropriate use of the wealth of data collected by the numerous devices and platforms of IoMT, and not only in technology and its autonomy but which can be much more significant. Reaching fields of modern medicine such as precision medicine, it can gather large volumes and a wide variety of patient data in a highly precise and detailed manner.

This can allow doctors an unprecedented level of perception of patients' health. Considering that IoMT platforms can be used to collect data directly from diagnostic devices, such as those used to measure blood glucose, blood pressure heart rate, and among many other aspects, and compiling this information in a centralized repository, considering that this compiled data can be used to obtain a clear picture of an individual/patient's health situation (HASSANIEN, DEY, BORRA, 2018; MANOGARAN, CHILAMKURTI, HSU, 2018; FRANÇA, MONTEIRO, ARTHUR, IANO, 2021).

Therefore, this chapter aims to provide an updated overview of the Internet of Medical Things and your technologies, showing the fundamentals of this disruptive technology, demonstrating a landscape view to the applied aspect, as also key concerns, and challenges, with a concise bibliographic background, featuring the potential of technologies.

2 | IOMT FUNDAMENTALS

Health applications aggregating IoT potentially have the possibility of offering patient care in various configurations, including treatment for acute cases (in the hospital), long-term treatment (through "home care"), community-based treatment (typically residential), and even has the potential to precisely track people, supplies, equipment, or even service animals and also analyzing the captured digital data (FRANÇA, MONTEIRO, ARTHUR, IANO, 2020; FRANÇA, MONTEIRO, ARTHUR, IANO, 2020)

With the emergence of the Internet of Medical Things, a strand of IoT within the health sector emerged, relating to the adoption of IoT technology by the various branches of activity in the medical sector. Since patients are connected to sensors to measure vital signs and other biometric information, problems can be quickly diagnosed, through IoMT a better quality health service can be provided, and the resources are used more efficiently (SAHEB, IZADI, 2019; CHEN, HO, LIU, LU, 2017; DIN, ALMOGREN, GUIZANI, ZUAIR, 2019).

A more global view of IoT in health can include the following areas such as patient monitoring and diagnostics; data collection, transfer, storage, and collaboration between digital systems; the performance of IoMT among smart health devices and tools such as smart wheelchairs, RFID tags, sensors, smart beds, among others; and even with regard to the connected emergency units, response vehicles such as ambulance, and other hospital sectors connected by the IoMT (KSHIRSAGAR, POTE, PALIWAL, HENDRE, CHIPPALKATTI, DHABEKAR, 2020; ZAMANIFAR, 2020).

In this context, it is worth mentioning the importance of applying IoMT wearables through smart bracelets and watches, as more common examples, allowing the monitoring of a series of items, such as heartbeat, the number of steps, movement, among other aspects (QURESHI, KRISHNAN, 2018; LUNA-DELRISCO, PALACIO, OROZCO, MONCADA, PALACIO, MONTEALEGRE, DIAZ-FORERO, 2018; ADENIYI, OGUNDOKUN,

AWOTUNDE, 2021).

As well as several other application examples that are already being used by doctor's offices and hospitals to provide better care for their patients, such as the use of smart beds, reading various vital indicators of the patient, informing a central system about their condition. Or even the use of RFID tags, which allow equipment through radio frequency within an environment, monitoring, and management of medical assets (ASHWINI, VIMALA, 2020).

However, an important technological aspect is related to threats to digital security, recognizing the respective concerns of data leaks, geographical limitations, and even digital privacy. Although the technology has advanced enough to transfer data between the cloud and a multitude of connected devices, the security of IoT devices and data remains of concern, considering that IoMT is an applied aspect of IoT. In this respect, the concern is valid considering that an advanced and wearable intelligent IoMT sensor continuously transmits confidential data about a patient's health condition. In addition, data privacy becomes a highly confidential matter in the event of a pandemic, such as COVID-19 today, when it comes to contact tracking (FRANÇA, MONTEIRO, ARTHUR, IANO, 2021; HUREIB, GUTUB, 2020).

However, in general, IoT security concerns or their vulnerabilities need to be addressed by manufacturers and developers, technically listing advances in protecting devices or related software from digital intruders, before IoMT devices are distributed in a secure environment health institution. Relating that IoMT technology can be the precursor to help prevent and manage current and future pandemics, considering that when deployed on a large scale, IoMT provides society with an incomparable amount of data, from monitoring patients' biometric signals to identifying when an elderly patient falls using data from an accelerometer, and analysis in the face of catastrophes (SINGH, JAVAID, HALEEM, SUMAN, 2020; ZHANG, WU, 2020; NDIAYE, OYEWOBI, ABU-MAHFOUZ, HANCKE, KURIEN, DJOUANI, 2020).

In this sense, health IoMT applications must be digitally secure, since any component of an IoMT health system must have sufficient cybersecurity against a maliciously intended digital attempt. Because this proportionately affects digital privacy, as patients expect specific private information to remain confidential by relating private health information in relation to data collection by the IoMT with specific parameters related to patient privacy based on a wide spectrum of factors, such as profession, genre, age, religion, and even any others personal preference. Therefore, IoMT health systems must allow the sharing of information, considering that the technological factor is necessary to provide high-quality health care throughout the health care cycle and, however, it must also at the same time guarantee privacy (HUREIB, GUTUB, 2020).

IoMT's digital trust must correspond with respect to the aspects in which the

information being “captured” by the sensors, remain correct, not be corrupted in any way at the source or transmission, or deliberately altered by some “malware” that gains access to unwanted on the IoMT platform via the Internet. Considering that this information, if corrupted, results in aspects of reliability in the information traffic via the health IoMT system, which discredits the technology in relation to patient care, allowing a better evaluation, supervision, and treatment (ALSUBAEI, ABUHUSSEIN, SHANDILYA, SHIVA, 2019).

3 | IOMT IN HEALTH

Considering the existence of several benefits regarding the application of IoMT in health organizations and institutions, it is possible to consider the following advantages in relation to consistent data, considering that a common problem faced in the health sector is the lack of information about this sense, the access of consistent data by health professionals, hindering a more assertive service, based on past data (TARDIEU, DALY, ESTEBAN-LAUZÁN, HALL, MILLER, 2020).

Also considering the remote access that relieves health clinics and hospitals, allowing patients to be monitored through remote access, allowing a lot of data to be collected for assistance, and preventing patients from having to be kept waiting in the clinic environment or from the hospital. This guarantees greater comfort and tranquility to the patient, who can continue with all his activities normally and, if he has any health problem that needs assistance, he can get in direct contact with any available professional (THUEMMLER, BAI, 2017; ESTRELA, MONTEIRO, FRANÇA, IANO, KHELASSI, RAZMJOOY, 2018).

Personalized service is another benefit that IoMT provides, in view of the volume of consistent patient data through the use of IoMT devices implanted in it, guarantees a personalized analysis for each case. Since, through this, health professionals discover habits and other information concerning health problems helping in a later treatment or even avoiding the appearance of any complications (SHABAN-NEJAD, MICHALOWSKI, BUCKERIDGE, 2018).

Or even with regard to constant feedback based on the monitoring facilitated through these IoMT devices allowing there to be continuous and uninterrupted medical feedback about the patient’s reactions to the treatment applied. In this sense, the health professional will be able to check the clinical status in real-time of the patient’s behavior according to the treatment given, since the IoMT allows a more assertive decision making between continuing or changing the medical approach (FARAHANI, FIROUZI, CHAKRABARTY, 2020; PARK, CHOI, 2019).

It is also possible to mention applications of the capacity of IoMT technology in relation to sleep monitoring, through wearables used in conjunction with intelligent algorithms to identify atrial fibrillation. Or even with regard to IoMT application systems aimed at patients

suffering from bulimia (eating disorder), considering the use of sensors in the patient's environment, whether, in a hospital or even home monitoring, it can detect the increase in the temperature of the patient body or blood pressure or even types of odors, as vomit (YACCHIREMA, SARABIA-JÁCOME, PALAU, ESTEVE, 2018)

Or, the possibility of using IoMT sensors that can be used to detect abuse of physical exercises such as excessive cardiac training or an accelerated walking activity when compared to walking at a normal pace. Analyzing the data obtained and collected from these activities, representing that this can provide valuable information in the diagnosis and management of related diseases (ALEXANDRE, POSTOLACHE, 2018)

Also mentions that IoMT technology can be used in terms of geolocation, in relation to the prevention of errant behavior or other undesirable mobility behaviors of patients with Alzheimer's Disease. Considering that these patients suffer from comorbidities with other diseases, such as hypertension, macular degeneration, or even diabetes, aiming at the use of interconnected IoMT devices capturing data to monitor the unique signs and symptoms of these conditions. Since that, it is possible to use IoMT in conjunction with Artificial Intelligence techniques, such as Machine Learning, providing a more continuous, proactive, and personalized care for Alzheimer's patients. In this example, it is possible to highlight the use of IoMT technology in the area of care for the elderly, as a useful and timely approach (ALJEHANI, ALHAZMI, ALOUFI, ALJEHANI, ABDULRAHMAN, 2018)

As well, through the IoMT technology, it is possible to provide a policy level of "zero tolerance" to violence related to so much violence from visitors and families directed to health service workers or patients, or even records of violence among health workers, although health institutions are equipped with video surveillance systems. Through IoMT technology, it is possible to track the movement of medical service personnel, patients, and visitors, which can generate warnings of threatening behavior, or even through biometric sensors could also be used to detect aggression or stress of those who are using or residing in institutions of health (RODRÍGUEZ-RODRÍGUEZ, RODRÍGUEZ, ELIZONDO-MORENO, HERAS-GONZÁLEZ, GENTILI, 2020).

Also relating that in hospital environments, scarce resources are shared such as electrocardiogram equipment, infusion pumps, oxygen tanks, and analgesic medication pumps controlled by patients can be tracked via IoMT, keeping a record of maintenance and monitoring of this equipment. Also aiming that IoMT technology could also be used to monitor the equipment that needs maintenance (recharged or calibrated) to alert the maintenance team of such conditions (JOYIA, LIAQAT, FAROOQ, REHMAN, 2017; SHIN, HWANG, 2017).

It is also possible to employ an RFID tag or barcode tag allowing many supplies to be tagged for scanning, screening, or even checked out of the warehouse or administered to the patient, facilitating the billing of the service provided, in cases of care treatments for

acute cases or long-term treatment. Also considering that in a residential setting, medical supplies could be tagged with RFID tags to monitor and alert when the amount of that supply is small or even alert the home care team when an item is being overused (JOYIA, LIAQAT, FAROOQ, REHMAN, 2017; SHIN, HWANG, 2017).

4 | IOMT AND BIG DATA

With IoT, "wearable" devices, and mobility (in general), health will have something extremely valuable in your hands, i.e., patient data, considering data in different formats ("big data"), it is possible to use data analysis ("data analytics") to detect the "patterns" of data collected from patients via "wearables", which will monitor the symptoms of disease in patients, representing the evolution of data by "wearable" technology for science "big data" or even "data analytics". This will help the doctor measure the progression of the disease by capturing and, objectively, "measuring" the real experiences of the patients and, thus, accelerating the progress of advances in the development of medicines, diagnosis, and treatment, through the "trilogy": IoT, representing the "ability to enable better decisions by collecting and analyzing data from new sources; "wearable" and "big data" technology, representing the analytical part (of the data) (NANDA, KHATTAR, NANDA, 2019; BAIG, GHOLAMHOSSEINI, MOQEEM, MIRZA, LINDÉN, 2017; BALINSKI, BAZAR, NESBITT, OLSON, PATIL, PUNADIKAR, 2019).

The "Big Data" technology explores the possibility of manipulating structured data which contains a determined structure, with restrictions on possible categories and values; and unstructured, considering that these types are basically texts that diverge in their structure from one entry to another, consistent with the information that patients share with doctors, employers, insurance companies and government agencies. Considering that health systems are currently immersed in a "sea" of data regarding clinical histories and patient genetic information, the results of clinical trials, information from sensors that monitor biometric parameters, and even the various intelligent applications and solutions for digital health (FRANÇA, MONTEIRO, ARTHUR, IANO, 2021; FRANÇA, MONTEIRO, ARTHUR, IANO, 2020; PADILHA, IANO, MONTEIRO, ARTHUR, 2021).

In other words, the more sources there are, the greater the chances of generating useful information, even considering that in contrast, the computational complexity increases. Representing the Big Data differential is linked to the possibility and opportunity to cross this immense volume of information to obtain important insights. The key is that this volume of information can be analyzed and processed to generate insights and help doctors and specialists in strategic decisions, whether it be the approach to better clinical treatment or to optimize time and improve patient care. In general, with regard to data, the state of the art in artificial intelligence is applied to empower doctors in the delivery of increasingly accurate

reports (FRANÇA, MONTEIRO, ARTHUR, IANO, 2020; MARTIN-SANCHEZ, VERSPOOR, 2014; RISTEVSKI, CHEN, 2018).

Considering this huge data volume, many of these data are not structured, that is, X-ray exams, magnetic resonance exams, messages, and posts in internal healthcare management systems, among others, which cannot be managed with databases traditional data. From that, these data are generated, analyzed, and explored at a high speed of computational processing, processing that data that the IoMT sensors send in real-time and that also collect from a patient's vital signs (LEE, YOON, 2017).

From a global point of view, based on the development of an integrated database, including genomic data, clinical data or traditional electronic medical records and data from "wearable" technology, through the growing interest in Big Data related to IoMT in health, as well as serving as a basis for a more accurate understanding of the patient and his illnesses, and providing a more granular view of effective "interventions". In the same way, it is also possible to employ the use of medical data as a factor for product innovation, through the creation of customized products and solutions, generally oriented with investment in "wearable" technology. Since IoMT wearable technology for medicine includes the opportunity to measure health in order to participate more naturally in patients' life flow, providing a richer and more complete assessment of "nuances" than conventional ones that are already offered by traditional healthcare laboratories, and clinics (ESTRELA, MONTEIRO, FRANÇA, IANO, KHELASSI, RAZMJOOY, 2018; FERRER-ROCA, MÉNDEZ, 2012).

Also considering that the data collection must be equally heterogeneous, i.e., from requests for compensation to doctor's notes within the medical record, images of patient exams, messages exchanged between doctors and patients about health, as well as listing posts in the social media, and information from wearable technology and other monitoring devices. This heterogeneity makes the extraction and integration of this large amount of data generated and collected in many different formats a real challenge, stressing that the standardization of information is fundamental in order to create a large database of patients (ESTRELA, MONTEIRO, FRANÇA, IANO, KHELASSI, RAZMJOOY, 2018).

Obviously, at first, health institutions will face many problems for the implementation and development of the IoMT and the implementation of Analytics tools such as Big Data, having seen the diversity of economic and financial realities as well as the even more pronounced diversity when relating the structured hospital, and more specifically, the technological structure, wherein many of these institutions this reality does not even exist, with an evident discrepancy not only in information but also in infrastructure (LEE, YOON, 2017).

5 | ASPECTS OF DIGITAL SECURITY AND PRIVACY AT IOMT

In digital health, IoMT applications and devices for monitoring personal activities, electronic medical records, exams, and online reports sent remotely, and digital files provided by healthcare institutions, such as clinics, work wards, among many others. Considering that is collected what is generated and that can be captured in the health area as the patient's personal data (individual identification document, gender, name, date of birth, affiliation, place of residence), clinical data (risk habits, diagnoses, medications are taken, vaccinations, allergies), exam data (imaging exams, electrocardiogram exams (ECG), Electroencephalogram exams (EEG), blood exams, oximetry exams, spirometry exams among many others), and even considering data from medical procedures (hospitalizations, interventions received, surgeries, ICU stay times, among others) (FRANÇA, MONTEIRO, ARTHUR, IANO, 2021).

In this sense, it is necessary and important the attention to and adequacy of internal processes and cultures in order to guarantee the digital security of patient data against the sharing of information without consent. Preventing the proliferation of a type of personal data market for commercial purposes without the patient's authorization, such as the sale of personal information initially collected for other purposes to other companies (TAITSMAN, GRIMM, AGRAWAL, 2013; ABOUELMEHDI, BENI-HSSANE, KHALOUFI, SAADI, 2017).

It is essential to aim to increase the security of confidential information, treating more rigorously the data passed between the systems of the health institutions themselves, between clinics and hospitals, laboratories or health operators, valid for every information transaction, not necessarily only for the electronic part, that is, data recorded on paper, for example, also need authorization. In addition to needing to be authorized by patients, sharing of this information must be done if the messages are encrypted, that is, encrypted (ABOUELMEHDI, BENI-HSSANE, KHALOUFI, SAADI, 2017).

This should be applied to a wide range of situations, such as telemedicine, health service charges, information exchange between different healthcare institutions, such as requests for laboratory tests, messages exchanged between doctors and patients, or even mailboxes with messages. Persistent drugs must also be protected, as it contains patient identification, among others. Or even employ digital measures in which patients' personal data, as well as all information transmissions in the system, must be encrypted and, after fulfilling the objective; must be erased. Considering the clarification that, in principle, the sending of information regarding billing will not need consent, but if there is more detailed clinical data, such as a medical report, there is absolute clarity about the patient, there is also a need for encryption of this document (GARG, BREWER, 2011; MAKRIS, ARGIRIOU, STRINTZIS, 1997).

In this sense of digital security, when adding any IoMT device to the network, it is

necessary to be aware of the cybersecurity risks and measures necessary to ensure that the devices do not impair security. Starting one of the first steps to keep the healthcare environment digitally safe is to know which devices are connected to IoMT (updated inventory of connected devices), their locations, the type of data it generates, what it controls, and the networks it use to connect to communicate, including from sensors for medical equipment to devices and tablets used by employees (BAKER, XIANG, ATKINSON, 2017; HASSANIEN, DEY, BORRA, 2018).

Considering that for a digital security plan it is necessary to consider everything as basic as the definition of effective passwords, which is one of the best ways to prevent cyber attacks until having a broad view of all devices connected to the IoMT that share information, as well as the type of information transmitted, which may be different. Noting that not all devices have the same security measures and some devices are designed to be safer than others. These measures have an extremely important technological profile for the creation of a strong healthcare digital security system, as well as to ensure that everything is protected and all IoMT devices are updated with the latest security measures and protections (TAITSMAN, GRIMM, AGRAWAL, 2013; MANOGARAN, CHILAMKURTI, HSU, 2018).

Or the use of digital solutions such as the use of encryption, even for data collected and stored in the database of the internal network of the health institution. Or even considering that IoMT devices often depend on Cloud Computing services, it is necessary to know the requirements of the digital privacy policy of the cloud provider partner of the health institution and make sure that the encryption and protection features are offered necessary data. Or with respect to monitoring the external traffic of these IoMT devices, or even applying SSL certified (Secure Sockets Layer) devices consisting of a global standard security technology allowing encrypted communication between an Internet service (IoMT) and a web server, produced in the manufacturing process or added later to ensure the identity of the IoMT device and facilitate the digital authentication process (THAKUR, SINGH, GHRERA, ELHOSENY, 2019; DE SÁ, IANO, DE OLIVEIRA, PAJUELO, MONTEIRO, FRANÇA, 2019).

6 | DISCUSSION

The Internet of Medical Things (IoMT), represents the introduction of new applications of digital technology that promises to trigger the adoption and spread of precision medicine, representing a medical model that proposes the personalization of health care, with decisions, treatments, practices, medical tools or products for the benefit of the patient. These applications are demonstrating the difference made by the sensors and actuators that constitute the endpoints of the network, which allow to collect data and act on the data through analyzes, performing quite complex functions without human intervention. This also includes monitoring patients' health indicators and initiating corrective actions when these

indicators get out of control, representing not only saving a lot of effort on the part of doctors but most importantly, helping to care for and save lives in units emergency and intensive care.

The concept of IoMT over the years begins to materialize, referring to the adaptation and innovation of medical treatment to the individual characteristics of each patient. This does not literally mean the creation of medical devices exclusive to the patient, but the ability to classify, connect, generate data for analysis and integrate, patients in their susceptibility to a specific disease or condition, in the biology or in the prognosis of diseases that these patients may develop, or even in response to a specific treatment.

Preventive or therapeutic interventions through the intelligent analysis of data collected by IoMT devices can then be concentrated and administered in an assertive manner, saving costs and side effects for those who manage the criticality of patients. As also related that Artificial Intelligence (AI) represents a paradigm shift towards medicine, through machine learning algorithms used to analyze and extract inferences from the vast amounts of data collected by these IoMT devices from patients and healthcare institutions recorded at every moment, resulting in improving the quality of patient care, enabling cost-effectiveness and reducing readmission rates and even mortality rates.

With the advancement of technology, the speed of information, and connectivity, it became even more evident the need for transformation in the health sector, overcoming traditional processes, even effectively breaking paradigms in new solutions, cultures, work formats, and tools. Whereas IoMTA has been transforming communication, mobility, data analysis, negotiation, and health, in addition to people management itself. Alongside the algorithms and machines, fed by the collected data, AI is able to simulate the human ability to reason, make decisions and solve problems, analyzing that this increases the productivity and agility of a job or activity, relating the greatest current advances within this digital intelligence it happens in the perception and cognition of systems.

When it comes to IoMT, the “object” is always related to health, producing a constant flow of health data generated by the patient, such as a wheelchair, a heart rate monitor, or any other wearable health device, so these data can be used to assess the patient’s physical condition.

On a broader scale, data collection from treatment groups can also be used to support clinical studies and other advances, or even considering chronic diseases and data from ‘wearable’ sensors (IoMT) relating to the treatment of diseases such as diabetes type 2, obesity, hypertension, and smoking, among others. Since is considered that the management of these types of chronic diseases depends on significant changes in the patients’ lifestyle, such as exercise and diet, which occur outside of clinical control. Considering that these and other chronic diseases can also benefit from the use of this data collected by IoMT devices through monitoring the quality of life of patients using wearable

data as a way to obtain an accurate assessment of a patient's activity level, which is often a marker of your health.

Or even relating the level of digitization through innovations in healthcare units, such as IoMT devices and applications at the head of the hospital bed, decreasing the interaction with infected patients, which is very fundamental in times of pandemic such as COVID-19, which increases the team protection. Given the ability that IoMT technology provides to allow patient data to be remotely evaluated, reducing the obligation and duration of hospital consultations, or even with remote consultations in offices, remote diagnosis, and monitoring, significantly reducing the exposure of the most vulnerable members of society (such as the elderly and individuals with chronic illnesses) in a situation like the current pandemic of COVID-19.

Thus, it is possible to highlight the applicability of collecting medical data from patients through IoMT devices, whether through various types of sensors spread by the health institution or wearables, making the technology allow doctors and health professionals to be more assertive in their own health care for patients.

7 | TRENDS

Machine Learning (ML) is a technology composed of a set of mathematical tools, used to analyze data, with different techniques to evaluate and discover patterns in the information, search for answers to problems or find new solutions stored in the collected data volumes. It is important to note that the ML, especially aimed at exam analysis, increases the capacity of doctors, and does not replace the expertise of the human professional and his diagnostic capacity (which takes into account the overall assessment of the patient). This type of intelligent technology helps in the identification of patterns, and thus, doctors gain more time to dedicate themselves to each patient and will certainly be able to provide a more humanized and personalized service (FRANÇA, MONTEIRO, ARTHUR, IANO, 2021; FRANÇA, MONTEIRO, ARTHU, IANO, 2020; BEAM, KOHANE, 2018).

With ML it is possible to overcome adversities in the health area since many of them can be modeled as classic problems oriented on supervised learning and unsupervised learning. Classification is a supervised learning approach considering a pattern recognition problem from examples, since in medicine, for example, it is possible to use this from a large volume of chest X-ray exam data with and without collapses, allowing the algorithm to 'learn' the patterns of collapsed lungs and rely on them to classify new X-ray images. Clustering is an unsupervised learning approach related to a task that essentially consists of gathering more similar data for identifying groups. Whereas in medicine, for example, the creation of patient clusters based on their eating habits can reveal different groups and which diseases their members are developing (WORDEN, MANSON, 2007).

Blockchain technology has the potential to provide a reduction in the risk of compromising IoMT devices through a switch and improve the scalability of IoMT implementations. At first, Blockchain would allow the protection of IoMT networks in several ways, such as the formation of consensus groups on suspicious behavior, functioning in which each deletion or modification of data is recorded, even considering that as more blocks are placed, an even bigger chain of blocks is created. With IoT and blockchain working together, it is possible to achieve a verifiable and secure method for devices and processes associated with IoMT, since each transaction made is accompanied by a digital signature and can never be changed or deleted. Also highlights the decentralized nature of the technology, preventing a vulnerable device from "inserting or manipulating" false information (DE SÁ, IANO, DE OLIVEIRA, PAJUELO, MONTEIRO, FRANÇA, 2019; ANGRAAL, KRUMHOLZ, SCHULZ, 2017).

Digital transactions carried out on Blockchain by various sources can be managed through an immutable and transparent record, helping to reduce operating costs, since it eliminates intermediaries or intermediaries, given that data and physical goods are tracked across the supply chain. In the case of an erroneous decision or system overload, the blockchain registry must be able to identify the point at which something went wrong (ANGRAAL, KRUMHOLZ, SCHULZ, 2017).

8 | CONCLUSIONS

It is important to note that the absence of systems aggregating IoMT technology implanted in healthcare facilities reflects the novelty of the technology and also the significant existence of healthcare problems, also considering some of the real challenges dealt with by these new technologies. Even considering that despite the existence of technological problems, such as the effects of electromagnetic radiation and problems with the level of digital signal quality in hospitals, within hospitals, which may interfere with the transmission of collected data.

Still considering that any healthcare system must be digitally safe, considering the example of a particular hospital, it can implement a real-time tracking system employing barcode IoMT devices, Bluetooth transmitters, beacon systems, and code tags of bars on patients, nurses, and supplies, with properties to track workflows ("workflow"), analyzing that this quality should be incorporated into any specifications in this domain, considering a set of real implementation of IoT health systems addressing cybersecurity, digital privacy, and trust.

Another point that should be of great interest due to its complexity and importance is information security at IoMT, considering the large generation of confidential data about patients, consisting of great interest and attention from cybercriminals, a factor that increases

the number of cyberattacks in search of this information.

Still pondering the potential of IoMT to transform the shape of social and digital relationships, and even business, through data capture, as more and more billions of devices will be connected to the Internet and even the power of this digital ability to create your own data stream. Emphasizing that the idea of the ("basic") manual for capturing data from any type of transaction tends to be replaced, and the dynamics, ingestion in real-time and the application of information will dominate the future scenario.

However, about a large number of hospital and clinical environments have access to the internet via wired or Wi-Fi connection, consisting as one of the main challenges to be overcome in terms of the insertion of greater means of connectivity, even though despite the IoMT being in full growth, with the use still considered initial, the question of connectivity is essential since this allows IoMT devices to communicate, and increase the number of smart devices. Given the potential of IoMT to become a model in the effective use of technology (and innovation) both with regard to connected devices monitoring patients and disruptive immersion for the healthcare industry as existing and emerging technologies will enable the provision of healthcare services faster and more efficient patient care.

Thus, from the goal of saving lives to the management of medical records, powered by IoMT through the possibility of exploiting the computational power of smartphones, social networks, electronic medical devices, and data generation wearables. Considering that it is through sensors and other IoMT devices or even IoMT wearables, to really find the best treatments and cures for diseases, the data captured from patients by these IoMT technologies has to reach beyond a single patient, and become part of an aggregate, allowing medical researchers to access and analyze this medical data obtained.

ACKNOWLEDGMENTS

We thank the State University of Campinas – UNICAMP, Campinas, Brazil, and the Brazilian agencies CAPES and CNPq, which provided infrastructure and financial support to this research and publication.

REFERENCES

ADRYAN, B., OBERMAIER, D., & FREMANTLE, P. (2017). **The Technical Foundations of IoT.** Artech House.

BAKER, S. B., XIANG, W., & ATKINSON, I. (2017). **Internet of things for smart healthcare: Technologies, challenges, and opportunities**. IEEE Access, 5, 26521-26544

ALJEHANI, S. S., **Alhazmi**, R. A., **Aloufi**, S. S., **Aljehani**, B. D., & Abdulrahman, R. (2018, April). **iCare: Applying IoT Technology for Monitoring Alzheimer's Patients**. In 2018 1st International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-6). IEEE

ADENIYI, E. A., **Ogundokun**, R. O., & **Awotunde**, J. B. (2021). **IoMT-Based Wearable Body Sensors Network Healthcare Monitoring System**. In IoT in Healthcare and Ambient Assisted Living (pp. 103-121). Springer, Singapore.

ASHWINI, N., & **Vimala**, S. **A Survey on Autonomous RC Hospital Smart Bed for Accident Patients Using IoT.**

ALSUBAEI, F., **Abuhussein**, A., **Shandilya**, V., & **Shiva**, S. (2019). **IoMT-SAF: Internet of medical things security assessment framework**. Internet of Things, 8, 100123.

ALEXANDRE, R., & **Postolache**, O. (2018, September). **Wearable and IoT technologies application for physical rehabilitation.** In 2018 International Symposium in Sensing and Instrumentation in IoT Era (ISSI) (pp. 1-6). IEEE.

ABOUELMEHDI, K., **Beni-Hssane,** A., **Khaloufi**, H., & **Saadi**, M. (2017). **Big data security and privacy in healthcare: A Review**. Procedia Computer Science, 113, 73-80.

ANGRAAL, S., **Krumholz**, H. M., & **Schulz**, W. L. (2017). Blockchain **technology: applications in health care.** Circulation: Cardiovascular quality and outcomes, 10(9), e003800.

BALINSKI, P. A., **Bazar**, S., **Nesbitt**, P. A., **Olson**, J. T., **Patil**, S. R., & **Punadikar**, S. C. (2019). U.**S. Patent No. 10,226,632**. Washington, DC: U.S. Patent and Trademark Office.

BAIG, M. M., **GholamHosseini**, H., **Moqeem**, A. A., **Mirza**, F., & **Lindén**, M. (2017). **A systematic review of wearable patient monitoring systems–current challenges and opportunities for clinical adoption**. Journal of medical systems, 41(7), 115.

BEAM, A. L., & **Kohane**, I. S. (2018). **Big data and machine learning in health care.** Jama, 319(13), 1317-1318.

CHEN, L. G., **Ho**, Y. L., **Liu**, T. T., & **Lu**, S. S. (2017). **Internet of Medical Things: The Next PC (Personal Care) Era.** In Smart Sensors and Systems (pp. 265-333). Springer, Cham.

DE SÁ, L. A. R., Iano, Y., de **Oliveira**, G. G., **Pajuelo**, D., **Monteiro**, A. C. B., & **França**, R. P. (2019, October). **An Insight into Applications of Internet of Things Security from a Blockchain Perspective**. In Brazilian Technology Symposium (pp. 143-152). Springer, Cham.

DIN, I. U., **Almogren**, A., **Guizani**, M., & **Zuair**, M. (2019). **A decade of Internet of Things: Analysis in the light of healthcare applications**. IEEE Access, 7, 89967-89979.

DORSEY, E. R., MCCONNELL, M. V., SHAW, S. Y., TRISTER, A. D., & FRIEND, S. H. (2017). **The use of smartphones for health research**. Academic Medicine, 92(2), 157-160.

ESTRELA, V. V., **Monteiro**, A. C. B., **França**, R. P., **Iano**, Y., **Khelassi**, A., & **Razmjooy**, N. (2018). **Health 4.0: Applications, management, technologies and review**. Medical Technologies Journal, 2(4), 262-276.

FRANÇA, R. P., **Monteiro**, A. C. B., **Arthur**, R., & **Iano**, Y. (2020). **The evolution of robotic systems.** Safety, Security, and Reliability of Robotic Systems: Algorithms, Applications, and Technologies, 1.,

FRANÇA, R. P., MONTEIRO, A. C. B., ARTHUR, R., & IANO, Y. (2020). **An Overview of the Integration between Cloud Computing and Internet of Things (IoT)** Technologies. Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS), 1.

FRANÇA, R. P., **Monteiro**, A. C. B., Arthur, R., & Iano, Y. (2021). **An Overview of the Machine Learning Applied in Smart Cities. Smart Cities**: A Data Analytics Perspective, 91-111.

FRANÇA, R. P., MONTEIRO, A. C. B., ARTHUR, R., & IANO, Y. (2020). An **Overview of Internet of Things Technology Applied on Precision Agriculture Concept.** Precision Agriculture Technologies for Food Security and Sustainability, 47-70.

FRANÇA, R. P., **Monteiro**, A. C. B., **Arthur**, R., & **Iano**, Y. (2021). **The Fundamentals and Potential for Cybersecurity of Big Data in the Modern World**. In Machine Intelligence and Big Data Analytics for Cybersecurity Applications (pp. 51-73). Springer, Cham.

FRANÇA, R. P., **Monteiro**, A. C. B., **Arthur**, R., & **Iano**, Y. **An Overview of Narrowband Internet of Things (NB-IoT) in the Modern Era**. Principles and Applications of Narrowband Internet of Things (NBIoT), 26-45.

FRANÇA, R. P., **Monteiro**, A. C. B., **Arthur**, R., & **Iano**, Y. (2020). 9 **An Overview of the Internet of Things Technologies Focusing on Disaster Response**. Big Data Analytics in Supply Chain Management: Theory and Applications, 151.

FERRER-ROCA, O., & **Méndez**, D. G. (2012). **Health 4.0 in the i2i Era.** International Journal of Reliable and Quality E-Healthcare (IJRQEH), 1(1), 43-57.

FARAHANI, B., **Firouzi**, F., & **Chakrabarty**, K. (2020). **Healthcare IoT.** In Intelligent Internet of Things (pp. 515-545). Springer, Cham.

FUKUDA, K. (2020). **Science, technology and innovation ecosystem transformation toward society 5.0.** International Journal of Production Economics, 220, 107460.

GARG, V., & **Brewer**, J. (2011). **Telemedicine security: a systematic review**. Journal of diabetes science and technology, 5(3), 768-777.

HASSANIEN, A. E., DEY, N., & BORRA, S. (Eds.). (2018). **Medical Big Data and internet of medical things: Advances, challenges and applications**. CRC Press.

HUREIB, E. S., & **Gutub**, A. A. (2020). **Enhancing medical data security via combining elliptic curve cryptography and image steganography**. Int. J. Comput. Sci. Netw. Secur.(IJCSNS), 20(8), 1-8.

KSHIRSAGAR, P., **Pote**, A., **Paliwal**, K. K., **Hendre**, V., **Chippalkatti**, P., & **Dhabekar**, N. (2020). **A Review on IOT Based Health Care Monitoring System**. In ICCCE 2019 (pp. 95-100). Springer, Singapore.

LEE, C. H., & **Yoon**, H. J. (2017). **Medical big data: promise and challenges**. Kidney research and clinical practice, 36(1), 3.

LUNA-DELRISCO, M., **Palacio**, M. G., **Orozco**, C. A. A., **Moncada**, S. V., **Palacio**, L. G., **Montealegre**, J. J. Q., & **Diaz-Forero**, I. (2018, June). **Adoption of Internet of Medical Things (IoMT) as an opportunity for improving public health in Latin America**. In 2018 13th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-5). IEEE.

MARTIN-SANCHEZ, F., & **Verspoor**, K. (2014). **Big data in medicine is driving big changes**. Yearbook of medical informatics, 9(1), 14.

MAKRIS, L., **Argiriou**, N., & **Strintzis**, M. G. (1997). **Network and data security design for telemedicine applications. Medical Informatics**, 22(2), 133-142.

MANOGARAN, G., **Chilamkurti**, N., & **Hsu**, C. H. (2018). **Emerging trends, issues, and challenges in Internet of Medical Things and wireless networks**. Personal and Ubiquitous Computing, 22(5-6), 879-882.

NANDA, S., **Khattar**, K., & **Nanda**, S. (2019, February). **Internet of Things Based Remote Wearable Health Solutions: Prospects and Area of Research**. In Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.

NDIAYE, M., **Oyewobi**, S. S., **Abu-Mahfouz**, A. M., **Hancke**, G. P., **Kurien**, A. M., & **Djouani**, K. (2020). **IoT in the wake of COVID-19: A survey on contributions, challenges and evolution**. IEEE Access, 8, 186821-186839.

PARK, K. S., & **Choi**, S. H. (2019). **Smart technologies toward sleep monitoring at home**. Biomedical engineering letters, 9(1), 73-85.

PADILHA, R., **Iano**, Y., **Monteiro**, A. C. B., & **Arthur**, R. (2021). **An AWGN Channel Data Transmission Proposal Using Discrete Events for Cloud and Big Data Environments Using Metaheuristic Fundamentals**. In Metaheuristics and Optimization in Computer and Electrical Engineering (pp. 293-311). Springer, Cham.

SHABAN-NEJAD, A., **Michalowski**, M., & **Buckeridge**, D. L. (2018). **Health intelligence: how artificial intelligence transforms population and personalized health**

QURESHI, F., & **Krishnan**, S. (2018). **Wearable hardware design for the internet**

RISTEVSKI, B., & **Chen**, M. (2018). **Big data analytics in medicine and healthcare**. Journal of integrative bioinformatics, 15(3)

RODRIGUEZ-RODRIGUEZ, I., **Rodríguez**, J. V., **Elizondo-Moreno**, A., **Heras-González**, P., & **Gentili**, M. (2020). Towards a Holistic ICT Platform for Protecting Intimate Partner Violence Survivors Based on the IoT Paradigm. Symmetry, 12(1), 37.

SAHEB, T., & **Izadi**, L. (2019). **Paradigm of IoT big data analytics in the healthcare industry: A review of scientific literature and mapping of research trends.** Telematics and Informatics, 41, 70-85.

SHEHABAT, I. M., & AL-HUSSEIN, N. (2018). **Deploying internet of things in healthcare: Benefits, requirements, challenges and applications**. Journal of Communications, 13(10), 574-580.

SHIN, D., & HWANG, Y. (2017). **Integrated acceptance and sustainability evaluation of Internet of Medical Things**. Internet Research.

SINGH, R. P., **Javaid**, M., **Haleem**, A., & **Suman**, R. (2020). **Internet of things (IoT) applications to fight against COVID-19 pandemic**. Diabetes & Metabolic Syndrome: Clinical Research & Reviews.

TAITSMAN, J. K., **Grimm**, C. M., & **Agrawal**, S. (2013). **Protecting patient privacy and data security.** New England Journal of Medicine, 368(11), 977-979.

THAKUR, S., **Singh**, A. K., **Ghrera**, S. P., & Elhoseny, M. (2019). **Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications**. Multimedia tools and Applications, 78(3), 3457-3470.

TARDIEU, H., DALY, D., ESTEBAN-LAUZÁN, J., HALL, J., & MILLER, G. (2020). **Case Study 2: The Digital Transformation of Health Care**. In Deliberately Digital (pp. 237-244). Springer, Cham.

THUEMMLER, C., & **Bai**, C. (Eds.). (2017). **Health 4.0: How virtualization and big data are revolutionizing healthcare**. New York: Springer.

YACCHIREMA, D. C., **Sarabia-Jácome**, D., **Palau**, C. E., & **Esteve**, M. (2018). **A smart system for sleep monitoring by integrating IoT with big data analytics**. IEEE Access, 6, 35988-36001.

ZAMANIFAR, A. (2020). **Data analytics in IOT-based health care**. In Data Analytics in Biomedical Engineering and Healthcare (pp. 119-130). Academic Press.

ZHANG, J., & **Wu**, M. (2020). **Blockchain Use in IoT for Privacy-Preserving Anti-Pandemic Home Quarantine**. Electronics, 9(10), 1746.

WORDEN, K., & **Manson**, G. (2007). **The application of machine learning to structural health monitoring**. Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 365(1851), 515-537.

Engenharia Moderna: Soluções para Problemas da Sociedade e da Indústria 3

www.atenaeditora.com.br
contato@atenaeditora.com.br
@atenaeditora
www.facebook.com/atenaeditora.com.br

Atena Editora
Ano 2022

Engenharia Moderna: Soluções para Problemas da Sociedade e da Indústria 3

www.atenaeditora.com.br
contato@atenaeditora.com.br
@atenaeditora
www.facebook.com/atenaeditora.com.br

Atena Editora
Ano 2022