KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 9 (2023) 571–588

www.elsevier.com/locate/icte

Digitization of healthcare sector: A study on privacy and security concerns

Metty Paul[a], Leandros Maglaras[b,c,*], Mohamed Amine Ferrag[d], Iman Almomani[c,e]

[a] *Cyber Technology Institute, De Montfort University, Leicester, UK*
[b] *School of Computing at Edinburgh Napier University, Edinburgh, UK*
[c] *Prince Sultan University, Riyadh, Saudi Arabia*
[d] *Technology Innovation Institute, Abu Dhabi, United Arab Emirates*
[e] *The University of Jordan, Amman, Jordan*

Received 26 October 2022; received in revised form 31 January 2023; accepted 15 February 2023
Available online 21 February 2023

Abstract

The digital revolution has taken business sectors to a new height through the advancement of technology. The healthcare sector also embraced digital technology to facilitate technological change from mechanical and analogue electronic devices to the digital technology that is available today. The common use of digital technology in the healthcare sector includes searching medical knowledge resources, monitoring quality patient care and improving clinical support. The article presents the impact of technology in healthcare along with the privacy and security concerns related to technology use in healthcare.
© 2023 The Author(s). Published by Elsevier B.V. on behalf of The Korean Institute of Communications and Information Sciences. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

Keywords: Cybersecurity; Digitization; Healthcare; Privacy

Contents

* Corresponding author at: School of Computing at Edinburgh Napier University, Edinburgh, UK.
E-mail addresses: metty.paul@dmu.ac.uk (M. Paul), l.maglaras@napier.ac.uk (L. Maglaras), Mohamed.Ferrag@tii.ae (M.A. Ferrag), imomani@psu.edu.sa, i.momani@ju.edu.jo (I. Almomani).
Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2023.02.007
2405-9595/© 2023 The Author(s). Published by Elsevier B.V. on behalf of The Korean Institute of Communications and Information Sciences. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

The current trend that is reshaping the worldwide financial landscape and presenting opportunities for the development of new business models is the convergence of digitization and globalization. Businesses that embrace digitalization can rapidly expand their operations into foreign markets. As stated in [1], in recent years, international business people have given the phenomenon of early internationalization a greater amount of their attention than in previous years.

Due to the Internet, it is possible to live in a world where people are constantly in touch and can get quick answers to any question, no matter where they are. Any business communication, commercial or otherwise, must thus use the internet or other digital methods [1]. This encompasses informing customers and corporations about their data, products, and services and internal communication between organizations and customers. Because customers will always make inquiries online, a company that has embraced digitization can react more rapidly and efficiently to variations in client purchasing behavior worldwide. As per Tyrväinen et al. [2], the company's ability to adapt, pivot, or seek new industries depends on its digitalization status. This would raise or maintain sales.

Many internationally expanding enterprises faced the "globalization penalty" of rising complexity costs. In contrast, digital technology has made global growth cheaper for enterprises. Some multinational activities, like back-office processes or R&D, may now be localized thanks to digital solutions for remote collaboration and speedy communication [3]. Virtual global employees span boundaries, or a truly universal headquarters can be abandoned entirely. Digitization makes cheaper business ideas conceivable. Some companies prefer to focus their marketing and sales activities in a few locations rather than opening several offices abroad. All who sell digital goods do not require an overseas presence.

Digital transformation has changed organizations work style. Digitization can enhance production and revenue. This process can be called the 4.0 industrial revolution. Industry 4.0 has given all economic sectors new creative and growth potential. Companies are ready for the changing workplace. The authors in [4] state that rapid digital transformation scares and excites business owners. Research shows many digital conversions fail. Covid-19 wreaked worldwide chaos. According to [4], businesses sought ways to work remotely as internet access grew. Before the outbreak, office technology had evolved. Many companies use technology to enhance customer

service, offer flexible working, and speed up monotonous operations. Only 23% never use digital means (digital products and services). Innovation today requires digital technologies. Digitization is key to innovation. Digital innovation is also needed to solve difficult business concerns. Digital revolution creates new, ground-breaking commercial approaches

Over the years, the healthcare sector has integrated comprehensive, equitable and integrated models to facilitate the changes. Aiming for progressive improvement and prioritizing individual needs, the attempt to develop comprehensive healthcare began in the last decades [5]. Digitalization undoubtedly complemented the entire process. Along with effective clinical support and quality care, digital technology helps healthcare map and monitor the spread of infectious diseases and track vaccine and drug supply. Data integration has become a support act to ensure better application of digital technology in the healthcare sector [6]. Concerning this, the latest technologies such as blockchain, cloud and artificial intelligence (AI) and machine learning tools help the healthcare sector to identify and evaluate large volumes of patient data [7]. Digital technologies in healthcare create a profound effect on how health services are being delivered and how the entire health service runs. To do so, data management emerged as the main focus for digital healthcare.

By 2025, the digital health market is projected to reach 38 billion [8]. Based on this, the prospect and the current usage of digital technologies in healthcare can be understood. As of 2020, global funding for digital health was 13.9 billion which showcases the eagerness of the healthcare sector in implementing digital technologies in healthcare practices [8]. Mobile health (mHealth), health informatics, telehealth and electronic health (eHealth) are the creation of digital technologies. These facilities collect relevant and adequate patient data to analyze and generate significant insights to facilitate patient care. Electronic health collects and records patient data and medical treatment-related information to support clinical trials and offer large-scale observational data [9]. Healthcare data management is the compilation of patient data collected from various sources across organizations and providers.

Effective integration of healthcare data management allows caregivers to keep necessary patient information in a single database where it can be stored, evaluated and shared with the relevant stakeholders [10]. Moreover, by using healthcare data management, medical experts extract relevant insights to improve medical outcomes. At the same time, healthcare institutions are also committed to securing and protecting patient data privacy. Despite a valiant effort, the healthcare sector has failed to maintain data security and protect privacy effectively [11]. For that, medical data leak has become a common phenomenon in the healthcare sector. In addition, the healthcare sector also bears the highest costs due to data breaches which are more than three times of other industries. According to an IBM report, the average cost of healthcare data breaches is 7.1 million [12]. Based on this, the severity of data protection and security within the healthcare sector can be understood. Despite data protection and security-related challenges, a complete revamp in the healthcare sector through digitalization is expected.

1.1. Challenges

Digital technology adoption in healthcare bought several challenges out of which cybersecurity-related challenges happened to be the main concern. Cyber threats are extremely costly [13]. In healthcare, endpoint leakage, user authentication deficiencies and excessive user permissions are the main vulnerabilities. These three vulnerabilities are common and yet put healthcare at the risk of being compromised. On the other hand, the integration of the "Internet of Medical Things (IoMT)" has made data management systems more vulnerable [14]. IoMT devices pose threats in terms of compromising data security and privacy. This highlights the main issue of digitalization which are maintaining and ensuring patient data privacy and security-related concerns. Ransomware attacks are the most common cyber security issue in healthcare. An FBI report in 2021 revealed that the healthcare sector faced most ransomware attacks [15]. The FBI received 148 complaints in 2021 from the healthcare sector which is more than the financial sector even [15]. Software vulnerability exploitation, phishing attacks and remote desktop protocol (RDP) emerged to be the most common attack methods of ransomware in healthcare [15]. Based on this, the gravity of this can be understood.

Data privacy and protection are the fundamental rights of an individual [16]. Information collected by healthcare organizations often contains patients' personal details along with medical information and a data breach risks all that information being compromised which certainly hampers the overall purpose of digitalization within healthcare. Considering this aspect, the need for effective data protection in respect of the healthcare sector can be identified. Moreover, this also proves the relevance of this research and design guidelines for key considerations of the study. "Electronic health records (EHRs)" is a typical digital tool which allows patients to access necessary medical information as per their needs. Service providers can also share important patient data through "health information exchanges (HIEs)". However, this process comes with inherent data security risks. Patient records in EHRs contain details related to their medical history, social security number, treatment and insurance or payment information [9]. Access to the system is directly beneficial for cyber criminals or hackers. Therefore, gathering such information and presenting it as a compilation is expected to create significant awareness among relevant stakeholders within the healthcare sector which further justifies the study.

1.2. Importance of this research

The integration of digital technology in healthcare has been an advantage undoubtedly. Digital technologies through AI, machine learning and blockchain revamped the overall process of patient care. To do so, an adequate amount of relevant patient data collection has become necessary and that involves greater risks of data privacy maintenance. The healthcare sector happens to be the main victim of data breaches and security threats.

As per an FBI report, 148 organizations from the healthcare sector have complained about data breaches and cyber-attacks. Considering this, the importance of the study can be identified. Moreover, the report published by the FBI was of 2021, which makes it a contemporary issue and thus proves the relevance of the study. The main aim of this study is to investigate security and privacy-related concerns in the healthcare sector that appear due to digitalization. On the other hand, the significance of this study lies in determining different security and privacy threats that jeopardize patient data and the application of digital technology. Apart from that, the concerned study also recommends appropriate solutions to strengthen data security and protect privacy which makes the study worthy.

The contributions of this article are:

- Analyzes the impact of digital technologies in the healthcare sector
- Investigates security and privacy concerns of digitalization within the healthcare sector

Digitalization has become an integral part of industrial growth and the healthcare sector is no exception. By integrating digital technologies, the healthcare sector has improved service capacity, efficiency and overall performance [17]. The concerned study focuses on data security and privacy protection within the healthcare sector which is the most significant part of the entire digitalization process. Therefore, ensuring appropriate data protection can be identified as the main consideration before digital technology integration in any business sector. This research discusses the context and the need for digitalization in healthcare through which shortcomings in traditional healthcare can be identified. The significance of the research lies in highlighting various applications of digital technologies which offer an idea of how digitalization is impacting healthcare. In addition, the main theme of this study is to focus on specific challenges in maintaining data security and privacy. This certainly can help medical institutions and the overall healthcare sector to identify and become aware of potential data privacy and security-related issues. Moreover, the concerned research recommends various techniques and strategies to combat cyber-attacks and protect patient data. Considering this, healthcare organizations can take necessary and effective measures to prevent cyber-attacks and data breaches [18]. This study can be used as a compiled source of information related to digitalization in healthcare and conduct further research to improve patient care.

2. Digitization in healthcare

In this modern society, national borders are irrelevant because of cyberspace. Businesses across multiple industries have received new revenues and opportunities with the shift of their business models, incorporating the use of digital technologies. Therefore, with digitalization, businesses have reached new heights. Through healthcare digitalization, there is a change in the way of interacting with healthcare professionals, making quick decisions regarding treatment and outcomes and sharing medical data. Moreover, through mobile experience and integrated web, the primary goal of healthcare innovation is to optimize the work of medical professionals and medical software systems, improve patient outcomes, lower costs and minimize human errors [19].

Data integration in this sector enables the smooth exchange of electronic information and also helps in minimizing the expenses and issues of building interfaces between different systems. The incorporation of the “Internet of Medical Things (IoMT)” has increased the vulnerability of data management systems. These devices pose risks in terms of privacy and data security, which is one of the main issues of digitalization.

2.1. Digital technologies in the healthcare sector

Many medical advances have been and gone over millennia, and none has impacted digital technology. Networking and computer innovations have enhanced the spectrum of medical therapies and changed how doctors work [20]. The security objectives for the Healthcare sector are focused on protecting patient information, ensuring privacy and confidentiality, and maintaining the availability and integrity of healthcare systems, as presented in Table 1. Meeting these security objectives is essential to ensuring the safety and protection of patient information, and building trust in this growing technology. Table 2 presents the Digital technologies in the healthcare sector.

2.1.1. EHR

Electronic health record (EHR) devices and other technical assistance are becoming standard. EHRs improve doctors’ ability to obtain and share customers’ medical records, and computers and tablets are as common in hospitals as stethoscopes.

2.1.2. RPM

The use of remote patient monitoring (RPM) enables medical professionals to keep an eye on their patients even when they are not physically there. RPM has been shown to have positive effects on patient outcomes, as well as shorter reaction times and lower expenses over the long run. RPM is complementary to telemedicine because it lessens the burdens of travel on patients and protects them.

2.1.3. Artificial intelligence

AI is widely used in healthcare. In 2022, artificial intelligence in medicine will focus on using machine learning to analyze patient data (Herrmann et al. 2018). These algorithms replicate human reasoning to produce intelligent-looking systems.

2.1.4. Telemedicine

Telemedicine advanced during Covid-19. By 2020, 24 percent of health providers will use telehealth. Forrester anticipated Americans would have over a trillion virtual care sessions by year’s end. Many telemedicine regulatory restrictions have been eased as the business has matured, and healthcare facilities now have a year of information on evaluating and improving telehealth services.

Table 1
Security objectives for the healthcare sector.

Security objective	Description	Techniques
Confidentiality	Only authorized individuals such as healthcare providers and staff have access to patient information	Encryption and virtual private networks
Privacy	Prevent unauthorized access as well as protection against personal data breaches	Anonymization, pseudonymization, and encryption of data
Availability	Healthcare systems are always accessible to authorized users, even in the event of failures or attacks	Distributed storage systems, virtualization, and data backup and recovery systems
Integrity	Preventing unauthorized changes to patient information	
Authentication	Verifying the identity of users and accessing the Healthcare to prevent unauthorized access to patient information	Password-based authentication, Two-factor authentication, Biometric authentication (fingerprint, face recognition, iris scanning), Smart card authentication, Token-based authentication, Certificate-based authentication, and Public key infrastructure (PKI) authentication
Authorization	Controlling access to patient information based on a user's role and responsibilities within the healthcare organization	Role-Based Access Control (RBAC), Access Control Lists (ACLs), Token-based authentication, and Certificate-based authentication
Non-repudiation	Preventing individuals from denying actions taken within the healthcare organization, such as changes to patient information or access to sensitive data	Digital signatures and Blockchain

2.1.5. Federated learning

Federated learning provides a secure and privacy-protected way of sharing machine learning models across multiple devices in the Internet of Medical Things (IoMT). To take advantage of federated learning for IoMT, devices with sensors and other data-generating components must be linked to a central server. The server will then train a machine-learning model with data from these devices and send it back to each device for use. Predictions can be made using the model, while the data remains locally stored and safeguarded from data breaches. In this way, medical professionals can access the benefits of IoMT insights without putting patient privacy at risk. Furthermore, by combining data from multiple devices, federated learning can enhance the accuracy of predictions and lead to better results in the medical field.

Digital developments in multiple areas are causing massive shifts. Other fields have changed quicker than healthcare in recent years. The arrival of digital firms, payers' efforts to manage rising costs, and aging patients' desires for better care are all driving a digitized and real-value shift in health care. Digital transformation can speed up healthcare by reducing costs and improving services. Macroeconomic disruption can be facilitated, and business models improved. Established corporations might join with newer companies to reduce investment costs. The authors in [21] say well-established organizations' expertise with appropriate regulations could help startups disrupt the healthcare industry digitally.

Overall, digitalization could improve healthcare results and save costs. It is flexible and fast in handling large amounts of heterogeneous data. Its mining is only due to data warehouses and cloud-based data management technologies. Health IT still uses data warehouses. Big data can only produce so many insights without the right IT structure, tools, visualization methodologies, workflows, and user interfaces. Big data techniques must balance social advantages with patient privacy to create value in health care. Big data requires many changes to database use, accessing, sharing, privacy, or sustainability procedures and regulations.

2.2. Evolution of digitalization in business

Today, entrepreneurs are faced with one of the most common questions, which is, whether they should opt for a traditional business or a digital business. A traditional business usually sells its goods and services through retail outlets. These businesses include restaurants and everything that reflects an office setup. In contrast, a digital business is an advanced type of business. These businesses use technology to create value and improve the customer experience. In modern times, traditional businesses are also employing a digital strategy to optimize their workflow and organizational output for ultimate value creation for their customers. Digital technology is widely distributed across industries as it accelerates the development of products and services [22]. This is commonly referred to as digitization or digitization, which is the process of converting analog information into digitization products. This conversion is the driving force behind digitalization which is essentially changing the ways of manufacturing, distributing, and consuming products and services through these advanced technologies. Prevalent digital technology has altered global businesses. An increasing number of studies have been conducted to investigate the interconnections of businesses and digital technologies.

Digitalization affects almost all business activities in multiple industries and necessitates crucial changes in existing businesses [23]. Therefore, digitalization can be considered a critical strategic issue. However, many businesses face significant challenges in designing their digital strategies, especially, in a manner concerning the privacy and security of their customers.

Table 2
Digital technologies in the healthcare sector.

Technology	Description	Features	Platforms	Open Issues
Electronic Health Records (EHR)	Digital systems that store and manage patient health information	Secure sharing of information between healthcare providers	Modernizing medicine, Greenway health, GE centricity, and NextGen healthcare	Interoperability and data exchange between different systems
Medical imaging	Digital methods for visualizing and analyzing medical images	Integration with Electronic Health Records (EHRs) and remote monitoring	Cloud-based platforms, Mobile devices (smartphones, tablets), and Wearables (smartwatches)	Data privacy and security, interoperability, and the integration with existing healthcare infrastructure
Artificial intelligence	Machine learning to enhance health outcomes	Predictive analysis and early detection of potential health issues	Health applications and portals for patients and healthcare providers	Regulation and standardization of AI in medical applications
Blockchain	Technology for secure health data management through distributed ledgers	Eliminates the need for a central authority to manage the data	Ethereum, hyperledger, and corda	The decentralized characteristic of blockchain technology presents challenges in regulating data privacy, which is a significant issue in the healthcare sector
Telemedicine	Remote medical treatment through technology	Patients are able to track their essential vital signs, including blood pressure, heart rate, and oxygen levels, through the use of wearable devices	Telemedicine services can be accessed by both healthcare providers and patients through web-based portals	Guarantee the preservation of data privacy and security
mHealth	Mobile technology used for health monitoring, diagnosis, and treatment	Remote monitoring and data management and analysis	iOS, Android, and Web-based	mHealth raises concerns about the privacy and security of sensitive health information stored on mobile devices and in the cloud
Wearable Devices	Health-tracking devices worn on the body	Continuous monitoring of vital signs as well as health and fitness tracking	Apple WatchOS, Google Wear OS, and FitbitOS	Limited battery life as well as data privacy and security
Robotic process automation	Automation of routine tasks in healthcare	Real-time data processing and analysis	UiPath, Automation Anywhere, Blue Prism, WorkFusion	Data privacy and security concerns
Federated learning	Preserving data privacy and reducing communication costs	The model can be updated in real-time, as new data is collected from the devices	TensorFlow Federated (TFF), PySyft	The battery life of devices can be affected by the high energy consumption of federated learning

2.3. The approach of industry 4.0 and business intelligence

With the progression of the Internet, tech organizations were able to connect a large quantity of real-time data at lower costs [24]. These data are complex due to their size and even lack of structure. It is challenging for traditional software to process this data. Thus, new data analytics techniques are introduced in the markets to enable data mining, which sorts information to find patterns and relationships for better decision-making in the future. These advancements in digital technologies have been serving in improving the quality of products and services and accelerating the distribution processes.

Industry 4.0 is a set of technologies that businesses need to promote innovation strategies and respond quickly in volatile markets [25]. These technologies are aimed to enhance interconnectivity, predictive analytics, machine learning and digital technology to transform how businesses operate and develop. Some of these technological stools are Artificial Intelligence (AI), Internet of Things (IoT), cloud computing and Business Intelligence (BI). BI is a decision-making process aided by data integration and evaluation within an organization. This process, being the most valuable asset of a company, is becoming increasingly important in a variety of organizations as data is a vital resource for the development of businesses [25]. Since business environments are becoming more complex, organizations need modern and advanced technology to respond quickly in these volatile situations. In this perspective, technology tools such as BI are required for both data processing and sensible corporate decision-making. Besides customer data management, the implementation of technology tools in a company has several advantages like design and efficient data management.

Companies manage large amounts of decentralized data. However, with the advent of industry 4.0 and corporate evolution, it is fundamental to have a comprehensive, accessible, confidential and private database.

2.4. Bringing new opportunities to traditional management

According to a growing number of studies, digital entrepreneurship differs from traditional entrepreneurship and innovation in several ways, including not only the digitization of products and services but also how they are characterized and delivered, as well as how business models are implemented [22].

Advanced information systems have altered how managers approach planning and evaluating performance. Because of these advanced technologies, traditional management control ideas such as performance efficiency have changed in meaning [?]. It is difficult to find a clear and all-encompassing definition that captures the full scope of what managers do.

Management control encompasses all the techniques used to plan and supervise processes, such as cost calculations and budgets. From another perspective, it is about how environments are created to provide opportunities to achieve organizational goals. Again, management control is related to measuring performance in various forms including dimensions such as customer experience profitability, ability to change and efficient internal processes [?]. The digital organization provides a new scope for management control to operate. Unlike traditional management, it is not possible to discuss not only the capital required for a particular unit to achieve a particular goal but also the process of converting strategy into robust actions. Digitalization allows micro-management of critical resources and immediate correction of poor performance or deviations, in a few cases without even a management decision. However, increased digitization creates challenges that can disrupt and alter supply chains. Organizations are under rising pressure as a result of advancements in the field of sustainability and expanding digitalization [26]. Managers need to put fairness, social justice and equality at the center of their code of conduct to enable the employees to work together and create business sustainability and prosperity.

2.5. Role of digitalization in healthcare

Digital technology is critical to health care innovation as in other fields. However, digitalization in healthcare has multidimensional problems, and, therefore, it is still in its early stages [?]. Digitization of healthcare has introduced several tools and methods for improving healthcare services such as keeping the information about patients safely in one location and introducing software that makes health-related data more accessible to patients. The World Health Organization (WHO) conducts surveys regularly among countries to compile an inventory of the structural system and spread of healthcare digitization. Moreover, a report on digital healthcare innovation in France reveals that there is still a lack of innovation integration that has hindered the expansion of healthcare digitization. Scaling up is important when it comes to National Health Service (NHS) mobile health services as most of these services are confined to the pocket of adoptions and pilot studies.

Researchers noted that combining technologies into health care has both advantages and disadvantages. To its advantage, the new technology promotes innovative health services and administrative processes resulting in the reduction of healthcare expenses and improved efficiency of both internal and inter-hospital services [27]. On the contrary, the challenges include deeper comprehension of social barriers such as disagreements with hospital strategy and medical staff behavior. The major inherent technical threat includes information security risks.

2.6. Industry 4.0 in healthcare

As a part of industry 4.0, the healthcare industry uses modern technologies like AI, IoT, user response data, digitization, machine learning, human psychology, augmented reality (AR), big data mining, etc. [5]. These modern technologies aim to improve user comfort through proactive intervention in treating and detecting diseases. The sector is prepared to take a step forward toward industry 5.0, but there are a few challenges that prompted the review of this paper. Privacy and security concerns are one of the main aspects to be considered in the current research in the healthcare sector. Identifying the complexities regarding privacy and security concerns in healthcare will serve a major role in preparing the sector for an industry 5.0-ready.

Connecting objects, people and data yield insightful information in a variety of environments [28]. Real-time solutions are offered by several smart environments for a wide range of applications including healthcare, education, natural resource development, private and government organizational development and end-user data processing. Three major factors are regarded as the primary assets for developing a smart environment for solving various real-world problems. These are cost, accessibility and consumption of resources. Modern businesses that enter into industry 4.0 are eligible to provide several real-time solutions to multiple business and organizational issues.

Various digital projects have been developed around the world by integrating digital diagnostic systems that have significantly improved agility in MRI and X-ray investigations. This has further enabled clinical anamnesis and retrospective diagnosis of patients' health care data to provide timely feedback.

2.7. Role of IoMT in healthcare

IoT has resulted in a massive flow of data and services changing the authorization approach from a fixed desktop environment to interactive cloud environments [25]. This results in reduced organization and data-driven costs. During emergencies, healthcare providers can easily access the data and information about an individual/ a patient and speed up the treatment process. Due to the introduction of the internet of things (IoT), living in rural areas receive quality health care services which are done through data analytics and telemedicine.

To facilitate the changes, the healthcare industry has incorporated equitable, integrated, and comprehensive models over the years. Patient outcomes can be improved when individual

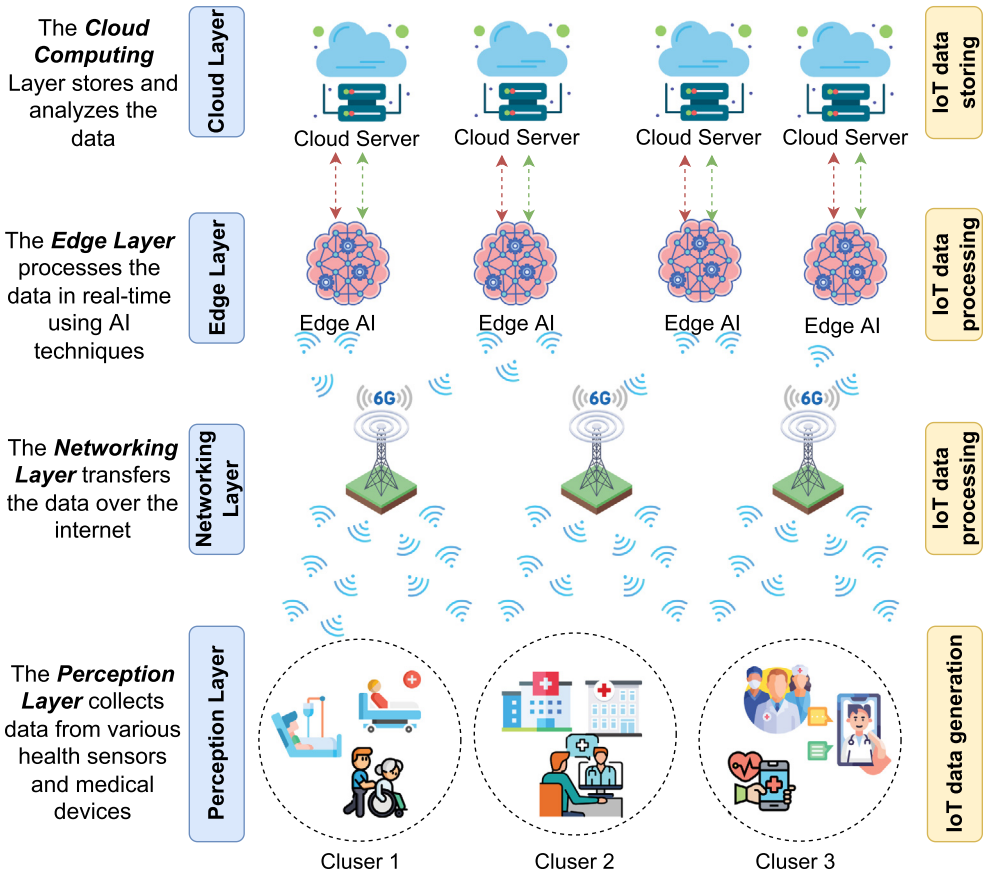

Fig. 1. Internet of Medical Things (IoMT) architecture. The architecture of IoMT is composed of four different layers that work together to allow for the integration of health data. The combination of these four layers creates a robust and scalable architecture that can provide healthcare providers with access to a vast amount of data that can be used to enhance the quality of healthcare services.

needs will be prioritized. Therefore, the incorporation of digital technology serves in comprehensive healthcare by focusing on individual needs. Multiple nations have used the IoMT in conjunction with other strategies to reduce the spread of the Covid-19 pandemic, increase efficiency by reducing the impact of the disease on human lives, improve the safety of front-line professionals and lower mortality rates [29]. Significant advantages have been made concerning the applications and technology as well as securities that have been amplified by the fast and extensive adoption of IoMT around the world. The number of studies regarding the implementation of security measures in the field of technology allows for the adoption of secure IoMT applications. Moreover, the advancement of new IoMT technologies that integrate with big data, AI, and blockchain provides more realistic solutions (see Table 3).

3. Internet of Medical Things (IoMT) architecture

The Internet of Medical Things (IoMT) refers to the utilization of interconnected medical gadgets, sensors, and wearable devices that are linked to the internet to gather, store, and evaluate data. The architecture of IoMT consists of four different layers that function together to make it possible for the integration of health data. These layers are the Perception Layer, Edge Layer, Networking Layer, and Cloud Computing Layer, as presented in Fig. 1. In this section, we will examine each layer in detail and how they contribute to the overall structure of IoMT.

3.1. Perception Layer

The Perception Layer is the first layer of the IoHT architecture, and it is responsible for gathering information from various health sensors and medical devices. This layer comprises different sensors, such as heart rate sensors, blood pressure monitors, and glucose detectors, attached to the user's body. The data obtained from these sensors is transmitted to the Edge Layer for processing.

3.2. Edge Layer

The Edge Layer is the second layer of the IoHT architecture and acts as a link between the Perception Layer and the Networking Layer. This layer handles the real-time processing of data collected from the sensors and converts it into a format that can be transmitted over the internet. The Edge Layer has been designed to be scalable and can handle the processing of large amounts of data.

Table 3
Comparison Between the Internet of Medical Things (IoMT) Devices.

IoT device categories	IoT device types	Features	(+) Advantages	(−) Open issues
Wearable Devices	Smartwatches, Fitness trackers, Heart rate monitors, Blood pressure monitors, Glucose monitors, ECG monitors, Respiratory rate monitors, Sleep trackers, Wearable patches, Smart clothing, Eye-tracking devices, Pain management devices, Medication reminders, Motion sensors, Clinical grade wearables.	The device keeps track of crucial health indicators like heart rate, blood pressure, sleep patterns, and physical activity and has the ability to immediately communicate with healthcare professionals.	The continuous monitoring of health parameters through wearable devices allows for real-time assessment of the wearer's health status. Personalized health recommendations, generated from individual data, result in a more tailored and effective approach to healthcare.	Wearable devices collect sensitive medical information, which means that there are concerns about the security and privacy of the collected data.
Smart Medical Devices	Smart blood glucose meters, Wearable ECG monitors, Wireless blood pressure monitors, Intelligent insulin pumps, Remote respiratory monitors, Smart body composition analyzers, Wireless spirometry devices, Telemedicine video consultation devices, Connected neurological monitors, Portable Ultrasound devices...etc.	This device has been created specifically for the medical field. It tracks different health metrics such as glucose levels, oxygen levels, and temperature. Additionally, it allows for real-time communication with healthcare providers.	Medical devices that are equipped with smart technology produce copious amounts of data that can enhance patient treatment and advance medical innovations. The utilization of these intelligent medical devices can minimize healthcare expenses by decreasing the frequency of hospitalization, trips to the emergency room, and physician consultations.	Possible technical difficulties that could arise with smart medical devices include software errors, device breakdowns, and connectivity issues.
Telemedicine Devices	Wearable fitness trackers, Smart blood pressure monitors, Digital stethoscopes, Telemedicine cameras, Remote patient monitoring devices, Telehealth thermometers, Wireless health monitors, Remote video consultation devices, Virtual reality medical devices, etc.	Patients are given the option to access medical care from the convenience of their homes through the use of video conferencing, remote monitoring technology, and mobile health applications.	Patients can receive medical care from the convenience of their own homes, eliminating the need for travel and reducing wait times in medical facilities. Through remote monitoring and tracking, healthcare providers are able to closely monitor a patient's health and respond quickly to any changes, resulting in better overall health outcomes.	The use of telemedicine technology and the associated data collection raises concerns about privacy and security due to the potential vulnerability of these devices to hacking and cyber-attacks.
Smart Home Devices	Smart blood pressure monitor, Smart body scale, Smart blood glucose monitor, Smart pill dispenser, Smart thermometer, Smart medication reminder, Smart ECG monitor, Smart oxygen monitor, Smart heart rate monitor, Smart insulin dispenser, ...etc.	Based on the integration of smart home technology, these devices can keep track of a patient's health and notify healthcare providers if there are any issues.	These devices can help individuals manage their health more effectively, leading to a better quality of life.	The use of Smart Home Devices raises security and privacy due to the potential vulnerability of these devices to hacking and cyber-attacks.

3.3. Networking Layer

The Networking Layer is the third layer of the IoHT architecture, and it is responsible for transmitting the data gathered from the Perception Layer to the Cloud Computing Layer. This layer consists of different networking protocols and technologies, such as Wi-Fi, Zigbee, and Bluetooth, that are used to transfer data over the internet. The Networking Layer is secure, reliable, and fast to ensure that the data transmitted from the Edge Layer to the Cloud Computing Layer is not lost or corrupted.

3.4. Cloud Computing Layer

The Cloud Computing Layer is the final layer of the IoHT architecture, and it is responsible for storing and analyzing the data collected from the Perception Layer. This layer is composed of various cloud computing services, such as Amazon Web Services (AWS) and Microsoft Azure, that are used to store and process data. The Cloud Computing Layer provides healthcare providers and researchers with access to a large amount of data that can be utilized to develop new treatments and therapies for various medical conditions.

Table 4
Security and privacy solutions for the healthcare sector.

Security framework	Year	Network model	Methods	Security models	Pros (+)	Cons (−)
Singh et al. [30]	2023	Internet of Things Smart Healthcare Financial System	Blockchain-based solution	Data privacy	+ The proposed system uses a blockchain-based zero-knowledge proof mechanism, which preserves the privacy of the users while sharing information between devices	− The scalability of the system may be limited due to the inherent characteristics of blockchain technology
Bhowmik et al. [31]	2023	Healthcare Internet of Things network	Data aggregation	Privacy-preserving	+ Reduces the communication and computational cost compared to conventional methods	− The lack of real-world implementation
Das et al. [32]	2023	Internet of Things-based smart healthcare	lightweight cryptographic primitives	Privacy-preserving	+ The security and performance analysis of the proposed authentication technique assesses its effectiveness over existing well-known schemes	− Reliability issues, limited accessibility, and high-cost communication
Wang et al. [33]	2023	Smart healthcare systems	Federated Learning	Privacy-preserving	+ FRESH effectively resists Source Inference Attacks (SIAs) by using certificates ring signature defense	− The proposed system is vulnerable to adversarial machine learning attacks
Ahmed and Kannan [34]	2022	Remote patient monitoring using IoT network	Elliptic Curve Cryptography-based solution	Privacy preserving	+ The proposed RPM system provides secure RFID based authentication, end-to-end secure communications, and privacy protection	− Reliability issues, limited accessibility, and high cost communication
Othman et al. [35]	2022	IoT-based healthcare	Homomorphic Encryption	Privacy-preserving	+ The proposed EPPADA scheme reduces energy consumption by eliminating redundant data through data aggregation	− The scheme involves the use of complex encryption and decryption methods
Chen et al. [36]	2022	Internet of Health Things	A Lightweight Authentication Protocol	Mutual authentication	+ The protocol incorporates authentication and key negotiation to guarantee the privacy and access control and uses biometrics to protect user anonymity	− The protocol involves the use of complex encryption and decryption methods
Yu et al. [37]	2022	Wireless Medical Sensor Network	Blockchain-based solution	Anonymity and Untraceability	+ The proposed scheme uses smart contracts and PUF which can provide security and decentralization	− The paper does not provide any information about the feasibility of the proposed scheme in real-world scenario
Kumar et al. [38]	2022	Internet of medical Things-based cloud-healthcare infrastructure	Elliptic curve cryptography	Patient anonymity	+ The comparison study shows that RAPCHI is more effective than other protocols	− The lack of real-world implementation
Wang et al. [39]	2022	Medical monitoring system based on RFID	Encryption operation based on cyclic shift and XOR operation	RFID security authentication	+ The use of RFID technology in the medical monitoring system ensures the security of medical records as well as protecting the privacy of patients.	- The resource constraint of RFID tags/readers presents a challenge in designing an efficient and effective authentication protocol

(*continued on next page*)

4. Internet of Medical Things (IoMT) devices

Table presents the comparison between the Internet of Medical Things (IoMT) Devices.

The Internet of Medical Things (IoMT) involves connecting healthcare technologies, systems, and devices to the internet to enhance patient care and health outcomes. With the rise of the

Table 4 (*continued*).

Security framework	Year	Network model	Methods	Security models	Pros (+)	Cons (−)
Ryu et al. [40]	2022	The network model consists of the registration center, telecare servers, and patients	Elliptic Curve Cryptography	Patient Anonymity	+ The protocol is resistant to an insider, privileged insider, and stolen mobile device attacks	− The protocol has high energy costs compared to existing protocols due to use of cryptography methods
Rahman et al. [41]	2020	Internet of Health Things	Federated Learning	Data privacy	+ Addresses privacy and security concerns through the use of federated learning (FL) and differential privacy (DP)	− Fully decentralized FL is a challenge due to lack of training capability at all federated node
Garg et al. [42]	2020	Internet of Medical Things	Blockchain-based solution	Anonymity and untraceability	+ The entire healthcare data is stored in a blockchain maintained by the cloud servers, making it secure and tamper-proof	− The protocol involves the use of complex encryption and decryption methods

Internet of Things (IoT) technology, IoMT has become more accessible and cost-effective, leading to a new era of healthcare services. IoT devices can be connected to the internet, facilitating real-time data collection, storage, and analysis. This section concentrates on IoT devices suitable for the Internet of Healthcare, their characteristics, and how they can enhance healthcare delivery.

4.1. Wearable devices

IoT wearable devices are designed to be worn on the body and include popular technology such as smartwatches, fitness trackers, and smart clothing. These devices have the capability to track various aspects of one's health, such as heart rate, blood pressure, sleep patterns, and physical activity. With the ability to communicate with healthcare providers, wearable devices enable real-time monitoring of patient's health. For instance, if the blood pressure levels monitored by a wearable device surpass the normal range, the device can alert healthcare providers to a potential health concern.

4.2. Smart medical devices

IoT-based medical devices, known as smart medical devices, are created with a specific purpose in mind — to provide medical support. They have the ability to track vital health indicators like glucose, oxygen and body temperature, and have a direct line of communication with healthcare professionals. This results in real-time monitoring of patients' health. As an example, a smart insulin pump can regulate insulin levels according to glucose readings, reducing the chances of both low and high blood sugar.

4.3. Telemedicine devices

Telemedicine is a type of IoT technology that enables individuals to receive medical treatment without leaving their homes. These gadgets encompass video conferencing tools, remote monitoring systems, and mobile health programs. Telemedicine can enhance access to healthcare services for people residing in remote or rural locations, minimizing the necessity of physical visits to the clinic. For instance, through video conferencing, patients can have consultations with healthcare professionals remotely, thus avoiding the need for travel and time away from work.

4.4. Smart home devices

IoT devices, known as smart home devices, are integrated into homes to enhance comfort, ease, and security. These devices encompass smart thermostats, lights, and locks, among others. Additionally, smart home devices have the potential to revolutionize healthcare delivery by keeping track of patient's health and notifying healthcare providers in the event of any abnormalities. For instance, a smart bed can track sleep patterns and send notifications to healthcare providers if there are any deviations from normal sleep patterns, indicating a possible health concern.

5. Security and privacy solutions for the healthcare sector

Table 4 presents the security and privacy solutions for the healthcare sector.

5.1. Mutual authentication solution

Chen et al. [36] designed a three-factor IoT-based protocol that aims to address the security issues frequently encountered in healthcare IoT systems. The protocol incorporates authentication and key negotiation to guarantee privacy and access control. The study also introduces the use of biometrics to protect the anonymity of users and improve user experience. The protocol uses asymmetric encryption and decryption for higher security and formal security analysis is performed to evaluate the security, soundness, and integrity of the session key and protocol. The study also conducts a comparative analysis of other protocols of the same type to evaluate the performance of the proposed protocol, which is found to exhibit a significant performance advantage in terms of computational cost, time efficiency, and security properties.

5.2. Authentication and key agreement solution

Based on the Blockchain and physically unclonable functions, Yu et al. [37] proposed a security scheme to ensure effective physical security, decentralization, data integrity, and transparency. It can prevent various security attacks, including "impersonation", "Session key disclosure", and "forgery" attacks, and guarantee "mutual authentication", "untraceability", and "anonymity". The scheme's security was evaluated using simulation and mathematical analysis, and testbed experiments were conducted using cryptographic primitives. A performance comparison analysis was also performed with existing schemes in terms of computation and communication costs and security functionalities.

5.3. Lightweight authentication solution

Kumar et al. [38] presented a new method called RAPCHI (Robust Authentication Protocol for IoMT-based CHI) to enhance the security and privacy of CHI (Connected Health Infrastructure) in IoMT (Internet of Medical Things) applications. RAPCHI establishes an authentication and key agreement between the patient, cloud server, and doctor, and forms a session key between the patient and doctor without storing data in a cloud database system. The proposed method is also resistant to various security threats and meets multiple security requirements. The paper includes formal security analyses of RAPCHI and a simulation of RAPCHI using the AVISPA tool. Additionally, a comparison study is conducted which shows that RAPCHI is more effective than other protocols in similar contexts, especially during a pandemic.

5.4. RFID security authentication solution

Wang et al. [39] examined the implementation of Radio Frequency Identification (RFID) technology in the field of smart healthcare and its effect on patient management, reducing medical service labor costs, and enhancing patient care. It also highlights the dangers of the inappropriate use of RFID tags and the potential harm to patient privacy and safety. To tackle this problem, the authors present CRUSAP, a highly efficient RFID security authentication protocol that leverages a cloud server and employs Bit-Crossing XOR rearrangement operations. The aim of CRUSAP is to improve security while minimizing resource usage by resisting attacks such as forgery, replay, desynchronization, and denial of service. The protocol has undergone formal validation and been proven safe and practical. Through security analysis and experimentation, the proposed protocol has demonstrated its ability to provide robust security at a lower cost.

5.5. Elliptic curve cryptography-based solution

Ryu et al. [40] examined the protocol by Sahoo et al. and determine that it is susceptible to insider and privileged insider attacks and fails to protect patient anonymity. To rectify these issues, they present a new protocol that incorporates biometrics and ECC to ensure secure communication in TMIS environments. The security of the new protocol is evaluated through the use of BAN logic, ROR model, and AVISPA, revealing its resistance to multiple security attacks, including insider and privileged insider attacks and stolen mobile device attacks, while also preserving patient anonymity. A comparison of computation costs, communication costs, and security features to existing protocols show that the new protocol is more efficient and provides better security. Ahmed and Kannan [34] explore the growth in ICTs and the possibilities of IoT applications across various industries, specifically in healthcare. IoT has the ability to enhance healthcare delivery through Remote Patient Monitoring using wearable technology and sensors. The RPM system suggested is secure and protects privacy, consisting of a MOTO 360 watch, a server, and a smartphone app to monitor health indicators. The evaluation found the proposed system has the potential to enhance the quality of life and healthcare services.

5.6. Federated learning-based solution

Rahman et al. [41] proposed the application of Internet of Health Things (IoHT) in health management and highlights the importance of secure data management to maintain privacy. To address the challenges of lack of training capability and trust management, the authors suggest a hybrid federated learning framework that incorporates blockchain smart contracts for the management of trust and authentication of federated nodes. The framework provides full encryption and anonymity of IoHT data through the use of DP. The efficacy of the framework was evaluated through deep learning applications for COVID-19 patients and demonstrated strong potential for secure and widespread adoption of IoHT-based health management. Wang et al. [33] proposed a smart healthcare framework for sharing physiological data, called FRESH, that uses Federated Learning (FL) and ring signature defense to protect against source inference attacks (SIAs). The framework collects physiological data from wearable devices and processes it using edge computing devices for local training of machine learning models. The model parameters are then uploaded to the central server for joint training. The ring signature is used to hide the source of parameter updates and reduce the success rate of SIAs. The proposed batch verification algorithm also improves the efficiency of signature verification. FRESH is suitable for large-scale smart healthcare systems involving many users.

5.7. Blockchain-based solution

Garg et al. [42] presented the BAKMP-IoMT, a blockchain-based protocol for secure authentication and key agreement in the Internet of Medical Things (IoMT) environment. IoMT connects medical devices and applications to healthcare systems through the Internet but leaves private health information vulnerable to tampering. BAKMP-IoMT ensures secure key management between implantable medical devices and servers and provides access to healthcare data stored in a blockchain

maintained by cloud servers. The protocol has undergone security verification using the AVISPA tool and has been shown to offer superior security and functionality compared to other schemes, with low communication and computational costs. The simulation results highlight the impact of BAKMP-IoMT on performance parameters. A decentralized healthcare finance system that uses blockchain technology and the non-interactive zero-knowledge proof is introduced by Singh et al. [30] to ensure privacy and security. This system is specifically created for resource-limited devices in IoT networks and minimizes communication costs through the use of lightweight cryptographic algorithms. The system is primarily intended for micro-level healthcare finance, but can easily be expanded to other financial systems. Additionally, it is highly efficient, lightweight, and can be audited, with transactions validated in just milliseconds.

5.8. Homomorphic encryption-based solution

Othman et al. [35] discuss the challenges of using the Internet of Things (IoT) in healthcare, specifically focusing on the issue of energy consumption and security. The use of multiple medical devices that transmit data wirelessly can cause high energy consumption and security issues. To address these challenges, the paper proposes the use of a privacy-preserving and efficient data aggregation scheme called EPPADA, which uses homomorphic encryption to protect healthcare data. The proposed system was experimentally developed using the E-health sensor shield platform and was found to improve end-to-end delay, computational cost, and communication overhead while maintaining security features.

5.9. Lightweight cryptographic primitives-based solution

Das et al. [32] introduced a privacy-preserving mutual authentication scheme aimed at overcoming the security and privacy challenges faced by IoT-based healthcare systems. The scheme utilizes efficient cryptographic methods such as XOR, concatenation, and hash operation, taking into account the processing limitations of IoT devices. The proposed scheme establishes a secure connection between authorized devices and a gateway, blocking any unauthorized access to the healthcare system. The results of the security and performance analysis demonstrate the superiority of the proposed scheme compared to existing authentication methods.

5.10. Data aggregation-based solution

Bhowmik et al. [31] presented a solution, called the Edge-enabled Efficient Privacy-Preserving Data Aggregation (EEPPDA), for securing health information in IoT-based smart healthcare systems. This solution employs homomorphic encryption to secure the medical data collected from patients, which is then aggregated on the edge server before being transmitted to the cloud server. This allows authorized medical professionals to validate, analyze and process the encrypted data. The EEPPDA scheme ensures the privacy of patients and their medical information, protects against any potential threats, and verifies the integrity of the data. Additionally, it greatly minimizes computational complexity and communication overhead compared to current methods.

6. Impact of digital technologies in the healthcare sector

With an increasing number of diseases and rising pressure on the health care sector around the globe, it is important to put more emphasis on person-centered care (PCC) encouraging individuals' participation in care delivery and self-care. Due to demographic changes, chronic diseases are growing in number [43]. This makes PCC a crucial part of chronic care. Because of the current pandemic situation caused by Covid-19, the entire society is responsible for finding advanced solutions to the pandemic. The Covid-19 pandemic has encouraged digital transitions in several sectors around the globe, especially, in the healthcare sector [44]. Healthcare organizations quickly adopted digital solutions and advanced technologies in response to the first phase of the pandemic.

The accessibility of health-related data has allowed patients to seek guidance easily from anywhere they need it and at their own convenient time. The pulse oximeter is a biosensor that measures the level of oxygen in the blood as well as the rate of heartbeat. It demonstrates the ability of the respiratory system to oxygenate the blood by displaying haemoglobin saturation [45]. The most recent low-cost models enable measurement recording and data transmission through standard connections. To quickly intervene in a condition where saturation worsened, monitoring paucisymptomatic patients at home during the current pandemic would be remarkably useful. Therefore, the introduction of such digital devices and software serves in aligning with the rising on-demand health care that has been observed especially after the Covid-19 pandemic.

6.1. Big data improving healthcare management

Big data analytics (BDA) has had a greater impact on healthcare organizations in recent decades [28]. Currently, clinical data is creating a huge impact in health care organizations by acting as a foundation to build multiple digital tools in this sector. Government and private enterprises are collaborating to carry forward this era of open information in healthcare as a decade of progress in digitizing medical records have already been observed. The federal government and other public stakeholders have enabled open access to decades of stored data to assist the health care sector in taking better actions [46]. However, protecting patient privacy is more important now as more data becomes public. Ensuring proper safeguards for the organizations that release personal information is essential.

The concept of evidence-based medicine has gained popularity among clinical stakeholders. In this system, decision-making is done for a specific treatment based on the best scientific evidence available. To get accurate information about a patient, huge data sets aggregate into big data algorithms which serve as the best source for evidence compared to data

sets of individuals with smaller data sets. Organizations that scale up faster in terms of BDA are supposed to achieve positive results faster as per reason studies (Groves et al. 2016). This is prompting other organizations to enter into the world of analytics since they do not want to be left behind. While preserving or improving the quality of services by the providers and pairs of BDA, they have to continuously improve healthcare values. There are multiple ways to instil value in this system such as by ensuring affordability of care and eliminating fraud abuse or waste in the system.

6.2. Using the EHR to build multiple Covid-19-specific tools

Electronic health records (EHRs) are computerized health records for patients that contain data relating to their past, present or future health conditions that recite in electronic systems used to collect, transfer, obtain, store, recover, connect and modify multimedia data for the ultimate goal of providing best health care and health-related services. Over several years, many different types of EHRs have been developed particularly since the millennium which recognize citizens to be responsible for their well-being and the data collection and storage of all their medical history [45]. This initiative allows the physicians to check patients' clinical parameters easily, allowing the practitioner to connect any alarming physical condition to recent medical records. Therefore, it allows the practices to shift the medical practices based on personal experience to one based on evidence. This enhances the communication between patients and physicians and improves the availability of personal medical data. New personal disease monitoring tools, for example, those that allow transmission, analysis of medical images and acquisition, assist physicians in personalized treatments [10].

The EHR can be used to build multiple Covid-19-specific tools for the management of a crisis. These tools include electronic check-ins, scripted triaging, secure messaging, standard ordering and documentation, telemedicine capabilities and real-time data analytics. The EHR collects data that are related to the environmental conditions of the patient, the socio-behavioral aspects and medical imaging. The advantages of such electronic devices include handling modern healthcare-related data and improving access to the previous medical history of a patient [10]. This has a positive impact on the speed of treatment as the reduction in the time lag of previous test results, recognizing and treating medical conditions is now more time efficient. The ultimate goal of healthcare organizations is to provide quality and quick medical services to patients. With digital technology like the EHR system, immediate public health surveillance is enabled, which provides relevant data about Individuals and ultimately enhances the quality of care. The complexity that big data brings in can be kept aside for a while to appreciate its potential to eliminate management delays and confusion. Proper planning is required for the correct implementation of advanced digital technology in the healthcare sector. However, digital records are critical to patients' survival.

7. Eliminating security and privacy concerns of digitalization within the healthcare sector

The pace of digital advancement in modern business is fast. It can be overwhelming for healthcare management to keep up with the digital transformation. In between incorporating and adopting the new digital technologies, there may be casualties concerning the privacy and security of the patients and other health care stakeholders. Management is essential in several industries but it is especially important in medicine because patient safety is of paramount importance [47]. Worldwide active research is going on to measure the security aspects of manufacturing medical devices and, hence, international standards are being designed for them.

7.1. Threats to the healthcare sector

The health care sector is an ideal target for medical information theft and it has been observed in the past that it lags behind other leading industries in safeguarding vital data [13]. This study focuses on privacy and security concerns in the healthcare industry as it is critical to invest money and time in ensuring and maintaining the security of advanced healthcare technology and the confidentiality of patient information from authorized access, given the increasing number of cyber-crimes in this tech-savvy era.

With the evolution of healthcare devices, the interconnectedness in the healthcare system has improved [48]. Interconnection has numerous advantages including increased efficiency, remote monitoring, automation and error reduction. These advantages are changing the way severe and chronic long-term conditions are treated. Outside the medical setting, interconnected technology enables proper monitoring and adjustment of implanted devices by health care professionals without the need for a hospital visit or medical interventions.

Due to the week security poster of healthcare management, is one of the easy targets around the world and poses greater cyber risks than other sectors. About 81% of 223 organizations surveyed in the United States (US) were targeted and over 110 million patients had their data jeopardized in 2015 alone [49]. Only half of the health care providers in the US believe that they were capable of safeguarding themselves again cyber-attacks despite a 300% rise in attacks over the last 3 years [49]. The two major reasons that make the health care industry an appealing target for cyber-attacks are its region in terms of information and being a soft target.

Till this point attacks on health care have primarily been motivated by monetary gain and political impact. However, in the future, cyber-attacks can be intentional or unintentional and might even cause damage by changing blood groups or test results. Another concerning possibility is harmful cyber-attacks on medical devices. More than 300 medical devices were classified as potentially dangerous in 2014. Patients adopting IoT technology, who have faced poor cyber security may become more reluctant to share information with clinicians and researchers which may further hinder the treatment process and cause a lack of accuracy and quality treatment.

7.2. Developing medical equipment management programs

The critical risk in detecting cyber-attacks is that several of them are undetected or unreported. Medical equipment management programs (MEMPs) are programs established and regulated by hospital biomedical engineering teams [47]. Concerning the privacy and security breaches caused by cyber-attacks on digital devices, MEMPs ensure the safety and trustworthiness of medical devices. Medical devices have been made in unison with rapid advancements in technology and are now embedded with data and communication technology. With the interconnection of such disparate technologies, however, security threats are constantly increasing both internal and externally. As a result, to minimize these threats from medical devices, critical systems must be identified and prioritized. Even though many MEMPs have been well designed an executed in healthcare organizations for more than 30 years, fewer investigations have been carried out effectively in providing an optimized idea considering cost, safety and reliability for service delivery of the medical equipment devices [50].

7.3. How are medical data stored in software like EHR?

To support the above observations, it can be said that EHRs have the potential to improve patient care by enabling health-related data widely available. However, cyber security is focused on safeguarding computer systems and data contained within them from intrusion and unintentional or harmful disruption [51]. Healthcare cyber security is insufficient and there have been growing concerns due to the lack of medical information confidentiality and information integrity. Physical objects like EHRs are distributed across several regions. As a result, unauthorized users can gain access to the platform and devices and damage all the information or may even program that device and extract security keys. Therefore, this research has been directed to raise a concern about the security and privacy risks of the digital technologies since the health care sector needs to improve a lot to fully avail the benefits of advanced technologies in providing quality care to patients.

8. Discussion

The creation of commercial value for users has been a major accomplishment of the IT sector over the past 50 years. Industrial automation was fueled by mainframes and PCs in the 1960s and 1970s, while business process automation was fueled by customer technology and the Internet in the 1980s and 1990s. Through the development of digital data platforms, technological advances in big data, cloud computing, mobile, and social networks since 2000 have expedited the digital transformation. The emergence of intelligent technologies like big data, machine learning, artificial intelligence (AI), and the Internet of Everything will make it possible to build an intelligent business.

Making unstructured data into semantically standardized, organized data sources requires smart, adaptable, adaptive medical extraction of information and high accuracy rule-based systems. Clinical data warehouses must be expanded into full-fledged knowledge discovery systems, depending on ontologies primarily for semantic reasoning techniques that result in hypothesis creation and knowledge discovery rather than simply for coding and code translation. Predictive analytics is crucial rather than straightforward analytical reporting. The ability to provide care must develop, and caregivers must learn how to train machine learning systems and mine clinical information (at least in part). Knowledge systems must also largely rely on ontologies, which classify illnesses or other medical concepts based on their similarities and differences and provide codification services. Right now, a lot of businesses are focusing on methods to save expenses. It can be thought that the best option for ensuring data management and security is to create and maintain on-premise copies of data and software. With cloud systems' compelling advantages, the situation may be different. Among the promise of cloud technology in healthcare include better patient data archiving and usage, lower storage costs, quicker innovation cycles, simpler collaboration, and increased telemedicine possibilities. With the four stages of digitization in mind, the adoption of cloud-based technology in healthcare will proceed at varying prices. As a result, several versions of the software will remain to be used; some on-premise and others within the cloud.

Big data processing with AI and ML offers extra potential for operational intelligence, streamlining company operations, enhancing patient care, and reducing costs. Recently, the FDA authorized an AI programme for diagnostic use.

Among the uses of machine learning are:

- Digital assistants and chatbots that will change how healthcare workers connect with patients and provide them more time to focus on difficult jobs
- Clinical decision support will play a key role in assisting healthcare workers in making decisions and in forecasting a variety of medical outcomes, including mortality, readmissions, and length of stay.
- ML-enabled NLP would advise a careful translation of texts to condense complex scientific language into understandable language.
- ML-enabled clinical information retrieval systems that offer high-quality knowledge from clinical narratives and learn from of the facility in which they are deployed
- Billing and invoicing that is automated and more precise will speed up the processing of claims and perhaps stop fraud.

8.1. Future works

8.1.1. Further research on privacy and security regulations in the healthcare sector

In the healthcare sector, privacy and security regulations are implemented to protect the sensitive personal information of patients. One method for achieving this is through the use of encryption technology, which ensures that any data transmitted or stored electronically is secure and cannot be accessed by unauthorized parties. Another method is through the use of access controls, which limit who can view or access patient information based on their role and

level of clearance. Additionally, healthcare providers are required to comply with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR), which outline specific guidelines for protecting patient privacy and data security. Overall, the healthcare sector employs a combination of technical and policy-based measures to ensure the privacy and security of patient information. A possible research direction in this topic could be related to studying the privacy and security regulations in the healthcare sector.

8.1.2. Study on the impact of digitization on patient outcomes

Digitization has had a significant impact on patient outcomes in healthcare. One method that has been used to measure this impact is through the use of electronic health records (EHRs). By digitizing patient information, healthcare providers are able to access a patient's medical history more easily and quickly, which can lead to more accurate diagnoses and better treatment plans. Another method is the use of telemedicine, which allows patients to consult with healthcare providers remotely, reducing the need for in-person visits and increasing access to care for patients in remote or underserved areas. Additionally, the use of big data and machine learning has allowed for improved analysis of large amounts of patient information, leading to the identification of patterns and trends that can inform the development of more effective treatments. Overall, digitization has the potential to improve patient outcomes by increasing the efficiency, accuracy, and accessibility of healthcare.

8.1.3. Investigation of privacy and security risks associated with wearable technology

There are several methods that can be used to investigate the privacy and security risks associated with wearable technology. One method is to conduct a thorough analysis of the device's software and hardware to identify any vulnerabilities that could be exploited by hackers. Another method is to use penetration testing techniques to simulate real-world attacks on the device to identify any weaknesses in its security measures. Additionally, researchers can conduct surveys and interviews with users of wearable technology to gain insight into their perceptions of privacy and security risks, and to identify any areas where additional education or awareness-raising may be needed. Overall, a multi-faceted approach that combines technical analysis, testing, and user feedback is essential for identifying and addressing the privacy and security risks associated with wearable technology.

8.1.4. Analysis of the role of artificial intelligence in healthcare

Natural language processing, which allows computers to understand and interpret human language, making it possible for doctors to input patient information and receive automated diagnoses or treatment recommendations. AI-powered chatbots and virtual assistants are also being utilized to provide patients with easy access to medical information and improve communication with healthcare providers. Additionally, AI-powered imaging analysis and diagnostic tools are being used to assist doctors with analyzing medical images and identifying potential health issues. Overall, the implementation of AI in healthcare has the potential to revolutionize the way medical services are delivered and improve patient outcomes.

8.1.5. Examination of the role of blockchain technology in healthcare

Blockchain technology has the potential to revolutionize the healthcare industry by providing secure, transparent, and decentralized methods for storing and sharing patient data. One method is through the use of electronic medical records (EMRs) on a blockchain platform, which allows for the secure and efficient sharing of patient information among healthcare providers. Another method is through the use of smart contracts, which can automate and streamline the process of claims and reimbursements for insurance companies and patients. Additionally, blockchain technology can also be used for supply chain management in the healthcare industry, ensuring the authenticity and traceability of drugs and medical devices. Overall, the implementation of blockchain technology in healthcare can greatly improve the efficiency and security of the industry, ultimately benefiting patients and healthcare providers.

8.1.6. Study on the role of patient engagement in privacy and security

Patient engagement plays a crucial role in privacy and security in the healthcare industry. By actively involving patients in the process of protecting their personal information and medical records, healthcare providers can ensure that patients are aware of their rights and responsibilities when it comes to protecting their privacy. This includes educating patients on the importance of keeping their personal information secure, as well as providing them with tools and resources to help them do so.

9. Conclusion

In order to update employment expectations and processes, digitalization demands modifications to healthcare practices, regulations, and activities. A review of the digitalization capabilities of healthcare professionals is necessary given the concerns about patient safety and incorporation of digitalization into the professional environment. It is becoming more widely acknowledged that in Developing Economies, digital health systems as well as other health information technology might more effectively replace the outdated, disjointed paper-based health record systems.

As a consequence, there has been an increase in the need from healthcare organizations to implement various types of digital technologies in order to streamline their procedures. The accessibility of more reliable, less expensive, and lower power equipment or software, expanded internet use and usage, and the rise of several highly publicized projects in most nations are some of the major factors that have contributed

to the rapid uptick in use of these technologies. It is anticipated that the adoption of these digital advances within the healthcare industry would result in considerable cost savings as well as increased efficacy and efficiency, especially given the short window for the provision of healthcare services. In poor nations, digital health systems have the potential to improve healthcare performance and make it easier to accomplish strategic objectives.

Despite the chances and advantages that digitalization offers the healthcare sector, its implementation is frequently hampered by context-specific difficulties that prevent success. If healthcare organizations wish to enhance their reaction to digitalization, they should both pay focus on the social atmosphere of a workplace and foster a good attitude. New technology deployment requires practical, organizational, and collaborative assistance. Some academics have suggested that not all computerized health care systems correspond to expectations, despite the tremendous potential benefits that healthcare digitalization offers. Researchers emphasized how the predicted advancements brought about by healthcare digitalization may not always manifest as anticipated.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors would like to thank the support of Prince Sultan University, Saudi Arabia for paying the Article Processing Charges (APC) of this publication.

References

[1] K.Y. Chau, M.H.S. Lam, M.L. Cheung, E.K.H. Tso, S.W. Flint, D.R. Broom, G. Tse, K.Y. Lee, Smart technology for healthcare: Exploring the antecedents of adoption intention of healthcare wearable technology, Health Psychol. Res. 7 (1) (2019).

[2] P. Tyrvainen, T. Kilpelainen, M. Jarvenpaa, Patterns and measures of digitalisation in business unit communication, Int. J. Bus. Inf. Syst. 1 (1–2) (2005) 199–219.

[3] J. Manyika, S. Lund, J. Bughin, Digital Globalization: The New Era Global Flows, Tech. rep., McKinsey Global Institute, 2016.

[4] A. Bereznoy, Multinational business in the era of global digital revolution, Mirovaia Ekon. Mezhdunarodnye Otnos. 62 (9) (2018) 5–17.

[5] V.V. Popov, E.V. Kudryavtseva, N. Kumar Katiyar, A. Shishkin, S.I. Stepanov, S. Goel, Industry 4.0 and digitalisation in healthcare, Materials 15 (6) (2022) 2140.

[6] D.K. Sharma, D.S. Chakravarthi, A.A. Shaikh, A.A.A. Ahmed, S. Jaiswal, M. Naved, The aspect of vast data management problem in healthcare sector and implementation of cloud computing technique, Mater. Today: Proc. (2021).

[7] F. Jiang, Y. Jiang, H. Zhi, Y. Dong, H. Li, S. Ma, Y. Wang, Q. Dong, H. Shen, Y. Wang, Artificial intelligence in healthcare: past, present and future, Stroke Vasc. Neurol. 2 (4) (2017).

[8] Digital health - statistics & facts, 2021, Online; accessed 7-October-2022, https://www.statista.com/topics/2409/digital-health/.

[9] M.R. Cowie, J.I. Blomster, L.H. Curtis, S. Duclaux, I. Ford, F. Fritz, S. Goldman, S. Janmohamed, J. Kreuzer, M. Leenay, et al., Electronic health records to facilitate clinical research, Clin. Res. Cardiol. 106 (1) (2017) 1–9.

[10] S.P. Dash, The impact of IoT in healthcare: global technological change & the roadmap to a networked architecture in India, J. Indian Inst. Sci. 100 (4) (2020) 773–785.

[11] K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, M. Saadi, Big data security and privacy in healthcare: A review, Procedia Comput. Sci. 113 (2017) 73–80.

[12] H. Landi, Average cost of healthcare data breach rises to 7.1 M, according to IBM report, Fierce Healthc. July 29 (2020).

[13] C.S. Kruse, B. Frederick, T. Jacobson, D.K. Monticone, Cybersecurity in healthcare: A systematic review of modern threats and trends, Technol. Health Care 25 (1) (2017) 1–10.

[14] N.S. Abouzakhar, A. Jones, O. Angelopoulou, Internet of things security: A review of risks and threats to healthcare sector, in: 2017 IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, 2017, pp. 373–378.

[15] I. FBI, Internet crime report 2021, 2021.

[16] M. Ventura, C.M. Coeli, Beyond privacy: The right to health information, personal data protection, and governance, Cadernos de Saude Publica 34 (2018).

[17] E.M. Kwiatkowska, M. Skórzewska-Amberg, Digitalisation of healthcare and the problem of digital exclusion, Cent. Eur. Manag. J. 27 (2019) 48–63.

[18] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, M.A. Ferrag, Cyber ranges and testbeds for education, training, and research, Appl. Sci. 11 (4) (2021) 1809.

[19] M. Evans, Y. He, L. Maglaras, I. Yevseyeva, H. Janicke, Evaluating information security core human error causes (IS-CHEC) technique in public sector and comparison with the private sector, Int. J. Med. Inform. 127 (2019) 109–119.

[20] M. Herrmann, P. Boehme, T. Mondritzki, J.P. Ehlers, S. Kavadias, H. Truebel, et al., Digital transformation and disruption of the health care sector: internet-based observational study, J. Med. Internet Res. 20 (3) (2018) e9498.

[21] J. Roski, G.W. Bo-Linn, T.A. Andrews, Creating value in health care through big data: opportunities and policy implications, Health Aff. 33 (7) (2014) 1115–1122.

[22] B. Chae, Mapping the evolution of digital business research: A bibliometric review, Sustainability 14 (12) (2022) 6990.

[23] A. Lipsmeier, A. Kühn, R. Joppen, R. Dumitrescu, Process for the development of a digital strategy, Proc. CIRP 88 (2020) 173–178.

[24] P. Barwise, L. Watkins, The evolution of digital dominance, in: Digital Dominance: The Power of Google, Amazon, Facebook, and Apple, Oxford University Press, 2018, pp. 21–49.

[25] C.A. Tavera Romero, J.H. Ortiz, O.I. Khalaf, A. Ríos Prado, Business intelligence: business evolution after industry 4.0, Sustainability 13 (18) (2021) 10026.

[26] B. Richter, J.H. Hanf, Cooperatives in the wine industry: Sustainable management practices and digitalisation, Sustainability 13 (10) (2021) 5543.

[27] M. Alloghani, D. Al-Jumeily, A. Hussain, A.J. Aljaaf, J. Mustafina, E. Petrov, Healthcare services innovations based on the state of the art technology trend industry 4.0, in: 2018 11th International Conference on Developments in ESystems Engineering (DeSE), IEEE, 2018, pp. 64–70.

[28] G. Manogaran, C. Thota, D. Lopez, R. Sundarasekar, Big data security intelligence for healthcare industry 4.0, in: Cybersecurity for Industry 4.0, Springer, 2017, pp. 103–126.

[29] A.H.M. Aman, W.H. Hassan, S. Sameen, Z.S. Attarbashi, M. Alizadeh, L.A. Latiff, Iomt amid COVID-19 pandemic: Application, architecture, technology, and security, J. Netw. Comput. Appl. 174 (2021) 102886.

[30] R. Singh, A.D. Dwivedi, G. Srivastava, P. Chatterjee, J.C.-W. Lin, A privacy preserving internet of things smart healthcare financial system, IEEE Internet Things J. (2023).

[31] T. Bhowmik, I. Banerjee, EEPPDA—Edge-enabled efficient privacy-preserving data aggregation in smart healthcare internet of things network, Int. J. Netw. Manag. (2023) e2216.

[32] S. Das, S. Namasudra, Lightweight and efficient privacy-preserving mutual authentication scheme to secure internet of things-based smart healthcare, Trans. Emerg. Telecommun. Technol. (2023) e4716.
[33] W. Wang, X. Li, X. Qiu, X. Zhang, J. Zhao, V. Brusic, A privacy preserving framework for federated learning in smart healthcare systems, Inf. Process. Manage. 60 (1) (2023) 103167.
[34] M.I. Ahmed, G. Kannan, Secure and lightweight privacy preserving internet of things integration for remote patient monitoring, J. King Saud Univ.-Comput. Inf. Sci. 34 (9) (2022) 6895–6908.
[35] S.B. Othman, F.A. Almalki, C. Chakraborty, H. Sakli, Privacy-preserving aware data aggregation for IoT-based healthcare with green computing technologies, Comput. Electr. Eng. 101 (2022) 108025.
[36] C.-M. Chen, Z. Chen, S. Kumari, M.-C. Lin, LAP-IoHT: A lightweight authentication protocol for the internet of health things, Sensors 22 (14) (2022) 5401.
[37] S. Yu, Y. Park, A robust authentication protocol for wireless medical sensor networks using blockchain and physically unclonable functions, IEEE Internet Things J. 9 (20) (2022) 20214–20228.
[38] V. Kumar, M.S. Mahmoud, A. Alkhayyat, J. Srinivas, M. Ahmad, A. Kumari, RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure, J. Supercomput. 78 (14) (2022) 16167–16196.
[39] X. Wang, K. Fan, K. Yang, X. Cheng, Q. Dong, H. Li, Y. Yang, A new RFID ultra-lightweight authentication protocol for medical privacy protection in smart living, Comput. Commun. 186 (2022) 121–132.
[40] J. Ryu, J. Oh, D. Kwon, S. Son, J. Lee, Y. Park, Y. Park, Secure ECC-based three-factor mutual authentication protocol for telecare medical information system, IEEE Access 10 (2022) 11511–11526.
[41] M.A. Rahman, M.S. Hossain, M.S. Islam, N.A. Alrajeh, G. Muhammad, Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach, IEEE Access 8 (2020) 205071–205087.
[42] N. Garg, M. Wazid, A.K. Das, D.P. Singh, J.J. Rodrigues, Y. Park, BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment, IEEE Access 8 (2020) 95956–95977.
[43] E. Granström, C. Wannheden, M. Brommels, H. Hvitfeldt, M.E. Nyström, Digital tools as promoters for person-centered care practices in chronic care? Healthcare professionals' experiences from rheumatology care, BMC Health Serv. Res. 20 (1) (2020) 1–15.
[44] D. Golinelli, E. Boetto, G. Carullo, A.G. Nuzzolese, M.P. Landini, M.P. Fantini, et al., Adoption of digital technologies in health care during the COVID-19 pandemic: systematic review of early scientific literature, J. Med. Internet Res. 22 (11) (2020) e22280.
[45] F. Girardi, G. De Gennaro, L. Colizzi, N. Convertini, Improving the healthcare effectiveness: The possible role of EHR, IoMT and blockchain, Electronics 9 (6) (2020) 884.
[46] P. Groves, B. Kayyali, D. Knott, S.V. Kuiken, The 'big data' revolution in healthcare: Accelerating value and innovation, 2016.
[47] D.-W. Kim, J.-Y. Choi, K.-H. Han, Medical device safety management using cybersecurity risk analysis, IEEE Access 8 (2020) 115370–115382.
[48] L. Coventry, D. Branley, Cybersecurity in healthcare: A narrative review of trends, threats and ways forward, Maturitas 113 (2018) 48–52.
[49] G. Martin, P. Martin, C. Hankin, A. Darzi, J. Kinross, Cybersecurity and healthcare: how safe are we? Bmj 358 (2017).
[50] H. Mahfoud, A. El Barkany, A. El Biyaali, Preventive maintenance optimization in healthcare domain: status of research and perspective, J. Qual. Reliab. Eng. 2016 (2016).
[51] A. Ahmim, M.A. Ferrag, L. Maglaras, M. Derdour, H. Janicke, A detailed analysis of using supervised machine learning for intrusion detection, in: Strategic Innovative Marketing and Tourism, Springer, 2020, pp. 629–639.