IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

CYBERSECURITY AND DATA PRIVACY IN WEARABLE HEALTH TECHNOLOGIES: EXAMINING THE SECURITY MEASURES AND PRIVACY CONCERNS ASSOCIATED WITH WEARABLE HEALTH DEVICES

VENKATESWARANAIDU KOLLURI

Sr. Software Engineer, Department of Information Technology

***ABSTRACT*—**The purpose of this paper is to assess the cybersecurity and data privacy in wearable health technologies. Wearable sensors measure and record data from physiological and biochemical systems, and they are used to transmit health data via mobile applications and web-based platforms to healthcare providers and health records stored in the cloud [1]. These digital tools, if used properly, could become a valuable aid to medicine decision making based on research evidence, could encourage better patient participation in changing health behavior and could soon lead to preventive strategies that are both timely and individualized. One of the innovative trends in wearable health technology is the application of portable or wearable medical devices for remote monitoring and chronic disease management. These technologies provide online data transmission of real-time health status between patients and healthcare givers at non-traditional clinical settings. While these technologies remain in their infancy, security and privacy concerns need to be taken into account so as to allow a wide adoption of health information systems by both health professionals and individuals. Health records also contain information on prescriptions, used for creating and selling fake IDs to obtain controlled substances; and specific details, such as diagnosis or lab results, which could potentially be used for blackmail or discrimination [1]. With the increase in amount and sensitivity of data being collected by wearable health technologies, this trend of targeting healthcare data is likely to shift towards the cloud servers and databases storing this information. Given the rate at which these technologies are being adopted, it is imperative that we think about proactively addressing these cybersecurity and privacy challenges, rather than waiting for a disastrous event to occur.

***Keywords*—** Healthcare, Cybersecurity, Data Privacy, Wearable Devices, Health Tech, Device Security, Privacy, Data Risks, Health Data Protection, Vulnerabilities, Encryption, Authentication, Regulatory Compliance, predictive analytics framework, data mining

I. INTRODUCTION

Wearable health technology is the integration and application of technology to monitor and manage health and wellbeing. The value of wearable health technologies in the prevention and management of health conditions cannot be overstated. Consumers are now able to monitor vital signs, symptoms, and signs enabling earlier and accurate diagnosis and management of conditions. They are able to access, understand, and use their health information to make informed decisions and participate in their health and wellbeing more than ever before. Consumers are able to share information with health professionals in real time irrespective of geographical location. This information can be used to tailor and deliver health services and treatment options in a way that is more convenient and cost-effective for consumers [1]. It also has the potential to enable an evidence-based approach to practice enabling policies and decisions to be based on a richer source of data and the impact of care and interventions to be measured.

With the adoption of wearable health technologies, the primary player is represented by supporting a whole health status and well-being. They offer an excellent opportunity to understand the role of daily routines and activities in health and happiness, and consequently in helping individuals set and attain life goals. This feature enables individuals and communities to have copious capabilities to make health decisions by a medium that is easy to use, available, and integrated with the modern lifestyles. An impeccably detailed and informative illustration of the organizational chart effectively visualizes the interconnectedness and interdependence of these three paramount goals, providing a profound roadmap for the understanding and unraveling of the essay's central ideas and concepts [3]. The indispensable Figure 1 serves as an illuminating guide, shedding light on the intricate web of connections that unite and harmonize these crucial objectives.

Cybersecurity is about protecting information systems, in particular, the data stored or transmitted from those systems. Most often, the aim is to secure data from unauthorized access or corruption, and wearable health devices are no exception. If we consider the data collected from these devices, it is often very personal, difficult, and sometimes impossible to reproduce, and it has a high value to attackers [3]. With the recent increase in ransomware attacks, it is not inconceivable to imagine a cybercriminal holding patient health data at ransom and forcing the patient to use the devices to their own benefit if they wish to recover the information. In extreme cases, some wearable health devices may be used connected to other medical systems for direct patient treatment. For instance, the use of Transcranial Direct Current Stimulation (tDCS) in treating depression is one illustration, where tDCS can only be given if the patient's own status is automatically detected and, based on the data gathered from previous health devices, thereby discouraging the unnecessary treatment [4]. Those systems under attack might have life-threatening consequences for the patients. One of the studies recently uncovered that St. Jude Medical's pacemakers and defibrillators possess vulnerabilities that could be used to drain power quickly or to deliver incorrect impulses. This led to St. Jude issuing an RF-enabled pacemaker firmware update which the US FDA had to approve. In order to force an automatic update of this nature, a 'man in the middle' attack could be simulated to sever the device's connection to St. Jude servers before sending it false information to make it seem that the update was not necessary. This would prevent access to the update without patient consent as per the device instructions for use, and with most devices receiving no update, there could be suspicion of device foul play. This highlights the far-reaching potential of cyber-attacks on health devices and the data they store.

II. RESEARCH PROBLEM

The main research problem in this study is to assess cybersecurity and data privacy in wearable health technologies. Despite the intentions of those developing and implementing wearable health technologies, recent history has shown that most data, particularly health data, is at risk for misuse or theft. The healthcare sector is already heavily targeted by hackers, as health records typically contain personal identification information (PII), which can be used for identity theft, and are worth ten times more than credit card numbers on the black market. There have seen many studies exploring the effectiveness of these devices in the monitoring and management of chronic disease [5]. However, there has been little investigation into the security and privacy considerations of wearable health devices, and the data that these devices generate. As the data from these devices is automatically generated and, in many cases, stored in the cloud, it is subject to a number of security and privacy concerns that have been explored in other areas of health information technology. For instance, in a recent paper, Chaudhry et al identified security and privacy as the two major barriers to the implementation of electronic health records. With wearable health devices effectively being another form of health records, it is likely that the same concerns will apply. Similarly, Wang et al has shown that there are a wide range of security and privacy concerns in the area of mhealth, and mobile health apps are likely to share similar functionalities with wearable health devices[5]. Given that the data from wearable health devices will be frequently uploaded to cloud-based services via smartphone apps, there is also the added security concerns surrounding the transmission of patient health data across different platforms.

III. LITERATURE REVIEW

A. Overview of Wearable Health Technologies

A current-era example of a wearable health technology for the early detection of an illness comes from Proteus Digital Health, a company which has developed an ingestible sensor. Combined with a wearable patch, this sensor can transmit information to a mobile device, alerting patients or healthcare providers of vital sign changes [6]. An application of real-time monitoring and delivery of medical information can be found with the many wearable ECG monitors with built-in mobile connectivity. Steps towards more advanced diseases are being made. Researchers at the University of Houston are currently developing a Bluetooth-enabled blood pressure monitoring device, with the hopes of producing automatic alerts during hypertensive crises to both the patient and their medical providers.

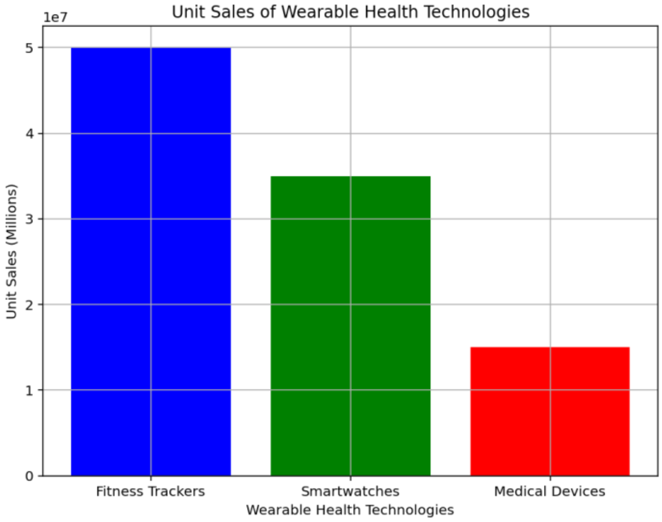

Fig. 1 Unit Sales of Wearable Health Technologies

Wearable devices have been used for the monitoring of fitness and health-related data. Spreading into wider horizons, an emerging group of health-centric wearable technologies, aimed at providing healthcare services, have begun to integrate with consumers' daily activities and lifestyles [6]. Wearable health technologies provide solutions for early detection of diseases, real-time monitoring of patient vital signs, and automated delivery of health-related information to healthcare providers. This could potentially lead to more optimal treatment and better prognosis for patients.

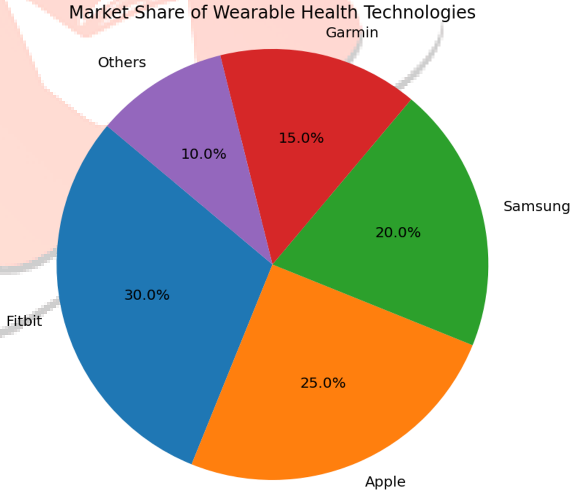

Fig. 2 Market Share of Wearable Health Technologies

B. Importance of Cybersecurity and Data Privacy

Cybersecurity and data protection are imperative when it comes to wearable health technologies. Information security and safety are significant in order to continue using these devices. Wearable health devices can save or transmit personal health data, which may include sensitive information about conditions or diagnoses. With the increasing trend of wearing sensors on or within the body, it is essential to ensure that the data collected and transmitted by these devices is only accessible to the appropriate individuals. Health information is valuable to both malicious hackers and various companies[7]. There is a possibility that data could be sold to third parties for marketing or other purposes, targeting individuals with specific medical conditions. Data integrity is also a concern, as any changes to the data could have a significant impact on an individual's health decisions or medical treatment. A study analyzing data security and privacy in 20 health-related apps and wearables found that none of them provided clear data encryption and transmission over the internet. This analysis also highlighted that most health apps share data with third parties. In mHealth ecosystems, which integrate data from various sources, it is difficult to track access and use of personal health data, making data control and monitoring security a challenging task. Failure to protect health information and data on these devices could have a damaging effect on patients.

C. Security Measures in Wearable Health Technologies

Security measures in the context of networked consumer devices have historically fallen victim to the tragedy of the commons: being under-invested in due to the collective agreement that individual contributions to security are not worth the costs, given that others will not invest. Given the critical nature of the data and the potentially life-altering implications of a cyber-attack on a wearable health device, it is important to break this mold. However, currently we are seeing little economic motivation to invest in security. In a highly competitive market, the priority for all firms is to enable rapid innovation and release new products ahead of their competitors. Security is seen as a non-function enabling the business rather than a feature to be added, and the prevailing attitude is that it can be bolted on to a product that is already developed, or worse yet: there is an enduring mindset to just cross fingers and hope that the product is not successful enough to attract an attack [7]. The latter case is a particularly dangerous gamble for devices storing health data given that very often security through obscurity is the only form of protection, and a high percentage of such devices will not be able to fly under the radar of an attacker that is specifically targeting data of this nature. This is essentially what the HIPAA Journal (2018) discovered through an analysis of the healthcare industry in the USA: "43% of healthcare organizations do not feel that they have sufficient budget to protect themselves against cyberattacks, and 48% of surveyed organizations said their security strategy for protecting patient data was ad-hoc [9].

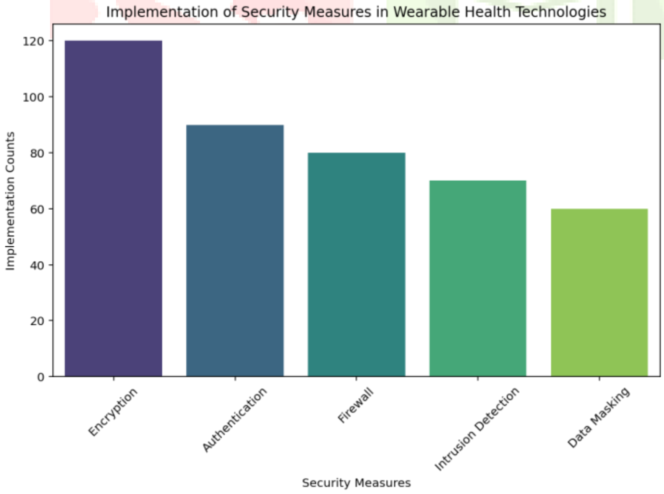

Fig. 3 Distribution of Security Measures in Wearable Health Technologies

D. Cybersecurity in Wearable Health Technologies

Risks and vulnerabilities continually threaten the security of sensitive health data transferred across less secure networks, and stored on devices and servers more prone to attacks than ever before. Wearable devices rely on wireless technologies to upload, access and transmit health data to and from health servers and other devices. Although wireless (both Wi-Fi and cellular) use is near ubiquitous, secure data transmission cannot be assumed [10]. Data leakage, transmission errors, and unauthorized access can all place the data's confidentiality and integrity at risk. In terms of data storage, health servers and cloud-based storage are susceptible to security breaches. By nature, wearable devices are intended for use outside of traditional clinical or home settings, expanding their reach and influence in the healthcare industry. Thus, data will be stored across a multitude of locations, varying from patients' smartphones to remote servers, adding complexity to the security landscape. Security measures for data stored on a wearable device can easily be compromised due to the limited computational resources available. These components are traditionally associated with the need of minimizing the level of power consumption, thus making it difficult to utilize advanced security protocols. This fact further requires engineering teams to take wearable technology into consideration while creating new approaches. Breaches of security for health data have far-reaching and serious effects. There is also a threat to public trust in e-health technologies which might decrease their adoption proportion thereby affecting the transitioning of healthcare from paper to digital [11]. Moreover, this also implies that shared data may become more vulnerable due to which clinical trials focused on wearable devices and other connected devices might face problems like data integrity and trustworthiness of the results. Consequently, strategic solutions of dealing with the key security issues should become the most important concern in the healthcare industry where protecting personal data and privacy is of the top priority.

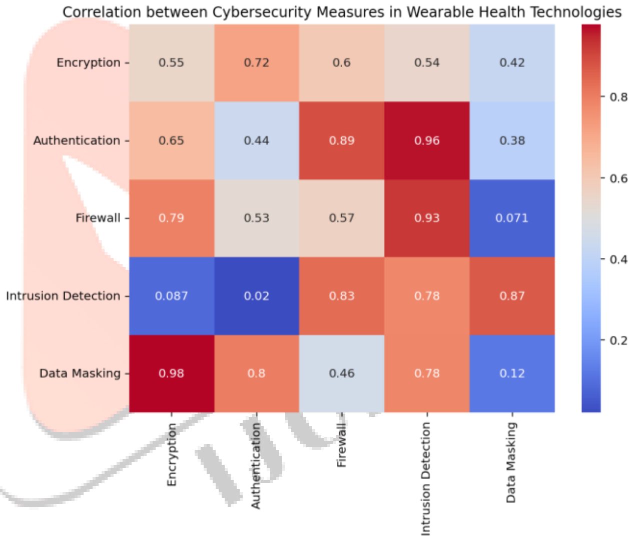

Fig. 3 Cybersecurity in Wearable Health Technologies

E. Privacy Concerns in Wearable Health Technologies

One of the primary concerns when it comes to health-related data is the danger of exposure to unauthorized access. Consequently, the implausible assets of wearable technologies for healthcare that have been repelled in Section 2 make the security data much more valuable. It would not be acceptable for any third party to have access to the personal medical records of a patient. Moreover, the data should be of solid quality if health providers are to act on this information [11]. Wearable health technologies generate a real-time data flow containing significant amounts of personal information which often is collected via the patient herself/himself. The protection of health data is of paramount importance and as such, it must be properly encrypted to ensure that it remains inaccessible to rogue actors. No one would want an unauthorized party to access their personal health information. Moreover, if health providers are to act on this information, it needs to be of sound quality. Wearable health technologies produce an ongoing stream of health-related data, much of which is in the form of subjective information from the user. If this data were to be altered in any way, it could be to the user's detriment. An extreme example of this would be if a data falsification resulted in a clinician making an incorrect decision with harmful effects to the user's health. Therefore, it needs to be ensured that stored data remains intact until such a time when it is no longer needed and securely transmitted to its storage destination.

In recent years, there has been a significant shift observed in the healthcare industry, with numerous healthcare organizations and patients embracing the use of wearable health technology. These technologically advanced devices offer unparalleled convenience in monitoring and tracking health-related data, and they seamlessly integrate with healthcare mobile apps [11]. The ability of these apps to effortlessly retrieve data from wearable devices and furnish patients with comprehensive analysis and reports regarding their well-being is truly remarkable. However, it is imperative to note that end users, who rely on these wearable devices and healthcare mobile apps, might not possess a thorough understanding of the intricate processes involving data collection, processing, and storage at the back-end servers.

The collected data during the operations are highly sensitive and confidential. This useful way of transmitting the information to third parties poses many serious risks and is harmful for the user. This type of health-related information is highly diverse since it accommodates plenty of data. Not only personal information but also critical health and fitness status updates are presented, too. Furthermore, any medical records an individual has received from anywhere are also included in this data set. With this comprehensive information, healthcare providers are able to tailor-make individualized and highly efficient treatment plans for each patient. Additionally, this data has pervasive implications that go beyond just health care services. The combined data derived from a great number of users may have important implications concerning medical research as well as health policy making [12]. This massive and inexhaustible source of information enables scientists and policymakers to have a thorough view of the general health trends and demography, thus enabling them craft unique interventions to the health problems that are predominant.

F. Impact of Cybersecurity Breaches in the Healthcare Industry

The impacts of a cybersecurity breach or other digital healthcare data incidents are well documented. In fact, a study in 1993 showed that 78% of hospitals had at least one data breach in the past two years. These impacts often result in vast financial costs, both direct and indirect, and potential harm caused to patients [12]. These costs are incurred in many ways. Some hospitals incur direct costs of hiring computer forensic experts to determine the extent of a cyber-attack or new staff to address security vulnerabilities. Other costs include potential legal action taken against a healthcare provider or insurer and the costs incurred from fixing the damage caused by the cyber-attack, for example from Ransomware, as was the case in an attack on Los Angeles Hollywood Presbyterian Medical Center. A 17-year-old youth arrested in July, suspected of launching the crippling cyberattacks on the UK's National Health Service, has been charged with securing and impairing the operation of a computer [12]. Further costs are incurred due to the loss of productivity during and after the cyber-attack, which, as shown by the 2017 global WannaCry ransomware incident, can be vast. In terms of the potential harm caused to patients, a cybersecurity breach has the possibility to directly impact patient health through altering healthcare data, and in some cases has led to loss of life. For example, in a cyber-attack on a German hospital in 2019, a patient happened to die while the hospital's IT systems were down [13]. Often these incidents lead to significant mental stress for patients, particularly in cases where their personal data is stolen.

G. Current Approaches to Addressing Cybersecurity and Data Privacy

Interconnected medical devices, such as wearable health technologies, present new challenges for ensuring cybersecurity and protecting privacy. The growing interest in exploiting the medical Internet of Things to aid diagnosis, monitoring, and treatment, and to manage healthcare operations is motivated by the belief that it will improve healthcare outcomes and efficiency [14]. Realizing the benefits of interconnected medical devices will depend on assurance of cybersecurity and preservation of privacy and trust. If the promise of these technologies is not realized due to security and privacy problems, the potential for benefits to healthcare will not be attained. Uncertainty about cybersecurity and privacy protection is a barrier to the adoption of medical IoT, so it is important to clarify the security and privacy issues and to identify approaches to addressing them. Unfortunately, for the sake of brevity, I will not be able to capture the considerable body of work on these issues and will instead focus on work relevant to wearable health technologies.

H. Current Approaches to Addressing Cybersecurity and Data Privacy

The lack of clear regulations and safety standards to govern data security and privacy is perceived as a major barrier for user adoption of m-health systems. Collaborative efforts are emerging between government, industry, and various user communities to define the nature and scope of security risks, develop and promote best practices, assess security solutions, and establish permanent monitoring systems for m-health security. Global in scale, these efforts are, however, at an early stage and currently show limited progress. Standardization of security protocols for mobile devices and network systems that take into account the specific challenges of health information is likely to be a lengthy process but will eventually be essential to ensure end-to-end security control[14]. The fast pace of development in mobile and wireless technology implies that m-health systems are highly dynamic with rapidly changing system and security component configurations. This exacerbates an already complex security situation where m-health applications must adapt to different local and national regulations for health information security and vary security controls according to patient or user preferences and special consent requirements [15]. The task is further complicated by the common reliance of mobile applications on third-party infrastructure and hosting. Widely varying application context and differing cultural perspectives on the use and disclosure of health information are important social and ethical considerations that must be factored into security system design. Security measures that are overly restrictive or culturally insensitive may result in rejection of the technology by users or loss of functionality. User stakeholders including patients, health consumers, and carers are often ill-equipped to participate in informed decision making about security requirements and assessing the trade-offs between security controls and system usability. This accentuates the need for clear and simple transparency mechanisms that inform users about security-related decisions and activities and involve them in ongoing management of the security lifecycle.

I. Case Studies of Cybersecurity Incidents in Wearable Health Technologies

Case studies in research are useful in learning the behavior of a certain case. In this essay, it's about cyber security incidents in wearable health technologies. Case studies in this section of the essay will give a clearer picture and example of what cyber security incidents are, the response from an organization that became a victim, the impacts, and efforts made to solve the problems. There are some incidents of cyber security on wearable technologies. One of the examples is an incident that happened to Medtronic Inc., a manufacturer of implantable cardiac devices and monitoring systems. In the end of the year 2008, Medtronic Inc. discovered that there are vulnerabilities in their systems that can be exploited by unauthorized access to the patient's personal information. Following this incident, Medtronic Inc. increased their spending to upgrade their system security by $21 million in the fiscal year ended in 2012 [16]. In the case of vulnerabilities to the patient's personal information, there are some impacts that might occur. Patient's personal information that leaked might be misused by irresponsible people for some advantages [16]. They can use the personal information to take some amount of expensive health care. The worst that might happen is to change the patient's personal information into another identity. This can cause the patient to get false accusations that they are changing their personal information. And the patient was totally unaware of this incident. In the next case, there's an incident of security breaches on the data of The American Recovery and Reinvestment Act that involves Pulse System Inc. Pulse System Inc. is a corporation that provides electronic health records, practice management, and revenue cycle management solutions. This incident happened in the spring of 2016, but it was reallocated in August 2018. During the data theft, Pulse System Inc. didn't give any official statement related to this incident and the impacts are unknown [17].

IV. SIGNIFICANCE AND BENEFITS

The significance of the research lies in its potential to drastically reshape and revolutionize the ways in which healthcare supply chains are managed in the United States. This facet's utmost relevant and remarkable contribution is the proposed work on learning and harnessing the power of advanced predictive algorithms to forecast and anticipate demand for crucial medical and surgical supplies. Startling evidence has emerged, suggesting that a staggering one third of the United States healthcare budget is currently being allocated towards supplies, and alarmingly, up to 40% of this expenditure may be attributed to wasteful spending practices [16,17]. By effectively and intelligently applying cutting-edge machine learning algorithms to extensive historical and transactional data, the envisioned outcome is nothing short of awe-inspiring: the creation and implementation of powerful decision support tools that will enable healthcare administrators to meticulously monitor and discern emerging trends in the utilization of supplies. This, in turn, will empower them to make more informed and precise forecasting decisions. The possible consequences of such progress are no doubt of great importance. The direct result from the decrease in both overstock and stockout incidents within hospitals and the stock suppliers will be the decrease in the associated costs for both parties [18]. This is as important as timely, considering the current economic challenges such as budgetary problems, fiscal issues, and capital restriction. Shifting to automation in the supply chain will reduce taxes, save on labor costs and bring in a host of other added benefits too. The most apparent benefit that emanates from this is that the levels of effectiveness of supply management are high which in turn translate into better healthcare for the patients. This injection of financial capital can enable healthcare institutions to spend on high-tech equipment, modern research, and experienced workers. Hence, the level of overall healthcare provision will improve which will also translate to better patient outcomes [18].

Moreover, cost cuttings that emerge from the impeccable supply chain management can also result in the reduction of financial dependencies as well as government institutions. Healthcare providers can alleviate the drain on public funds by creating a sustainable framework and minimizing waste so that the government entities can use the resources for something else more vital. This health insurance facility finances treatment and leads to the virtuous circle: the enhanced healthcare services develop the community and increase general well-being[19]. We can conclude that the prospects of this research research scale are extraordinary and utterly change-inducing. The healthcare supply chains can get transformed thanks to the leveraging machine learning and advanced data analytics, where the cycle can be changed into a seamless, efficient as well as cost-effective system. The promising fusion of technology and healthcare holds immense promise and intricately ties cost savings and improved patient care into a seamless tapestry of progress and transformation. Wearable devices use sensors to collect valuable information about the body and its well-being. Through this advanced technology, these devices are capable of measuring heart rate, counting the number of steps walked, monitoring skin temperature, and gathering various other vital data. The data collected by these wearable devices can then be effortlessly uploaded to a computer or smartphone for convenient access by health professionals [18]. Utilizing this data, health professionals can potentially recognize diseases at an earlier stage thereby prompting individuals to alter the unhealthy practices which they are prone to. Successful integration of wearable devices will forever make healthcare not only cheaper but also healthful for all the patients.

One of the major advantages of wearable devices for patients is the amount of freedom as well as the convenience it brings about. The constant monitoring capability makes people not suffer from regular sample tests or trips to hospital as before. Moreover, these devices allow them to follow up on their own health condition any time of the day and night, and furthermore, instantly deal with any health-related problems that show up. Moreover, patients can be observing and tracking their health data themselves, which allows them to be more informed and involved about their health. Such a high level of empowerment can improve the scale of a person's motivation to stick to a healthy lifestyle.

Additionally, wearable health devices are very helpful to older individuals in terms of ensuring that they maintain their independence, while they still keep a close watch on many health indicators [18]. For example, picture a future situation where a person diagnosed with heart disease could use a portable device to closely track their heart rate. The tool shall automatically review the patient health parameters and alert them once any abnormalities have been detected in order to take timely action. In critical cases, for example when an abnormally high or low heart rate is detected, the wearable device can warn an ambulance-based service or a designated family member so that help may be quickly provided and lives saved. Wearable devices, with their powerful sensors, have a potential to transform the entire healthcare landscape by continuously picking up and measuring some crucial body parameters. Besides, this data can be processed by health experts, permitting them to identify early signs of the disease and to encourage people to change their lifestyles for better health.

V. ENHANCEMENTS

The benefits to the United States healthcare system due to the introduction of smart, wearable technology are highly anticipated to take effect within the next five to ten years. These effects include a multitude of positive outcomes, such as significantly improving patient-disease management, empowering consumers with the necessary tools to effectively manage their own health, facilitating the much-needed shift from volume-based care to a more preventative approach, and serving as a key solution to address the challenges posed by an aging population [19]. Managing chronic diseases like diabetes, obesity, and heart disease have special significance for the USA being the most populous country with the most complications. The current spending on the above-mentioned prevalent diseases is a huge 75% of the $2 trillion dollars annually being spent on healthcare in the US today. Nevertheless, there is the possibility of wearable technology use to convert this procedure into a very easy, effective, and cost-saving task [20].

With the use of combined pocket and wrist-worn devices they will receive instant warnings when they approach critical levels of their condition. The alerts will encourage timely corrective steps and hence allow people to quickly restore a healthy range of their measures. More to that, these patient data will be safely sent to the healthcare professionals, thus allowing them for the detailed and thorough analysis of the patients' health status. This innovative strategy of controlling chronic diseases is anticipated to bring measurable financial results and is expected to amount to $1.3 trillion after twenty years. This significant input in turn is as a result of prevention of the complications and a subsequent reduction in the cost of treatment. There will be a drastic improvement in the quality of life for healthcare systems on the whole; this means, both, the patients and the healthcare providers will benefit in the current system monetarily. The universal utilization of smart, wearable devices will result in a system of greater efficiency, effectiveness, and patient-focus, guaranteeing a population with better health outcomes in the US.

VI. CONCLUSION

The purpose of this study was to dive deep into cyber security and data privacy issues related to wearable technologies in healthcare. The outcomes of the study create awareness on the utilization of wearable technologies in healthcare both by the patients and the healthcare providers with an aim of changing how healthcare is now being administered. Wearable technology has the potential to revolutionize the entire landscape of the US healthcare system. By leveraging these advanced technological solutions, the nation can significantly enhance patient-disease management, empower individuals to take control of their own health, shift the focus towards preventative medicine, and effectively address the challenges associated with an aging population. The substantial benefits and returns on investment projected in this field make it clear that the integration of wearable technology is an essential step towards a healthier and more sustainable future for the United States.Cyber attacks on health care wearable technologies can threaten the data integrity, confidentiality and availability. Both direct and indirect implications of these attacks on the patient and healthcare providers were discussed showing the importance of having good security measures to protect the devices. There should be a shared responsibility in security between provider and consumer,while the cloud service providers should ensure consumers that their data is safe. The privacy issue is also a serious issue as it involves the leaking of personal health info of an individual which will greatly affect the reputation of the patient himself and also health professionals. Measures that can be taken to protect the privacy of the patient were tabulated along with the level of security in implementing these methods. The issue of the HIPAA where it doesn't clearly state the method of privacy protection for patients' health info that's stored in electronic form was also discussed. The awareness on the importance of data security and privacy on health care wearable technologies will be known to the public and also to the developers of these devices in order to provide better protection on the personal health info of an individual.

REFERENCES

[1] R. Tong, *Wearable technology in medicine and health care*. London: Academic Press is an imprint of Elsevier, 2018.

[2] S. P. Murphy, *Healthcare information security and privacy*. New York: Mcgraw-Hill Education, 2015.

[3] E. Shahbazian and G. Rogova, *Meeting security challenges through data analytics and decision support*. Amsterdam, Netherlands: IOS Press, 2016.

[4] Y. Maleh, M. Shojafar, Mamoun Alazab, and Youssef Baddi, *Machine Intelligence and Big Data Analytics for Cybersecurity Applications*. Springer Nature, 2020.

[5] C. Chakraborty, *Smart Medical Data Sensing and IoT Systems Design in Healthcare*. IGI Global, 2019.

[6] N. Dey, A. Ashour, S. Fong, and C. M. Bhatt, *Wearable and implantable medical devices : applications and challenges*. London, United Kingdom ; San Diego, Ca: Academic Press, An Imprint Of Elsevier, 2020.

[7] J. Chaki, N. Dey, and D. De, *Smart Biosensors in Medical Care*. Academic Press, 2020.

[8] D. S. Herrmann, *Complete guide to security and privacy metrics : measuring regulatory compliance, operational resilience, and ROI*. Boca Raton: Auerbach Publications, 2007.

[9] S. P. Murphy, *Hcispp Healthcare Information Security And Privacy Practitioner All-In-One Exam Guide*. S.L.: Mcgraw-Hill Education, 2020.

[10] A. Armoni, *Healthcare information systems*. Hershey, Pa.: Idea Group Publ, 2000.

[11] P. A. Patrick, L. A. Ponemon, and Hcpro (Firm, *The complete guide to healthcare privacy and information security governance*. Danvers, Ma: Hcpro, 2014.

[12] B. Rosenberg, *RFID : applications, security, and privacy*. Upper Saddle River, Nj: Addison-Wesley, 2006.

[13] F. Xhafa, *Advanced Technological Solutions for E-Health and Dementia Patient Monitoring*. IGI Global, 2015.

[14] N. R. Silton, *Recent advances in assistive technologies to support children with developmental disorders*. Hershey, PA: Medical Information Science Reference, an imprint of IGI Global, 2015.

[15] C.-M. Kyung and Springerlink (Online Service, *Smart Sensors for Health and Environment Monitoring*. Dordrecht: Springer Netherlands, 2015.

[16] M. K. Watfa, *E-Healthcare Systems and Wireless Communications: Current and Future Challenges*. IGI Global, 2011.

[17] M. J. Mcgrath and Cliodhna Ní Scanaill, *Sensor Technologies Healthcare, Wellness, and Environmental Applications*. Berkeley, Ca Apress, 2013.

[18] H. Rivas, K. Wac, and Springerlink (Online Service, *Digital Health : Scaling Healthcare to the World*. Cham: Springer International Publishing, 2018.

[19] B. Fong, A C M Fong, and Chi Kwong Li, *Telemedicine technologies : information technologies in medicine and digital health*. Hoboken, Nj Wiley, 2020.

[20] I. P. Carrascosa, H. K. Kalutarage, and Y. Huang, *Data analytics and decision support for cybersecurity : trends, methodologies and applications*. Cham: Springer International Publishing, 2017.

[21] J. Pagaan, M. Mokhtari, H. Aloulou, B. Abdulrazak, M. F. Cabrera, and Springerlink (Online Service, *How AI Impacts Urban Living and Public Health : 17th International Conference, ICOST 2019, New York City, NY, USA, October 14-16, 2019, Proceedings*. Cham: Springer International Publishing, 2019.

.

.