NETWORKS, TECHNOLOGY, SECURITY, AND APPLICATIONS IN THE HEALTH SECTOR FOR IOT ENABLED SMART WEARABLE: A REVIEW

Abstract

With the advent of technology there is a lot of research work happening in the domain of Internet of Things(IoT) as it directly influences the common persons day to day life. This research work brings out several related works together with the relevance on technology, security, networking in IoT and its applications. The recent advancements which are influencing the wearable's and the way they are dealt with modern technology is also reviewed here. The technologies which are existing will have to deal with multiple issues when collecting data, processing, analyzing and contemplating the data are also summed here.

Keywords : Wearables, IoT, Security, Healthcare, Artificial Intelligence

Authors

Varalakshmi B D
Department of Computer Science and Engineering
Acharya Institute of Technology
Bangalore, India
varalakshmi@acharya.ac.in

Nagapushpa K P
Department of Electronics and Communication Engineering
Acharya Institute of Technology
Bangalore, India
nagapushpa@acharya.ac.in

Mallamma C G
Department of Computer Science and Engineering
Sambhram Institute of Technology
Bangalore, India
mallammagoudar79@gmail.com

Aruna M
Department of Electrical and Electronics Engineering
Nitte Meenakshi Institute of Technology Bangalore, India
aruna@nitte.ac.in

I. INTRODUCTION

An intelligent wearable collects data from the user and analyzes it, and in some cases, it can make intelligent judgments and respond to the wearer in a timely manner. Internet of Things based wearable devices are classified into four key groups in this paper: (i) Networks (ii) Technology (iii) Security (iv) Applications. Data are gathered for these topics within each cluster, and they are reviewed and analyzed in detail.

The paper is organized as below, in Section II provides an overview of the Networks in wearable supported by IOT. Sections III Wearable device technology, Section IV discusses Security in IoT wearables for healthcare, Section V focuses on applications of IoT related variables. Finally, the conclusion explains how when all these four aspects are put together the wearables in IOT become more effective and improves the quality of life of the people who are using it and also the people who are moderating it.

Despite the fact that mobile IoT offers numerous benefits and can significantly improve the functionality of IoT wearables, it has not been used effectively so far, according to the analysis that was conducted. [1] A comprehensive analysis of the chosen topic was performed by examining a variety of sources including IEEE Xplore and the digital library of the Association for Computing Machinery (ACM). There is a need for constructing a classification system for smart wearables, networks, and applications encompassing the Internet of Things as depicted in Figure 1.

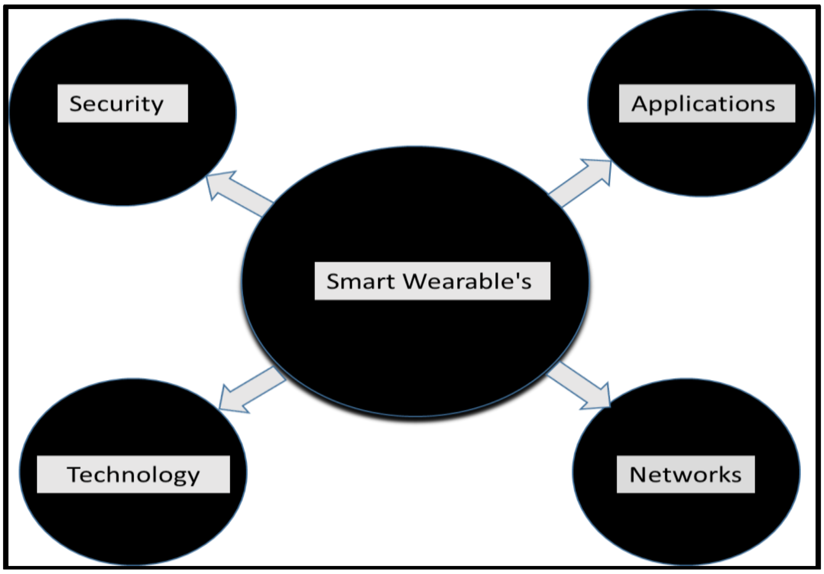

Figure 1: Different clusters in IOT and its applications.

II. NETWORKS

The study conducted by [9] presents a Health Monitoring Observer Network for monitoring the health of a patient via IoT and wearable devices. The architecture is motivated by the Forest Fire Observer Network and is made up of three layers. As the first layer, the sensor layer measures vital signs from the patient, and it is connected to the network modules so that it can share the information of the patient with the underlying network. Data from sensors is grouped into a common group by the second layer, which combines values and data from sensors. [9] The next layer is the analytical layer, which holds software and techniques for problem detection. Furthermore, in addition to these layers, the study recommends a supplementary layer that extends across all the layers of the architecture in a cost-effective manner. [9]

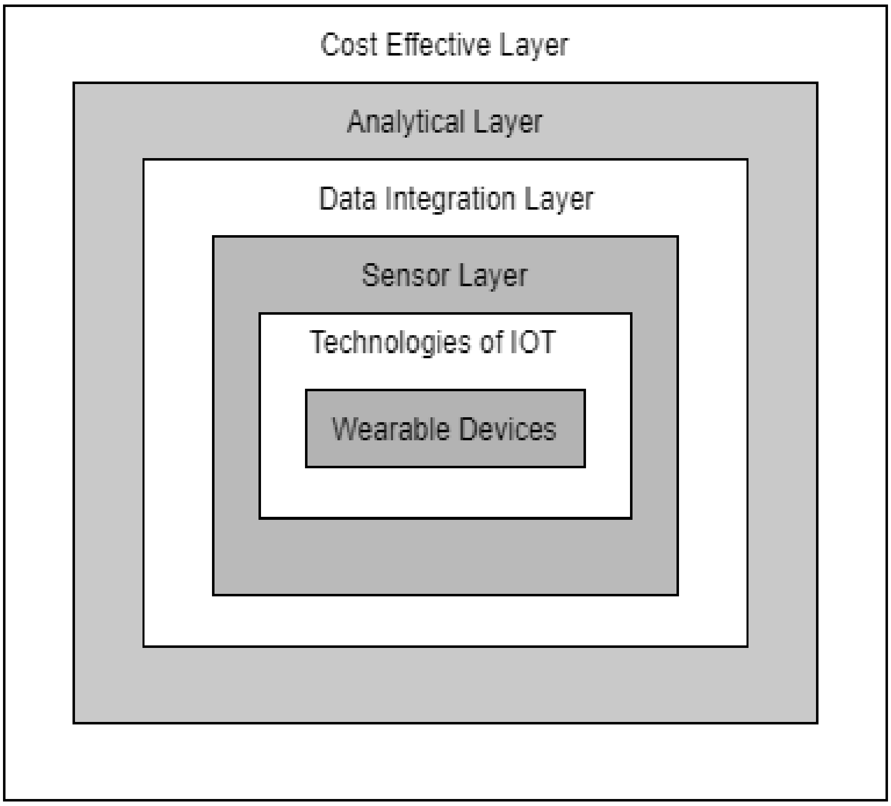

Figure 2: Organization of Wearable devices network

An interesting wearable hydrogel sensor provides an appropriate option for wearable electronics and matches well with the present manufacturing approach for connecting and correlating with a huge number of Internet of Things devices. This is due to their parts and structures, which are similar to human skin with the characteristics similar in their flexibility, ability to scale up, biocompatibility, and self-healing capabilities. Wearable hydrogel sensors are categorized to enable for a complete investigation of their configuration, mechanism, and design methodology. The article emphasizes current research on the primary structural components of wearable hydrogels: strengthening networks and conductive systems, giving prominence on various ways for increasing mechanical and electrical properties. The research gives an exhaustive analysis of wearable hydrogels and contains advice for the scheme of components and structures required to produce hydrogel sensors which are wearable and gives excellent performance. [15]

This paper suggests a distributed energy efficient clustering and routing technique for WBANs which are enabled by WioT. The distributed energy efficient clustering is divided into three phases: cluster development, Custer Head collecting, and direction-finding.

Cluster construction makes use of two hop neighbor statistics. The statistics related to two hop neighbors broadens the local picture of network topology, and aids in network topology maintenance. An analytical prototype is proposed which aids in computing the appropriate figure of collections in the setup. This routing uses low energy to boost communication within and outside the clusters. Their proposed distributed energy efficient clustering and routing protocol beats others in terms of better delay, factors influencing the control, time required for cluster formation, cluster durability, and network energy usage, according to simulated results. Besides, distributed energy balancing among nodes significantly increases the overall lifetime of the network.[16]

III. TECHNOLOGY

Wi-Fi and Bluetooth Recent events have seen hackers capture control of cars, trains, even dams. IoT devices are particularly vulnerable to hacking and covert hiring attempts to assault the online world. It poses a serious risk to internet security. For ethical hackers looking for security flaws, IoT and embedded devices present a new challenge. Globally, the media and governments are becoming increasingly concerned about their own security problems. 5G networks will be critical in smart healthcare wearable devices. Considering healthcare and wearables within the 5G network, 5G technology is critical from both a functional and financial standpoint. A few 5G applications in wearables and healthcare are mentioned in the research work.

A thorough examination of different technology advancements for fulfilling these standards in a 5G network was also carried out. Academics now have more options to undertake research projects in the field of 5G-based health-related devices, and shrinking and lightening wearables is a significant benefit. A small, attractive band is more likely to be worn than a large, bulky watch. Smart rings and "wearables," such as smart earphones, are becoming more popular as they get smaller and lighter. Analytics could be used by healthcare practitioners to analyse data sent through 5G from a wearable device for patients with chronic health issues. The patient would receive instant feedback on whether everything was well, whether to schedule an appointment, or, in the worst-case situation, whether to seek emergency care treatment. As a result, it has been observed that the network disappears anytime large groups of individuals attempt to utilize it. The wearable technology sector would benefit from 5G's ability to handle these issues. Earlier research focused mostly on using AI to improve resource efficiency, such as reducing delays and increasing reliability, or to improve overall security. The problem of identifying IoT 5G wearable medical devices has not been solved. [17]

Rectenna wearable energy harvester (RWEH) for power generation is a relatively recent area of research. However, more research is needed to improve the harvester's power production capacity. PWEH research has expanded due to promising results in wearable applications, as it can generate power in the mW range, which is adequate to power wearable systems and is recognized as acceptable for fabric applications. Despite the promising outcomes, surprisingly not much research is being done on the S.E.Hs and EWEHs for wearable applications. In the coming decades, the HWEHs, in particular the RWEHs, will emerge as a prominent study field and may perhaps expand. W.E.H.s are expected to be utilized in the future to fully power and run a range of wearable gadgets and devices, including those used in sports and fitness where they can be used for a fitness tracker, pedometer, heart rate, breathing rate, movement pattern, and electrical muscle activity, for entertainment in smart watches and ear buds; in education for smart eyewear; in the military for eyewear, smart textiles, smart key chains; and in health care.[18]

Therefore, in the future, research into materials and structural designs will be necessary to enhance the system's stability over lengthy use while retaining the wearability of the device.. However, due to significant differences in the amplitude, waveform, and frequency of electrical energy produced by various transduction processes, developing power management systems suitable for multiple energy harvesting techniques remains a challenge. Future systems are most likely to use H.E.H. technology, which integrates many transduction approaches.. Furthermore, a wider range of functional modules are being integrated into self-powered devices. To improve the efficiency of energy conversion and achieve power distribution among numerous functional units, design circuits should be constructed logically. One method to enhance the surface area of contact and boost the effectiveness of energy harvesting is to use surface micro- and nanostructures. The use of composite materials, external electrical systems, or even the creation of a mechanical structure are other choices. W.E.H.s are being studied by wearable technology researchers in order to solve the problem that batteries cannot provide the power needs of wearing devices. The literature on PWEHs stresses their size, power, and flexibility. Additionally, E.E.H. is suitable for wearable devices since it has a strong electromechanical coupling and performs well at low frequencies. WTEHs, on the other hand, are cheaper, lighter, and do not need an external power source. They are highly dependable and available. S.E.H.s have a high power density, however they are very light-dependent. HWEHs supply sufficient power to the wearable device despite requiring a complex circuit design.To summarize, wearable technology has improved tremendously and may dominate future generations of electronic gadgets and devices. Wearable devices will grow increasingly popular as materials science, smart technology, and process technology progress. [18]

IoT (Internet of Things) wearables have become more common in various healthcare services over time.. Early diagnosis, which improves predictive analysis, is one of the benefits of using wearable technology in eHealth. However, because wearable IoT devices have limitations, concerns about data privacy, service integrity, and network structure flexibility have developed. As a solution to these difficulties, a platform based on federated learning and private blockchain technology within a fog IoT network is proposed. With privacy-preserving characteristics, these systems secure data within the network. The distributive structure of a fog IoT network was used to build an adaptive network for wearable IoT devices. A testbed was used to evaluate the proposed platform's ability to maintain the integrity of a classifier.. According to the findings of the testing, the proposed implementation can successfully secure both a patient's privacy and the integrity of a predictive service. Additional research was conducted to learn more about how various technologies contribute to the security and adaptability of the IoT network.Overall, analysis, modeling, and experimentation were utilized to illustrate the platform's usefulness in addressing critical security and privacy issues associated with wearable IoT devices in predictive healthcare. [19]

Wearable technologies have their own advantages and disadvantages depending on their usage, power consumption, range, latency and transmission rates. The same has been brought out in the below mentioned table.[20][21]

Table 1: Technologies used in IOT

Technologies	Advantages	Disadvantages
Low-Energy Bluetooth	Low Power, Long Use	Small data range
Low-Energy Wireless	Low power consumption, device safety	Cannot be used over long distances
ZigBee, Z-Wave, and Thread	low-power, high throughput	Transmission rate is low
LTE-A	Reduces Latency, Increases throughput	Open to Interference
Wi-Fi-Direct	Connects without access points, low latency	Inefficient for large networks
LPWAN (Cat-M1/NB-IoT)	Provide long-range communication, uses small low cost batteries.	Can only send small blocks of data at a low rate.

IV. SECURITY

The research conducted in [3] focuses on the primary security concerns of IoT systems in order to educate consumers about the risks associated with these devices. IoT threats have been divided into several categories to aid comprehension. In addition, each class is thoroughly compared. Network attacks are initiated by injecting malicious nodes in order to steal information packets and degrade network performance. Side channel attacks are used by attackers to simultaneously target security and privacy. During strategy level attacks, attackers employ a variety of approaches to introduce harmful malware into IoT devices. Physical and logical attacks are differentiated by whether they can be carried out physically or remotely. Physical attacks wreak havoc on hardware components and necessitate physical contact. Remote logical attacks are possible. Because an attacker might be either an outsider with no prior knowledge of the targeted IoT system or an insider who is familiar with it, IoT attacks are categorized as internal or external based on antagonist location.

In hardware compromised assaults, the attacker tampers with the hardware in order to steal data. The deliberate insertion of malicious programs into a device in order to gain unauthorized access to it is referred to as a software attack. Due to faulty code, hackers get access to these IoT web applications, databases, or servers. Firmware attacks are carried out as a result of a failure to update firmware. [3]In order to aid manufacturers in safeguarding IoT systems, the complete literature study separated these categories into subcategories and evaluated over 75 IoT security concerns. In today's environment, new developing technologies such as block chain, artificial intelligence, machine learning, and other advanced technologies (fog and cloud computing) are being fused with IoT technology to address security and privacy problems. These emerging technologies, particularly block chain technology, have the potential to give a better and more cost effective solution to IoT security challenges. In the end, the review paper is summed up by suggesting some future research ideas in IoT security, which still need researchers' attention. [3]

The primary goal of the study was to investigate the factors that contribute to trust and, eventually, the intention to use WIoMT devices, as well as the impact of those independent variables on the outcome variable and the security concerns connected with WIoMT adoption The TAM model was used to determine the independent variables/domains of the study, which included perceived usability, perceived ease of use, reliability, functionality, and perceived security and privacy..[5]

The study adds to the literature on the adoption of WIoMT devices in our daily lives through investigating how usability, ease of use, security, and privacy affect consumer trust, which eventually leads to the behavioral purpose to use such devices on a regular basis. Furthermore, the study found that security and privacy considerations have the largest influence on the use of the WIoMT, and manufacturers, healthcare providers, and vendors must focus on what consumers believe if they want to promote the global acceptance of their technology.

According to the report, many potential users are unfamiliar with or do not use WIoMT devices. The usage of equivalent or updated WIoMT technology should be made more acceptable and widespread in future research. Researchers should look into more people who are utilizing WIoMT devices in bigger geographical areas to learn more about their attitudes toward adoption. [5]

The Internet of Things has opened up a world of infinite opportunities for applications in various sectors of society, but it also presents numerous obstacles. Security and privacy are two of these issues. Because of their limitations, IoT devices are more prone to security risks and assaults. Because there is a lack of security solutions for IoT applications, this universe of safely connected things is devolving into an internet of insecure things. The review conducted by [6] discussed the current state of IoT security and the clarifications that must be made to persuade users that IoT is more than just a source of inexpensive gadgets, but it is equally important to provide the best security solutions that address security threats and privacy concerns. IoT security must be maintained by users, security administrators, and forthcoming IoT developers. The developer's responsibility is to make sure that security is prioritized throughout the design and development of a system or application.[6]

The essay explores IoT security vulnerabilities from many perspectives (hardware, software, and data in transit), stressing precautions related to various security concerns. A discussion of existing security solutions is also provided. A thorough examination has been done to resolve the limitations that IoT devices face. A comparative review of all known hardware security solutions was undertaken with the purpose of providing security to IoT limited devices. The introduction of new technologies into the IoT ecosystem creates new vulnerabilities to overall network security. The study presented here focuses on the influence of two key developing technologies, machine learning techniques and block chain technology, on security when used in an IoT platform. It also proposed strategies to mitigate the risks that had been demonstrated. This could assist researchers with fresh directions to contribute to the field. [6]

To improve the performance of health data retrieval, the proposed method makes use of NDN benefits such as PIT aggregation, in network caching, and name based searching. IoT devices are the primary driving force behind the sensing and recording of patient health data. Furthermore, each wearable device serves as the leader in gathering and transmitting data to edge devices. Failure of any in charge would disrupt the entire monitoring for that specific patient, putting his life in danger in the event of an emergency. In the upcoming work, the research will move towards designing an optimal framework where periodic assignments will be considered for choosing and in charge from a single wearable device. This scheme will be tested in a more realistic setting, such as a multiage scenario, and examine the potential of defining separate edge servers with varying trust levels and dispersing all fragments across edges via Encryption. [8]

Wearable technology is becoming more and more popular, and a large portion of the population is using it to track their daily activities. As a result, the makers of these devices must be able to guarantee the privacy, accuracy, and accessibility of the data being collected. Some of the latest smartwatches gather private information, like health information, in a precise way that gives customers confidence in such gadgets, also helps them to decide on at what time to find medical advice. The devices are attacked passively in this case; it is helpful to know which components would make the greatest goals to take advantage of the shoddy coupling procedures and begin reading real-time data about the customers. As these technologies advancement and more sensors are added, the attackers will be capable of gathering critical real-time information and develop a sketch of a potential targeted person. [10]

The significance of an IoT legislative framework that requires suppliers to adhere to the criteria of privacy and security so that a new IoT product to developed, is emphasized in this work. A regulation requiring IoT security and privacy regulations assures that all components follow a set of minimal security and privacy requirements. Although this lies outside the purview of our study, the work assumes that it is important for creating justifications and additional work in these verticals, such as (a) protecting consumer confidentiality; (b) preventing cyberattacks; (c) promoting industry standards; (d) encouraging origination; and (e) establishing trust. Customers are more inclined to purchase and utilize an IoT gadget, given they are sure of their personal information which is being managed securely and responsibly. It is well recognized that consumers share some of the responsibility for information; smartwatch customers must be mindful of the dangers of exchanging private or delicate information through another device. In this situation, the fact that a smartwatch can employ the an association model like Just Works which is perhaps due to the fact that the data is not encrypted. However, it is natural that there are many misconceptions regarding how data sharing and pairing verification between a smartphone and a smartwatch function, and at the end of the day, vendors must also fulfill their obligations by guaranteeing that components will uphold the security and reliability of the user's data because it is challenging for an uneducated user to comprehend this procedure. [10]

V. APPLICATIONS

Smart Wearables can be classified as 1) Wearable 2) Implantable and 3) Stationary. Wearable devices are capable of changing many aspects of human existence, particularly healthcare, monitoring day to day activities, and computer interaction. But, a variety of technological and adaption obstacles impede the wide availability and regular use of wearable devices.

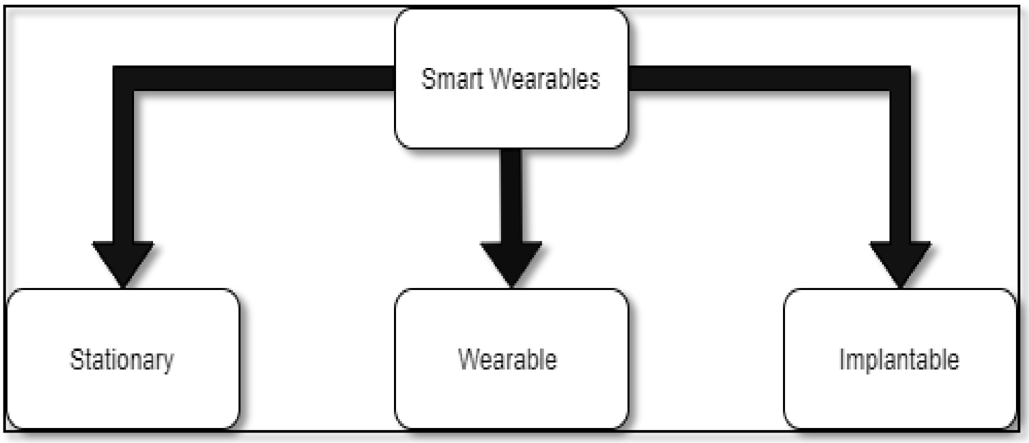

Figure 3: Wearable devices classification

Through recent research directions, wearable technology's potential on issues and finding answers can now be realized. The paper starts out by reviewing recent research on the challenges faced by wearable technology. The various solutions to each issue are discussed after that. The main applications that benefit wearable gadget users come first in our discussion. The proposal of physically malleable and bending devices that aim to increase user comfort is then presented. Modern energy harvesting and security techniques are also covered in order to increase wearable device user compliance. Overall, the goal of the article is to provide as a thorough resource for issues with and recommendations for self-powered wearables for activity and health monitoring, [2] as illustrated in the below Figure 4.[5]

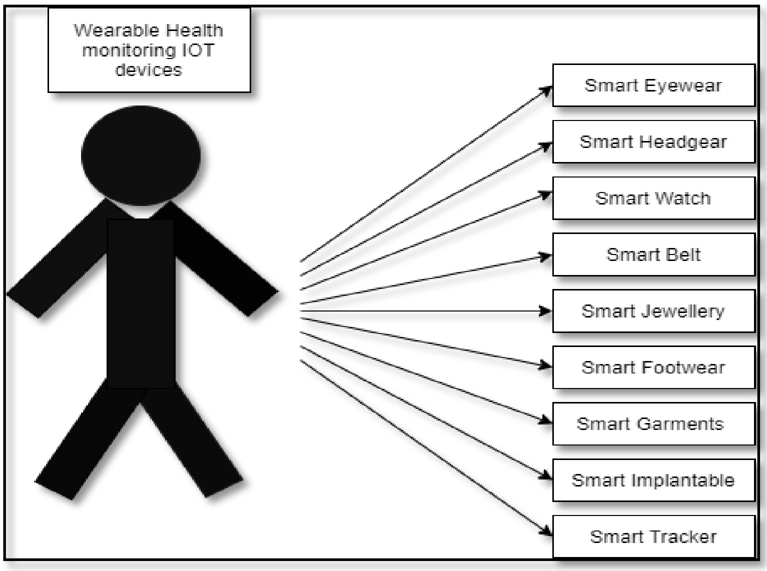

Figure 4: Different types of body wearables

The COVID-19 pandemic has, in summary, brought attention to the critical need for additional cutting-edge instruments and technology to control epidemics in the future. The study suggests a wearable, fitness monitoring system which are health based Internet of

Things that can remotely track the physiological characteristics of individuals under quarantine in real time. The method can greatly lighten the load on medical staff and aid in more efficient COVID-19 epidemic management. Additionally, it can be applied as a preventative strategy for stopping the upcoming pandemics reach. For solving the gaps in the currently available instruments in preventing epidemics, a one-to-many system made up of watch which is anti-epidemic and a tiny computer system is developed.

It can passively stop those in quarantine from leaving, restricting the spread of the virus's, tracks and stop the infection from spreading, safeguarding the public's health. A healthcare professional and the owner of the anti-epidemic watch can both view the status of the system, which continuously monitors the body temperature, heart rate, and concentration of the oxygen in the blood stream. Demands for quarantine have significantly decreased as the world gradually lowers the blockade. To address acknowledged issues and challenges, the one-to-many monitor system project will still continue to be developed and enhanced. For instance, the battery capacity of anti-epidemic watch, the PPG module, and the IoT design, which are aspects of the next-generation design, should be taken into account.

In order to meet more flexible server programming requirements, it is important to request a dedicated server or virtual environment. The second generation anti epidemic watch is being developed with an emphasis on hardware and software design, despite the limited funding and human resources available. The cloud-based IoT functionalities are also progressively growing. In the future, a system will be created to transfer data to various kinds of smartwatches and display information directly on the watch. Furthermore, abnormal condition warning features will be improved, such as better monitoring of physiological indices, printing reports, historical data inquiries, and data analysis. The current project's major goal is to develop a system that will eventually become a mature product capable of efficiently controlling not only COVID-19 but also future pandemics.[7]

According to [12] research conclusions such as 1) wearable devices are increasing yearly, and wearable devices have attracted much attention. 2) The evaluation factors of IoT wearable devices can be divided into factors for model evaluation and sub components for device evaluation. 3) Describes communication technologies used in IoT wearables, concluding with, a discussion is conducted on the open issues and challenges of wearable devices. This research work has only limited research papers and provides a reference for evaluation factors and field selection for research in wearable IoT. [12]

Because of wearable technology, the well-known category of gadgets now comprises entirely new and rapidly evolving technologies. Wearable technology has the potential to supply a lot of important data to artificial intelligence (AI) approaches, in addition to being appealing and furnished with cutting-edge hardware technologies like as communication modules and networking in the next generation. Several projects have previously been accomplished utilizing a variety of AI methodologies, including monitored, unattended, semi-supervised, and reinforcement learning (RL). The article looks at current wearable apps that have employed AI to achieve their goals. Users discuss particular examples of both supervised and unsupervised usage in medical diagnosis. In addition, cases combining augmented reality, wearables, and the internet of things are discussed. Wearables application samples for specific industries, such as healthcare, commercial, and athletic, are also offered. Personal exercise, mobility issues, and mental wellness are all implications in medicine.

Employee productivity can be increased by the usage of wearable technology at work. The fundamental objective of sports programs is to increase client happiness by encouraging physical activity or competition. The major problems with designing and building wearable technology are explored, as well as the computational expense of using Artificial intelligence methods. The potential and challenges for wearable technology in the future are examined.[14]

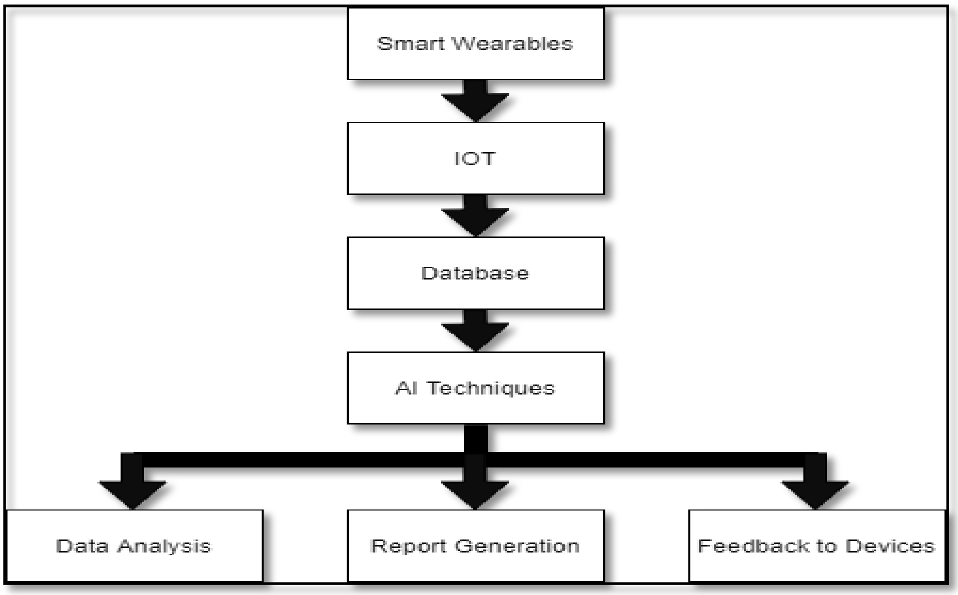

Figure 5: Wearable’s with AI Techniques

VI. CONCLUSION

Among the main domains the authors have focused on the recent works on wearable’s using IOT. The work covers the major field of networks, technology, security issues in wearable’s using IOT. The future studies can be done in detail in each of the mentioned domain and also will get to know the recent advancements in the related fields.

Declaration of conflicts of Interest: All the authors declare no conflict of interest.

REFERENCES

[1] F. John Dian, R. Vahidnia and A. Rahmati, "Wearables and the Internet of Things (IoT), Applications, Opportunities, and Challenges: A Survey," in IEEE Access, vol. 8, pp. 69200-69211, 2020, doi: 10.1109/ACCESS.2020.2986329.

[2] Bhat, Ganapati, Ujjwal Gupta, Yigit Tuncel, Fatih Karabacak, Sule Ozev, and Umit Y. Ogras. "Self-powered wearable iot devices for health and activity monitoring." Foundations and Trends® in Electronic Design Automation 13, no. 3 (2020): 145-269.

[3] Aqeel, Muhammad, Fahad Ali, Muhammad Waseem Iqbal, Toqir A. Rana, Muhammad Arif, and Rabiul Auwul. "A Review of Security and Privacy Concerns in the Internet of Things (IoT)." Journal of Sensors 2022 (2022).

[4] https://www.researchgate.net/figure/Different-types-of-wearable-technology_fig5_322261039/download

[5] Thapa, Sanjit, Abubakar Bello, Alana Maurushat, and Farnaz Farid. "Security Risks and User Perception towards Adopting Wearable Internet of Medical Things." International Journal of Environmental Research and Public Health 20, no. 8 (2023): 5519.

[6] Williams, Phillip, Indira Kaylan Dutta, Hisham Daoud, and Magdy Bayoumi. "A survey on security in internet of things with a focus on the impact of emerging technologies." *Internet of Things* 19 (2022): 100564.

[7] Wu, Ju-Yu, Yuhling Wang, Congo Tak Shing Ching, Hui-Min David Wang, and Lun-De Liao. "IoT-based wearable health monitoring device and its validation for potential critical and emergency applications." *Frontiers in Public Health* 11 (2023): 1188304.

[8] Gupta, Divya, Shalli Rani, Saleem Raza, Nawab Muhammad Faseeh Qureshi, Romany F. Mansour, and Mahmoud Ragab. "Security paradigm for remote health monitoring edge devices in internet of things." *Journal of King Saud University-Computer and Information Sciences* (2023): 101478.

[9] Zovko, Kristina, Ljiljana Šerić, Toni Perković, Hrvoje Belani, and Petar Šolić. "IoT and health monitoring wearable devices as enabling technologies for sustainable enhancement of life quality in smart environments." *Journal of Cleaner Production* 413 (2023): 137506.

[10] Silva-Trujillo, Alejandra Guadalupe, Mauricio Jacobo González González, Luis Pablo Rocha Pérez, and Luis Javier García Villalba. "Cybersecurity Analysis of Wearable Devices: Smartwatches Passive Attack." *Sensors* 23, no. 12 (2023): 5438.

[11] Savithri, M., M. Pradeepa, D. Rajendra Prasad, Durgaprasad Gangodkar, R. Rajalakshmi, Shaik Shafi, N. M. Sinchana, K. R. Prasanna Kumar, and Nagarajan Selvam. "Enhancement of QoS in Internet of Things Wearable Devices Dependent on 5G Technology." *Wireless Communications and Mobile Computing* 2023 (2023).

[12] Rahmani, Amir Masoud, Wang Szu-Han, Kang Yu-Hsuan, and Majid Haghparast. "The Internet of Things for Applications in Wearable Technology." *IEEE Access* 10 (2022): 123579-123594.

[13] Kumar, Virendra, Patel Jignasaben Babubhai, Fayaz Ahmed Fayaz, Kiran Dhobal, Praveen Kumar Rai, and Ashok Rachapalli. "Role of Artificial Intelligence in the Next Generation Wearable Devices." In 2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 1180-1184. IEEE, 2023.

[14] [15] Zhu, Junbo, Jingchen Tao, Wei Yan, and Weixing Song. "Pathways towards wearable and high-performance sensors based on hydrogels: toughening networks and conductive networks." National Science Review (2023): nwad180.

[15] Arafat, Muhammad Yeasir, Sungbum Pan, and Eunsang Bak. "Distributed energy-efficient clustering and routing for wearable IoT enabled wireless body area networks." IEEE Access 11 (2023): 5047-5061.

[16] [17] Devi, Delshi Howsalya, Kumutha Duraisamy, Ammar Armghan, Meshari Alsharari, Khaled Aliqab, Vishal Sorathiya, Sudipta Das, and Nasr Rashid. "5g technology in healthcare and wearable devices: A review." Sensors 23, no. 5 (2023): 2519.

[17] Ali, Ahsan, Hamna Shaukat, Saira Bibi, Wael A. Altabey, Mohammad Noori, and Sallam A. Kouritem. "Recent progress in Energy Harvesting Systems for wearable technology." Energy Strategy Reviews 49 (2023): 101124.

[18] Baucas, Marc Jayson, Petros Spachos, and Konstantinos N. Plataniotis. "Federated learning and blockchain-enabled fog-IoT platform for wearables in predictive healthcare." IEEE Transactions on Computational Social Systems (2023).

[19] https://www.zipitwireless.com/blog/5-types-of-wireless-iot-technology

[20] https://www.tutorialspoint.com/internet_of_things/internet_of_things_technology_and_protocols.htm