

2024421

by Matthew Perry

Submission date: 27-Apr-2024 01:24AM (UTC+0100)

Submission ID: 231085376

File name: 16803_Matthew_Perry_2024421_183168_1410734699.docx (665.32K)

Word count: 3826

Character count: 24197

Your Name: Matthew Perry

University Number: 2024421

Course: BSc Electrical / Electronic Engineering

Module Code: SGEE6005

Assignment Title: The Internet of Things

Date Submitted: 27/04/2024

Word Count: 2997 words

Table of Contents

1. Work plan for life-long learning	4
2. Executive Summary	5
3. Key Concepts of IoT and Industry 4.0	6
3.1 Applications	6
3.2 IoT Communication Protocols	7
3.3 Connectivity Models	8
3.4 Transformational Potential	9
3.5 Specified Application of IoT	10
4. Security and Privacy Challenges	11
4.1 Vulnerabilities	11
4.2 Cyber Security	11
4.3 Privacy Challenges	13
4.4 Regulatory Framework	14
5. Analysis and Evaluation	15
6. Conclusion	16
7. References	17
8. Appendix	20

Figure 1; Parameters to Secure IoT Devices 12

Figure 2; Example of Strava Heat Map 13

Figure 3; Medical IoT Applications and Sectors 20

Table 1; IoT Healthcare Applications 10

1. Work plan for life-long learning

This assignment will be carried out methodically, where an investigation into key concepts of IoT & Industry 4.0. Research into how this technology is implemented within industry and connectivity types. Additionally, Security and privacy challenges will be explored including a case study that shows that security and privacy is paramount when implementing these systems. Lastly, an analysis and evaluation on the work documented will be carried out and summarised within a conclusion.

2. Executive Summary

This assignment examined key concepts and the application of IoT in general and specifically IoT applications within the medical sector. How these devices operate were investigated in relation to connectivity and communication models.

It highlighted the issues such as poor built in security measures and reliance on weak protocols and challenges associated with open-source components and legacy equipment. These factors led to vulnerabilities that can compromise device functionality and user privacy. How these vulnerabilities were attacked with common ransomware practices and the consequences of these downfalls.

Real world consequences and statistics were stated, while regulatory framework and best practices were investigated to increase the security and overall efficiency of IoT devices.

Lastly, the research was analysed and evaluated where the data was commented on, the findings showed that the research consisted of trustworthy sources while referencing real world applications, consequences, and design practices.

3. Key Concepts of IoT and Industry 4.0

During 1997, Kevin Ashton, a British technologist began exploring a technology framework radio-frequency identification (RFID), that would allow physical devices to connection through microchips and wireless signals. Ashton then coined the phrase 'the internet of things' (Greengard, 2024).

The internet of things can be defined as a closed loop system in which a set of sensors is connected to servers via a network. The data that is collected from the sensors are stored within a database and then analysed by IoT analytics (Márquez, 2021).

3.1 Applications

Although when sensors and actuators are mentioned, it can be thought completely as industry based, however there are many applications where IoT is implemented whether it is consumer or industrial based.

Sensors can be integrated into wearable devices, such as equipment and inside the human body to transmit data from various sources such as vital levels. As an example, the VITALS system is an online life-signs sensor that implements four physiological indicators that are recognised by clinical equipment. This includes a micro-controller, a wireless communication module, and a system that can implement data analysis. Life signs are extracted and transmitted to the analysis every half an hour, which improves patient monitoring and care while being done remotely from a medical department (Chunyan Li, et al., 2024)

IoT is being implemented within retail, this is to further generate economic value within this sector and to monitor stock. An example from this sector could be an improved checkout system where a customer can leave automatically with items, then using the RFID on the items it can be calculated at checkout and paid for via a mobile app (Pilats, 2023).

Within agriculture, sensors are used to collect environmental and machine metrics which can be analysed or interpreted by technology or farmers. A popular use of IoT within farming is smart weather stations that are located remotely around an area that collect data such as climate conditions, specify an appropriate crop and implement measures to improve the capacity of the farm via actuators such as valves for watering also known as 'precision farming' (Shalimov, 2023).

3.2 IoT Communication Protocols

IoT Communication protocols are sets of rules and standards that specify how devices exchange data and communicate with each other and with other platforms. The protocols define a format, structure, and sequence of messages between devices, gateways, and cloud servers. Listed below are some commonly used protocols used within IoT medical device IoT communications and dependant on the application the appropriate protocol will be selected (Mendizábal, 2022).

- Message Queue Telemetry Transport (MQTT) – For constrained devices and low bandwidth, high latency, or unreliable networks.
- Hypertext Transfer Protocol (HTTP) – For device to cloud applications however it is not always viable due to financial constraints.
- Constrained Application Protocol (CoAP) – Most suitable for IoT devices and low power wireless networks.
- Data Distribution Service (DDS) – Suited for distributed systems which require scalability, low latency communications.
- LoRaWAN – For long range communication between IoT devices and gateways over wireless networks.
- Health Level 7 (HL7) – International standard for the exchange, integration, sharing and retrieval of electronic health information.

Key factors to consider when a communication protocol is implemented is to include security, reliability, and energy efficiency. By doing so, medical devices can ensure efficient and secure data exchange.

3.3 Connectivity Models

There are 4 common communication models implemented while using IoT, these are device-to-device, device-to-gateway, device-to-cloud, and back-end data-sharing. The right connectivity model for IoT medical devices depends on factors such as data transmission ranges, data volume, network reliability and specific healthcare applications.

Device-to-Device

This model is made for two or more devices that connect and communication between one another directly. The devices can do this via various networks including IP networks or the internet but most commonly use protocols like Bluetooth, Z-wave and Zigbee. This model is commonly used in small data applications at a low data rate such as home automation.

Device-to-Gateway

The device to gateway model is to connect an intermediary device to access the cloud service, this involves application software operating on a local gateway device such as a smart phone that can be used between an IoT device and cloud service.

Device-to-Cloud

Device-to-cloud communication involves an IoT device connecting directly to an internet cloud service such as an application service provider to move data and control message traffic, this is done through the means of wired ethernet, Wi-Fi connections and cellular technology. Cloud connectivity lets the user to obtain remote access to a device and supports updates to the device.

Back-End Data-Sharing

This model extends single device-to-cloud communication model so IoT devices and sensor data can be authorised by third parties. Object data can be exported and analysed from a cloud service in combination with data from other sources (Channel Futures , 2016).

3.4 Transformational Potential

IoT is implemented into a wide range of applications whether its to benefit customer satisfaction, remote working, financial gain and more.

In relation to the chosen application IoT within healthcare, it is revolutionising the sector. Previously, the healthcare sector was mostly organised with pen and paper, however electronic health records are the largest implementation of IoT to try meet evolving business models such as value-based reimbursement and virtual care.

The World Health Organisation adopted telemedicine to define healthcare support using information and communication technologies in which distance and/or geographical barriers hinder healthcare services (Silva, 2023). In recent years, telemedicine has become a common practice, with the outbreak of Covid-19 the use of telemedicine accelerated to prevent spread of infection.

Regarding patient contact care, remote patient monitoring his implemented often, where IoT sensors to offer healthcare units a stream of real-time health data such as heart rate, blood pressure. Healthcare advisors can work remotely, where if a patient is inconsistent with taking medication, smart medication dispensers can be employed in a patient's home to distribute the medication remotely, it can then be tracked how much has been dispensed and the frequency (Meola, 2023).

Lastly, it is estimated that the number of the IoT connections worldwide will double between 2021 and 2030 reaching 37.4 billion (GSMA, 2023). Additionally, Deloitte predicts close to 70% of all medical devices to be connected to the internet by 2025 (Rao, 2021).

3.5 Specified Application of IoT

From the research, the basis of how IoT operates is selected dependant on the application. The table below has been compiled of healthcare IoT products and their characteristics to show how different applications may select different methods.

IoT Healthcare Applications				
<u>Application</u>	<u>Description</u>	<u>Protocol</u>	<u>Connectivity Model</u>	<u>Reference</u>
Wearable Health Monitors	Fitness trackers, smartwatches and smart bands that monitor various health metrics that provide real-time data to both users and healthcare providers.	Bluetooth Low Energy (BLE), Near field communication (NFC)	Device-to-device, device-to-gateway, and device-to-cloud.	(Henriksen & Mikalsen, 2018)
Smart Pill Dispensers	Automatically dispenses medication according to a prescribed schedule and can send reminders to patients to take medication.	Open Mobile Alliance (OMA), Message Queue Telemetry Transport (MQTT)	Device-to-gateway, and device-to-cloud.	(Pak & Park, 2012)
Connected Medical Implants	Insulin pumps, pacemakers and cochlear implants can be connected to healthcare networks for remote monitoring.	Medical Implant Communication Systems (MICS)	Device-to-gateway, device-to-cloud, Back-end Data-Sharing	(Islam & Yuce, 2016)
Telemedicine Equipment	Devices such as cameras, microphones and connected medical instruments allow healthcare providers to carry out consultations and examinations.	Internet Protocol (IP)	Device-to-device	(GG, 2023)

Table 1; IoT Healthcare Applications

4. Security and Privacy Challenges

4.1 Vulnerabilities

IoT devices at present consist of vulnerabilities that can compromise security, privacy, and function ability. This is mainly due to inadequate built in security measures to prevent threats. Many IoT devices use low power, which restricts their functionalities such as limited processing power.

Due to IoT using communication protocols open the vulnerability of attacks. Often, standardisation of protocols in IoT isn't implemented or weak protocols are employed. Additionally, the use of opensource components by manufacturers to build devices creates a complex supply chain that is difficult to track. If a manufacturer is using legacy equipment, these components may inherit vulnerabilities known to attackers that create a landscape which is ready to be exploited (Arampatzis, 2023).

Lastly, with IoT devices being connected remotely to networks, the physical devices are often deployed in unsecured locations that can be tampered with and stolen.

4.2 Cybersecurity

Although IoT is beneficial within the healthcare industry, these applications can be subject to significant security challenges such as data breaches, cyber-attacks, and malicious use.

With IoT devices creating large amounts of data, this big data should be managed, secured, and analysed, however cyber-attacks in IoT solutions are prevalent (Pourrahmani & Adel Yavarinasab, 2023).

The most common method of breaching personal data within an IoT system are man-in-the-middle attacks and code injection.

- Man-in-the-middle attack is mostly to steal personal information such as log in credentials, account details and credit card numbers. In relevance to healthcare sector, this could be prevalent when using smart wearable devices and logging into accounts or accessing electronic health records (Imperva, 2024).
- Code injection is when an attacker injects malicious code into a vulnerable system and often allows the attacker to take control of the system or access sensitive data (Noman, 2023).

During 2018/2019 the US Food and Drug administration recalled 34,000 implantable cardiac pacemakers and more than 4,000 insulin pumps due to cyber circuitry flaws that would allow unauthorised access that would allow an attacker to remotely alter the function or dosage of these devices (AON, 2022).

Additionally, the most common methods where IoT systems can be compromised and disrupted is DDoS attacks and Botnet attacks.

- DDoS attacks flood a target system, server, or network with an overwhelming volume of traffic, this can disrupt essential services such as electronic health record systems, telemedicine services, and patient monitoring systems (Jain, 2023).
- Botnet attacks can obtain control of internet enabled devices without the permission of the owners to perform tasks (Penetration Testing , 2023).

During 2017, the UK National Health Service was stopped when a virus known as 'WannaCry' infected computers and demands a ransom payment to allow users access to their data was released worldwide. This caused issues with accessing electronic health records, emergency dispatching systems and appointments (National Audit Office , 2017).

Lastly, the cyber security can be improved within IoT by following the procedures in Figure 1 at 4 different levels which consist of device, application, system, and communications.

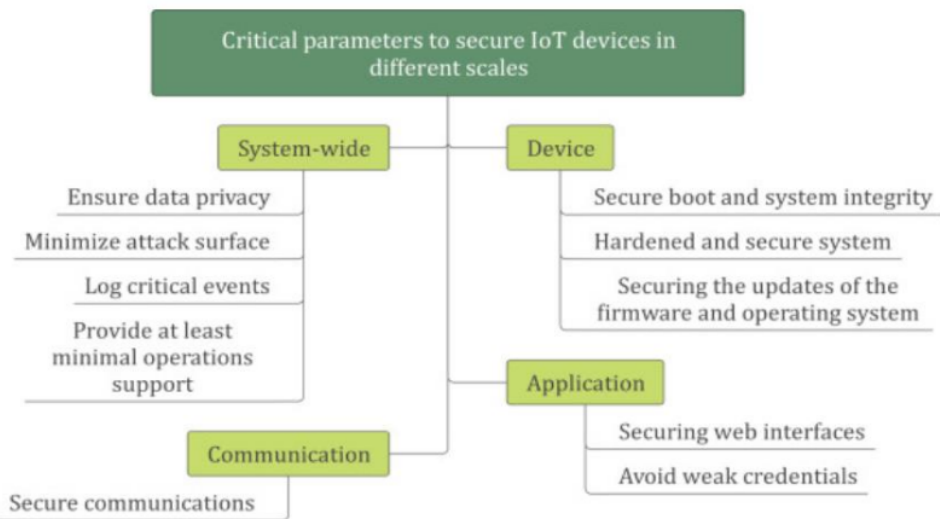


Figure 1; Parameters to Secure IoT Devices

4.3 Privacy Challenges

Highlighting the importance of cyber circuitry vulnerabilities posed by IoT, personal fitness tracking through the means of wearable smart devices shares the data via an application programming interface. It was revealed that a third-party platform was able to obtain fitness tracking data from nearly all the major wearable device providers and breach the data leaving an estimated 61 million records exposed (Ideka, 2021). Additionally, the data that is being recorded can be sold to advertisers or used without the individual's awareness or consent. An example, of this can be reflected on from 2011 when Fitbit faced a class action lawsuit in 2011 for allegedly selling personal health data to 3rd party advertisers without consent of the users (Silva, 2023).

Without breaches, the data that is being recorded can be sensitive. During 2018, a fitness tracking app, Strava, which allows users to track and share workout routines to then be posted to a platform. The platform records jogging routes, collects the data, and publishes heat maps, where a heat map is a popular route with users. This revealed the locations of military bases and personnel around the world where patrols and exercises are taking place (BBC, 2018).



Figure 2; Example of Strava Heat Map

4.4 Regulatory Framework

IoT medical devices in the UK must adhere to regulatory frameworks that include medical device regulations, data protection laws and cyber security standards to uphold and ensure the safety and privacy of users and patients. The regulatory framework that should be followed has been investigated below.

UK General Data Protection Regulation

The UKGDPR outlines framework that applies to controllers and processors within and outside of the UK if the processing activity relates to monitoring the behaviour of individuals. It governs the collection, processing and storage of personal data which is relevant to IoT medical devices. It also outlines that informed consent from data subjects, implementing secure data storage practices and respecting individual's rights (LGA, 2018).

BSI PAS 212:2016

This British standard provides a simple way for IoT applications and services to interpolate without the need for intervention from a human programmer. It covers conditional requirement for catalogue access for security mechanisms to protect access and prove provenance. This standard essentially shares the best practices for securing devices and protecting data (bsi.knowledge, 2016).

ISO/IEC 27001

This is an international standard for establishing, implementing, and maintaining an information security management system. The standard provides a framework to managing sensitive information and ensuring data security.

NCSC

Lastly, manufacturers of IoT devices should look for guidance and support from the national cyber security centre in the United Kingdom. The NCSC contributes to the development of national policies and standards and can provide resources and best practices to protect against cyber threats.

5. Analysis and Evaluation

The research conducted within this assignment covered a broad range of medical IoT devices, and how these devices are operating. Specific examples of applications such as the Vitals system within healthcare and outside of healthcare were shown for different implementations. A clear emphasis on potential benefits while using IoT were showcased included numerical statistics on the evolving use of IoT with estimated connected devices for the future and how this can be seen as a transformational potential in comparison to where IoT was first introduced.

The communication and connectivity models commonly used within IoT medical devices were investigated and the strengths and weaknesses of each were explained, however specific metrics such as latency, bandwidth and error rates were not discussed.

Multiple vulnerabilities were exposed within the IoT devices such as ransomware and exploring the high likelihood of security concerns within the IoT landscape. Case examples were referenced where IoT security had failed and how this affected a healthcare service or patients' privacy. This is often due to new technology with low power consumption, size and cost are often lacking in maturity in comparison to traditional ethernet or Wi-Fi. Additionally, without hacking being involved with IoT, it was shown how its important for a manufacturer or service to control what data is public, where Strava revealed foreign parameters of military bases.

Its important to note that regulatory framework outlines specifications that manufacturers should use for guidance when designing IoT systems. By following these specifications data breaches can be less of a threat while maintaining a good privacy for the users/patients. Although the recall of medical implant devices can seem worrying, its important for manufacturers to monitor and evaluate emerging threats, then take the best course of action.

Lastly, the research conducted consisted of a wide range of quality and trustworthy sources, however technical hardware specifications could have been investigated further.

6. Conclusion

In conclusion, this assignment has investigated key concepts within IoT and Industry 4.0. The development of IoT has been evolving rapidly and the number of the IoT connections worldwide will double between 2021 and 2030 reaching 37.4 billion (GSMA, 2023).

It was found that the IoT devices can be split into two main groups which are industry based and consumer based. In the selected application of healthcare, the applications can vary from telemedicine, implanted medical devices, remote dispensaries and more. Dependent on the application, different communication protocols and device connectivity may be selected.

While IoT within healthcare seems to be overall beneficial, there are security and privacy concerns with the devices. A primary concern identified from the research is limited built in security measures that lead to vulnerabilities that compromise the functionality and privacy of these devices. Additionally, when manufacturers use open-source components and legacy equipment it can create complex supply chain that attackers know how to exploit. The use of weak and unstandardised communication protocols can increase the likelihood of attacks such as man-in-the-middle-code injection, DDoS, and Botnet attacks.

A real-world example of a cyber security flaw was a recall of implanted medical devices where the flaw could allow unauthorised access to potentially stop or alter the functions of the device. Privacy concerns were investigated where personal fitness tracking data can be exposed and misused without user's consent, which resulted in a lawsuit. Data collected isn't always breached or misused intentionally, however the Strava heat map incident in 2018 emphasised the potential for sensitive data to accidentally shared, which leads to privacy breaches and ethical concerns.

The concerns showed the importance of improving cybersecurity within IoT through various measures such as robust security at different levels whether its device, application, system, and communication. While systems should be continually monitored, regular software updates and education at a user level if the application is consumer based. Additionally, regulation framework can be referenced when an IoT device is designed, which shows a need for a security first approach, focusing on security measure and data privacy.

Lastly, a recommendation for IoT design in the future is to have a coloration and standardisation of communication protocols and security measures to try improving the overall security and reliability of devices.

7. References

- AON, 2022. *Cyber Security of medical IoT devices*. [Online]
Available at: https://www.aon.com/cyber-solutions/wp-content/uploads/Cyber-Medical_Device_whitepaper_English.pdf
[Accessed 25th April 2024].
- Arampatzis, A., 2023. *Top 10 Vulnerabilities that Make IoT Devices Insecure*. [Online]
Available at: <https://venafi.com/blog/top-10-vulnerabilities-make-iot-devices-insecure/>
[Accessed 25th April 2024].
- BBC, 2018. *Fitness app Strava lights up staff at military bases*. [Online]
Available at: <https://www.bbc.co.uk/news/technology-42853072>
[Accessed 17th April 2024].
- bsi.knowledge, 2016. *Automatic resource discovery for the Internet of Things. Specification*. [Online]
Available at: <https://knowledge.bsigroup.com/products/automatic-resource-discovery-for-the-internet-of-things-specification?version=standard>
[Accessed 25th April 2024].
- Channel Futures , 2016. *The Four Internet of Things Connectivity Models Explained*. [Online]
Available at: <https://www.channelfutures.com/regulation-compliance/the-four-internet-of-things-connectivity-models-explained>
[Accessed 29th March 2024].
- Chunyan Li, Wang, J., Wang, S. & Yudong Zhang, 2024. A review of IoT applications in healthcare. *Neurocomputing*, 565(1st), pp. 40-45.
- GG, 2023. *Video Conferencing Protocols*. [Online]
Available at: <https://www.geeksforgeeks.org/video-conferencing-protocols/>
[Accessed 20th April 2024].
- Greengard, S., 2024. *Internet of Things*. [Online]
Available at: <https://www.britannica.com/science/Internet-of-Things>
[Accessed 17th March 2024].
- GSMA, 2023. *IoT For Development* , London: GSMA.
- Henriksen, A. & Mikalsen, H., 2018. *Using Fitness Trackers and Smartwatches to Measure Physical Activity in Research: Analysis of Consumer Wrist-Worn Wearables*. [Online]
Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5887043/>
[Accessed 17th April 2024].
- Ideka, S., 2021. *Mass Leak of Fitness Tracking Data Hits Fitbit, Apple, Microsoft, Google; 60 Million Records Exposed by Improperly Configured Third-Party Database*. [Online]
Available at: <https://www.cpomagazine.com/cyber-security/mass-leak-of-fitness-tracking-data-hits-fitbit-apple-microsoft-google-60-million-records-exposed-by-improperly-configured-third-party-database/>
[Accessed 17th April 2024].
- Imperva, 2024. *Man in the middle (MITM) attack*. [Online]
Available at: <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>
[Accessed 25th April 2024].

- Islam, M. N. & Yuce, R. M., 2016. *Review of Medical Implant Communication System (MICS) band and network*. [Online]
Available at: <https://pdf.sciencedirectassets.com/313521/1-s2.0-S2405959516X00069/1-s2.0-S2405959516301035/main.pdf?X-Amz-Security-Token=IQoJb3JpZ2luX2VjEGYacXVzLWVhc3QtMSJIMEYCIQDOuIBtqZ8Tz1P7g1f7lqky%2FfcwBzsnkfLM6ZdRQbfEqAlhALvw9x6fPH%2FsoduKewj3eAul1ertUt7eDjTfexcl>
[Accessed 20th April 2024].
- Jain, A. K., 2023. *A comprehensive study of DDoS attacks over IoT network and their countermeasures*. [Online]
Available at: <https://www.sciencedirect.com/science/article/pii/S0167404823000068>
[Accessed 25th April 2024].
- LGA, 2018. *The General Data Protection Regulation*. [Online]
Available at:
[https://www.local.gov.uk/sites/default/files/documents/The+General+Protection+Data+Regulation+\(GDPR\)++Guidance+for+Members.pdf](https://www.local.gov.uk/sites/default/files/documents/The+General+Protection+Data+Regulation+(GDPR)++Guidance+for+Members.pdf)
[Accessed 25th April 2024].
- Márquez, F. P. G., 2021. *Internet of Things*. 1st ed. London: IntechOpen.
- Mendizábal, I. d., 2022. *IoT Communication Protocols—IoT Data Protocols*. [Online]
Available at: <https://www.allaboutcircuits.com/technical-articles/internet-of-things-communication-protocols-iot-data-protocols/>
[Accessed 17th March 2024].
- Meola, A., 2023. *IoT Healthcare in 2023: Companies, medical devices, and use cases*. [Online]
Available at: <https://www.emarketer.com/insights/iot-healthcare/#:~:text=The%20IoT%20enables%20healthcare%20providers,sit%20down%20with%20a%20physician>
[Accessed 29th March 2024].
- National Audit Office , 2017. *Investigation: WannaCry cyber attack and the NHS*. [Online]
Available at: <https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/>
[Accessed 25th April 2024].
- Noman, H. A., 2023. Code Injection Attacks in Wireless-Based Internet of Things (IoT): A Comprehensive Review and Practical Implementations. *Sensors* , 23(13).
- Pak, J. & Park, K., 2012 . *Construction of a smart medication dispenser with high degree of scalability and remote manageability*. [Online]
Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3412374/>
[Accessed 17th April 2024].
- Penetration Testing , 2023. *Botnet Attacks and Their Prevention Techniques Explained*. [Online]
Available at: <https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/botnet-attack-prevention/>
[Accessed 25th April 2024].
- Pilats, M., 2023. *IoT in retail: 10 use cases, benefits, and challenges*. [Online]
Available at: <https://www.itransition.com/iot/retail>
[Accessed 18th March 2024].

Pourrahmani, H. & Adel Yavarinasab, 2023. *A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain.* [Online]

Available at: (<https://www.sciencedirect.com/science/article/pii/S2542660523002111>)
[Accessed 25th April 2024].

Rao, D. S., 2021 . *The Complete Guide to Connected Medical Devices: Strategies, Use Cases, and Benefits.* [Online]

Available at: <https://www.birlasoft.com/articles/complete-guide-connected-medical-devices>
[Accessed 17th April 2024].

Shalimov, A., 2023. *IOT IN AGRICULTURE: 9 TECHNOLOGY USE CASES FOR SMART FARMING (AND CHALLENGES TO CONSIDER).* [Online]

Available at: <https://easternpeak.com/blog/iot-in-agriculture-technology-use-cases-for-smart-farming-and-challenges-to-consider/>
[Accessed 17th March 2024].

Silva, C. R. D. V., 2021. *Telemedicine in primary healthcare for the quality of care in times of COVID-19: a scoping review protocol.* [Online]

Available at: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8277488/>
[Accessed 20th April 2024].

Silva, J. P. d., 2023 . *Privacy Data Ethics of Wearable Digital Health Technology.* [Online]

Available at: <https://cdh.brown.edu/news/2023-05-04/ethics-wearables>
[Accessed 17th April 2024].

8. Appendix

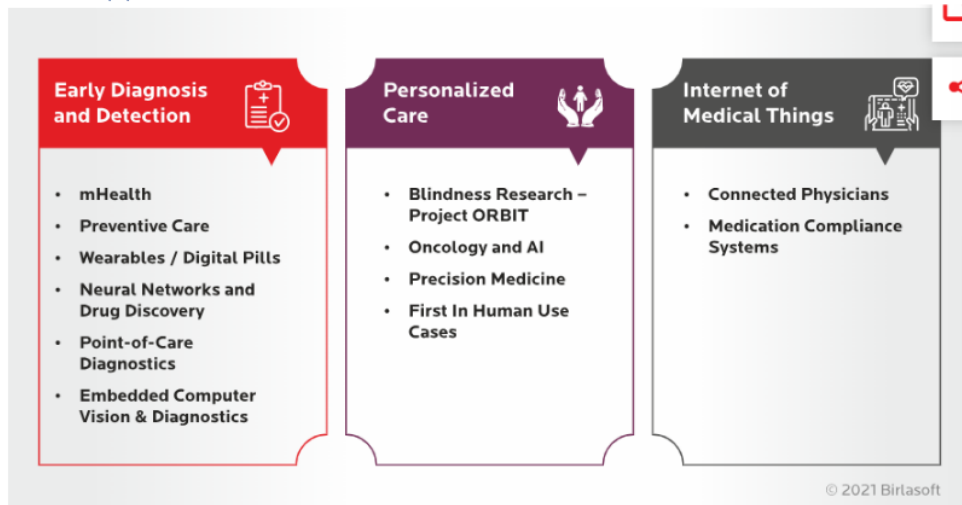


Figure 3; Medical IoT Applications and Sectors

FINAL GRADE

GENERAL COMMENTS

75/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

GRADING FORM: CSG-RUBIC

MATTHEW PERRY**75****RESEARCH-INFORMED LITERATURE**



There was evidence of considerable further reading and research from highly credible and reliable sources. Your interpretation and understanding of the additional research was exceptional and demonstrated a deep underlying appreciation of the subject. Your references were consistently applied to a high level of competency and your reference list was extensive for this assignment.

16**KNOWLEDGE AND UNDERSTANDING**



The knowledge and understanding of the subject demonstrated by this assignment was generally very good. There were few gaps in your knowledge of the basic principles and your understanding of the higher level concepts was demonstrated to a high degree. You have demonstrated a competent critical understanding

21

of the main concepts and expanded your knowledge beyond that contained in the course notes.

ANALYSIS



Your analysis of the task was generally very good, both in class and as shown in this assignment. You have demonstrated sound critical analysis skills and your approach to the task was logical. You carried out a detailed evaluation of the results and included a good conclusion relating the practical results to researched theory. The conclusions demonstrated very good cognitive skills and the ability to interpret quantitative and qualitative data without error.

30

PRACTICAL APPLICATION AND DEP.

SKILLS FOR PROFESSIONAL PRAC.



In this assignment you have demonstrated skills in working individually and also collaboratively. Your written report was written in a professional and confident style, however you still need to be more efficient with your word count. The report was very well presented, with excellent diagrams in appropriate places, good sentence/paragraph structure and clear calculations.

8