# IoT Application: Remote Monitoring of Heart Patients

# Industry: Healthcare

Student No. **21011025**

Word count (excluding references): 2920 words

**Table of Contents**

1 Introduction ..... 3

2 Technologies ..... 4

2.1 Sensing Layer ..... 4

2.1.1 Wireless Sensor Network ..... 4

2.1.2 ECG sensors ..... 4

2.1.3 Wireless Communication ..... 5

2.2 Network Layer ..... 6

2.3 Application Layer ..... 7

3 Data Analytics ..... 8

4 Security and Privacy Issues ..... 10

4.1 Jamming Attacks ..... 10

4.2 Sinkhole Attacks ..... 11

4.3 Virtual Machine (VM) Attacks ..... 12

4.4 Insider Attacks ..... 14

5 Market Implications ..... 14

5.1 Current Barriers and Adoption of Smart Healthcare ..... 14

5.2 Improving Adoption and Marketing of the IoT System ..... 15

Conclusion ..... 15

References ..... 16

# 1 Introduction

The healthcare industry is currently facing many challenges, including a lack of medical staff, resources, and an ageing population which has more complex needs. (NHS England, 2022) Traditional approaches to managing patient health typically require patients to physically visit a clinic to see a doctor who can make a diagnosis and prescribe any medication. Patients may need to meet with their doctor multiple times to monitor their treatment. However, this approach is not ideal for older and disabled patients who may have difficulty getting to the clinic.

Remote patient monitoring offers an alternative that enables healthcare providers to monitor their patients' health from their homes in real time, allowing doctors and ambulances to respond faster, potentially saving lives and reducing healthcare costs.

This report will evaluate an IoT application based on the system proposed by (Rahmani et al., 2018), which could be used remotely to monitor heart patients by collecting data, including ECG from wearable sensing devices. The system reports the data to a remote health centre for immediate analysis and to provide follow-up treatment if necessary.

# 2 Technologies

## 2.1 Sensing Layer

### 2.1.1 Wireless Sensor Network

This application uses wireless sensing devices that are attached to the patient's body to remotely measure vitals, including ECG, temperature, and heart rate. (S. Menaga, R. Vanithamani & P. Hema, 2022)

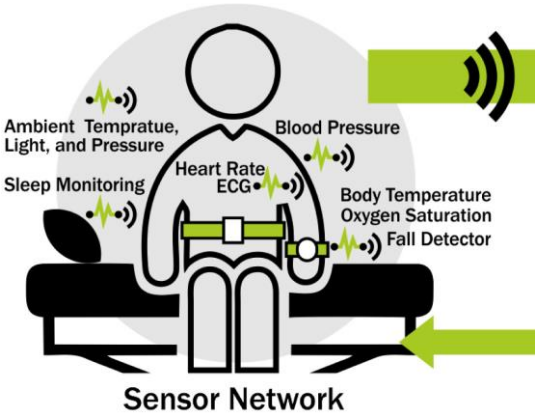


***Fig. 1*** *An example of a Wireless Sensor Network (Rahmani et al., 2018)*

Wireless sensors are less invasive than traditional wired systems such as a Holter monitor, and wireless networks can be scaled to add new sensors as required.

### 2.1.2 ECG sensors

Traditional ECG sensors are not internet-enabled and use wet electrodes that are unsuitable for long-term use. (M. Bansal, B. Gandhi, 2019) However, many wireless sensors that can monitor the heart in real-time have been developed. (S. Majumder et al., 2018)

**Dry ECG Electrodes**

These have some advantages over wet electrodes: they support long-term monitoring and have reduced motion artefacts. (M. Bansal, B. Gandhi, 2019) However, they require contact with the skin, which may be uncomfortable.

**Capacitively-coupled Sensors**

ECG sensors can be embedded into a patient's clothing. For example, one paper developed a contactless ECG sensor that attaches to the patient's shirt. Their sensor

operates on a small battery and transmits data wirelessly to the gateway. (Nemati, Deen & Mondal, 2012) However, the authors note that high impedance can degrade signal quality in capacitively-coupled sensors.

**Smart Watches**

Smart watches such as the Apple Watch can detect heart arrhythmias. (Samol et al., 2019). Watches are easy to use, and patients can view data from their watch. However, continuous ECG monitoring is not supported (Isakadze, Martin, 2020), and the device only measures a single lead ECG, which provides less information about the heart's activity. (Atrial Fibrillation Institute, 2023)

### 2.1.3 Wireless Communication

Sensors must be able to communicate wireless to the gateway and other sensors. One challenge is that sensors are battery-operated and have to last for several weeks, yet protocols such as Wi-Fi and Bluetooth can quickly drain their batteries. (Alf, Keeping, 2010) As a result, low-powered protocols are more suitable.

**ZigBee**

ZigBee is a short-range wireless communication technology that connects low-powered sensor nodes. It has several advantages:

- Low cost
- Suitable range (150m)
- Supports many sensors (653356 devices)
- Supports mesh topology to provide reliability
- Uses a low-power mode when data exchange is not required to reduce power consumption
- Offers in-built encryption

(Dhillon, Sadawarti, 2014)

However, ZigBee has a low data rate (250 kbps), which may not be suitable for transmitting lots of medical sensor data quickly. Additionally, ZigBee nodes can suffer from interference from other wireless transmissions, which degrades the quality of the data. (Hasan et al., 2019)

**Bluetooth Low Energy (BLE)**

BLE is another short-range technology and has several advantages:

- High data rate of 1 Mbps, which can support high-resolution sensor data
- Lower latency than ZigBee (2.5 ms)
- Can operate on a coin-cell battery
- Uses AES encryption
- Smartphones support BLE and could be used as the gateway

(Touati et al., 2015)

However, BLE operates in the crowded 2.4 GHz band, which can cause interference. (Omre, 2010)

## 2.2 Network Layer

Smart e-Health Gateways can be used to aggregate and transmit sensor data to a cloud server for further processing. In this setup, gateways are distributed at fixed geographical locations to provide service for the sensing networks. This allows the patient to freely move around without affecting the data transmission; if a patient moves outside the range of one gateway, another gateway can take over. Data is also processed on gateways in real-time to reduce latency (Rahmani et al., 2018)

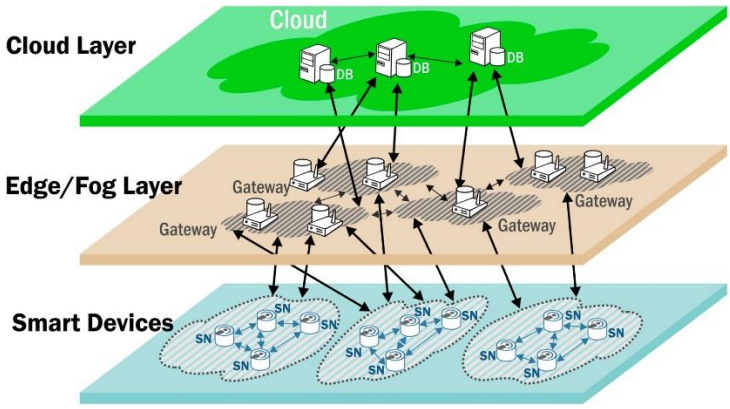


***Fig. 2*** *The three-tier architecture with distributed gateway devices at the Fog layer (Rahmani et al., 2018)*

Alternatively, the patient's phone could be used as the gateway to send data to the cloud. The advantages are that there is no need to build additional infrastructure as phones could use BLE to connect to sensing nodes, and cellular and Wi-Fi technology can connect the phone to the cloud. (Kakria, Tripathi & Kitipawang, 2015)

However, phones have a limited battery, and weak cellular signals could delay data being sent to the cloud, which may affect patient safety.

## 2.3 Application Layer

Cloud servers can provide services such as big data analysis, data storage and web applications to allow healthcare staff to access patient data in real-time. (Rahmani et al., 2018)

They can also connect ecosystems, such as diagnostic facilities, ambulances, and medical research, to provide more effective integrated healthcare. (A. N. Navaz et al., 2021) For example, data generated by the sensors and health records could be analysed in the cloud for medical research.

However, cloud services present many risks, as it involves handling sensitive data on untrusted third-party servers. An alternative approach could be to use peer-to-peer Blockchain to manage transactions securely.

For example, one paper proposes a blockchain-based platform for remotely monitoring patients. Their approach uses a private blockchain that allows entities in the network to fully trust each other. Smart contracts are used to manage the control of assets (including sensors and health records), participants (doctors, nurses, and patients) and transactions (adding/removing sensors, retrieving sensor data) in the system. (Jamil et al., 2020)

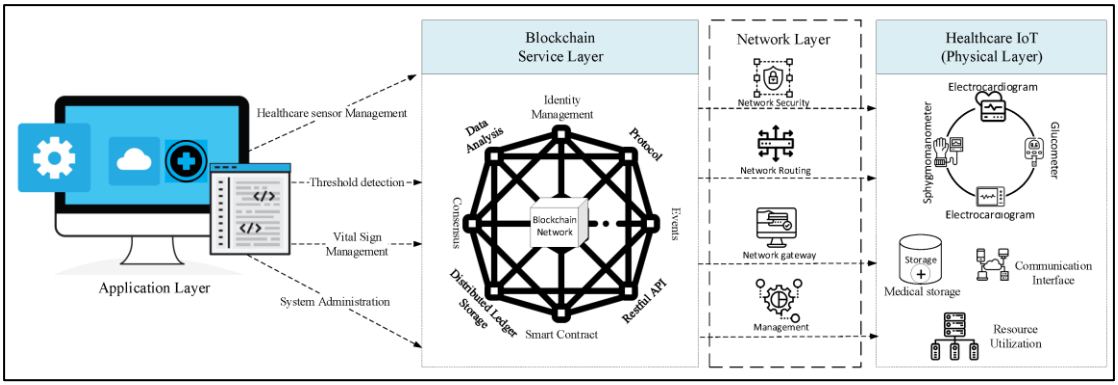


***Fig. 3*** *The blockchain architecture for remote patient monitoring proposed by (Jamil et al., 2020)*

This system could be effective for remotely monitoring heart patients, as the ledger would ensure transparency and protect the integrity of the data by forcing all transactions to be authenticated. However, every time a block is added to the ledger, a

proof-of-work algorithm must be performed, which could delay the system and increase response time for ambulances treating patients suffering from a heart attack. (Griggs et al., 2018)

## 3 Data Analytics

Data analysis is crucial for supporting clinical decision-making from real-time patient data such as ECG, as there would not be enough qualified medical staff to analyse the information of every patient in real-time without it.

In the architecture used by (Rahmani et al., 2018), local data analytics is performed in the Fog layer on smart gateways, which can detect and predict emergencies in real-time and react faster than if analysis was conducted on the cloud as there is reduced latency. Cloud servers are also used to provide big data analysis.

Several data analysis methods could be used in this application:

### Diagnostic Analytics

Diagnostic analysis could be applied to detect if a patient is suffering from heart problems from their ECG.

For example, in one study, a classification model is trained on 2,000 patients using linear regression, which can determine whether the patient has heart disease based on ECG attributes: P, Q, R, S, T. (Rahaman et al., 2022) This simple model could be used in the IoT system to alert doctors and advise patients that they may be suffering from heart disease, which could reduce medical costs and save lives.

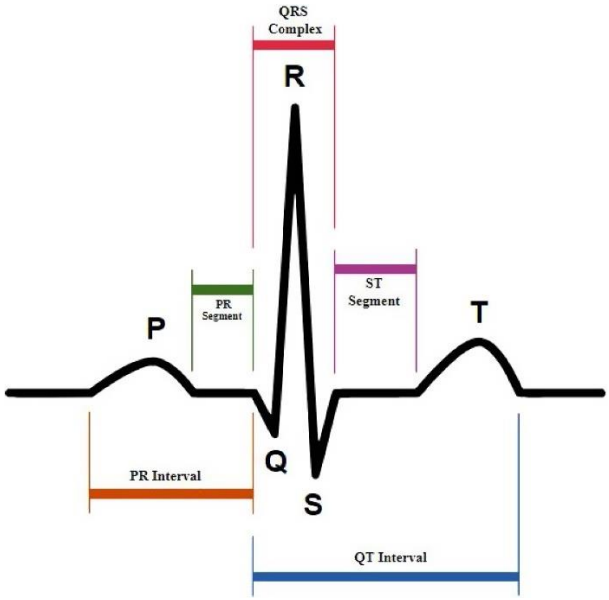


***Fig. 4*** *P, Q, R, S, T on an ECG (Madona, Basti & Zain, 2021)*

Another study proposes a deep-learning model that can classify ECG data on smart watches. (S. Saadatnejad, M. Oveisi & M. Hashemi, 2020) They use a Long Short-Term Memory model, which is trained on each patient to generate a patient-specific baseline. After training, ECG signals from a wearable device are fed into the model to classify heart arrhythmias. They show that their algorithm can accurately classify without significant computational costs. This algorithm could be used in the application to provide faster classification, as the data does not need to be sent to a gateway or cloud server for processing.

**Predictive Analytics**

One study proposes a system that analyses sensor data and Electronic Health Records using fuzzy inference and a gated recurrent unit to predict whether a patient is at risk of a heart attack. (Nancy et al., 2023) Their model analyses data from many sensors, including ECG, blood sugar and blood pressure, and data from the cloud, including patient records. This model could support clinical decision-making and benefit heart patients. For example, this data analysis can be connected to a smart pharmacy that can deliver appropriate medication to patients before they suffer from an attack.

**Big Data Analytics**

Big Data generated by the entire IoT system and connected systems can be analysed to support many other healthcare functions, including monitoring diseases across a population and improving medical research. (Raghupathi, Raghupathi, 2014)

For example, data collected by sensors could be combined with other verticals, such as pharmacies and search engines and analysed to predict if a new epidemic is spreading.

Big Data Analysis could be employed in this IoT application in the cloud servers. It would benefit heart patients as healthcare staff could make more informed decisions to improve their care and streamline the system.

## 4 Security and Privacy Issues

Maintaining security and privacy in any IoT healthcare application is crucial, as healthcare systems are often targeted by attackers who aim to steal, sell, and exploit the vast amounts of data these systems hold. (T. Floyd, M. Grieco & E. F. Reid, 2016)

### 4.1 Jamming Attacks

In the sensing network, nodes use radio signals to transmit data to the gateway device, and an attacker can interfere with these signals by directing a jamming radio signal at the sensors. This type of attack can prevent sensing devices from being able to transmit or receive data, causing a Denial of Service (Sharma, 2022).

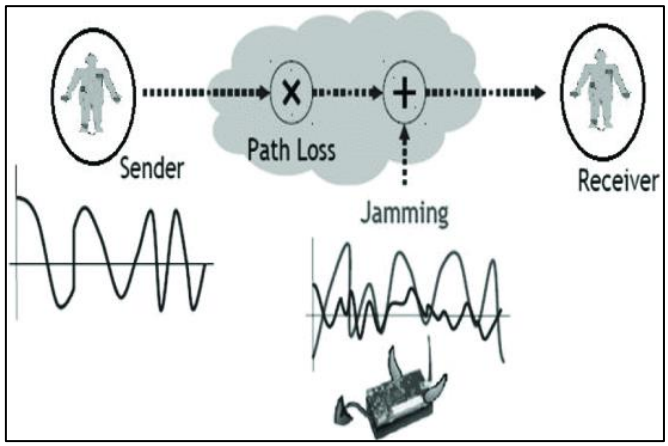


***Fig. 5*** *A typical jamming scenario (R. G. Tiwari et al., 2021)*

Jamming attacks could prevent data from being sent to the gateway, creating incomplete data that could cause the system to miss a patient's deteriorating health.

**Countermeasures for Jamming Attacks**

- *Spread Spectrum* – The data signal is purposely spread over a wider frequency band. For example, ZigBee nodes use Direct-Sequence Spread Spectrum, which can increase the reliability against jamming. However, this method is limited and ineffective against all jamming attacks. (H. Pirayesh, H. Zeng, 2022)

- *Frequency Hopping* - The sensing devices constantly switch between different frequencies to transmit data. For example, Bluetooth Low Energy nodes implement Frequency Hopping Spread Spectrum (E. Mackensen, M. Lai & T. M. Wendt, 2012). This method can mitigate jamming; however, it has been shown that the procedure used to establish the hopping pattern can make devices vulnerable to jamming. (H. Pirayesh, H. Zeng, 2022)

## 4.2 Sinkhole Attacks

Wireless Sensor Networks use multi-hopping, where data is sent to the gateway via other wireless sensors. A protocol ensures that data takes an efficient path to the gateway. (Chavva, Sangam, 2019)

Attackers can exploit this protocol by adding a malicious node that appears to be genuine and advertises that it has the shortest path to the gateway. This causes sensor nodes to send their data to the malicious node, which could allow an attacker to steal or manipulate the patient's data if it is not encrypted. The attacker could also drop the packets at the malicious node, preventing data from being forwarded to the gateway. (Nadeem Al Hassan, Alghamdi, 2018)

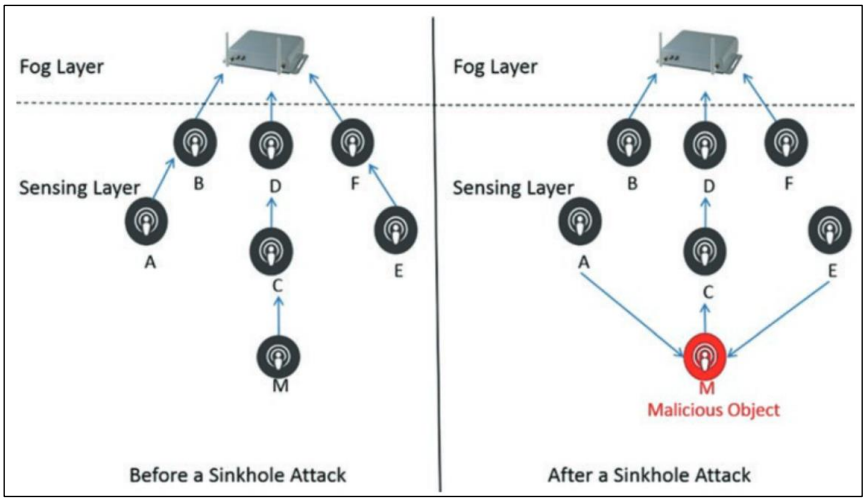


***Fig. 6*** *Before and After a Sinkhole Attack (Rayes, Salam, 2022)*

**Countermeasures for Sinkhole Attacks**

- *Single-hop communication* - Sensors could send data directly to the gateway. However, this could reduce the network's efficiency as certain sensors may be far from the gateway in patient monitoring. (Hasan et al., 2019)
- *Intrusion Detection System* – This could detect malicious nodes and prevent data from being sent to them. For example, one paper proposed an algorithm to detect sinkhole attacks, and their algorithm showed a high success rate. (Nadeem Al Hassan, Alghamdi, 2018)

## 4.3 Virtual Machine (VM) Attacks

Virtualisation is used in cloud and fog data centres to allow many applications to run on the same server. Each application runs on a VM, and a hypervisor is used to manage the virtualisation of resources for each machine.

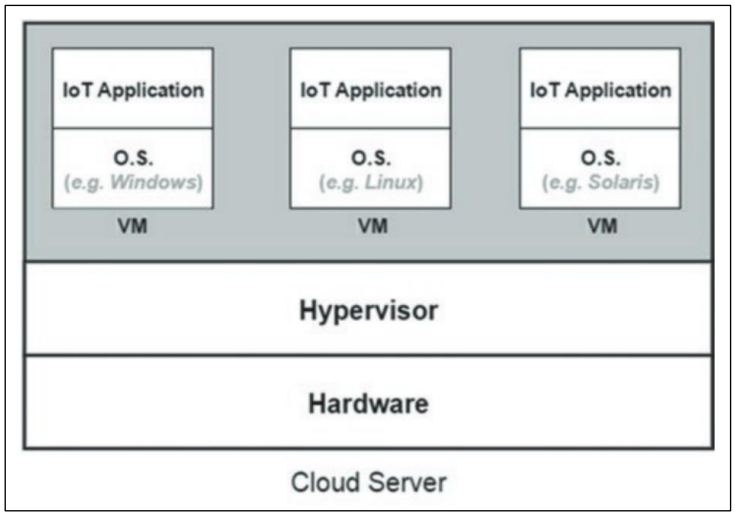


***Fig. 7*** *VM Virtualisation (Rayes, Salam, 2022)*

In a VM Escape attack, attackers exploit vulnerabilities in the hypervisor and can gain root access to the server. (L. Alhenaki et al., 2019) Patient data could be stolen, manipulated, or sold on the dark web during the attack.

Additionally, attackers could install malware, which can devastate the healthcare system. One notable example is WannaCry, a ransomware that encrypted data and files around the world in 2017. It led to NHS England declaring a major incident, as the malware disrupted one-third of hospital trusts in England. (William Smart, 2018)

**Countermeasures for Virtual Machine Attacks**

*Virtual Machine Introspection* – This can be employed in servers to detect abnormal changes in the VMs. While this method can detect and analyse malware on VMs - potentially preventing malware attacks - it can degrade performance and is not effective against all attacks. (Kapil, Mishra, 2021)

*Penetration Testing* - This can be performed on the servers to assess security vulnerabilities, simulate real cyber-attacks, and prevent exploit attacks. However, it can be challenging to perform penetration testing in the cloud and could cause irreversible damage to the system if the test is not isolated. (I. Yurtseven, S. Bagriyanik, 2020)

### 4.4 Insider Attacks

Data in the cloud is stored on servers managed and maintained by people. An insider employee could access or modify medical data and often cause more damage than an external hacker, as they know where sensitive data is stored and may already have access privileges. (Duncan, Creese & Goldsmith, 2015).

An insider attack could lead to a large-scale data breach of sensitive patient records, as medical data is stored centrally in servers. Insiders could manipulate a patient's record, leading to incorrect diagnoses from doctors who trust the data.

**Countermeasures for Insider Attacks**

*Homomorphic Encryption* – This method allows data analysis to be performed on encrypted data. For example, a system has been proposed that homomorphically encrypts the patient's data, which prevents insiders from learning about patient data. (Salim et al., 2021) However, this method can increase the performance requirements of the servers. (Alaya, Laouamer & Msilini, 2020)

*Blockchain* – This technology can maintain data integrity and detect insider activities. One paper has proposed a blockchain-based insider-detection system that uses smart contracts in the Ethereum blockchain to detect and fix abnormal records. (Tukur, Thakker & Awan, 2021).

## 5 Market Implications

### 5.1 Current Barriers and Adoption of Smart Healthcare

Several barriers are negatively impacting the adoption of Smart Healthcare. One of the principal barriers is concerns over data privacy and security both for patients and healthcare providers. (Kelly et al., 2020)

For patients, these concerns may have been exacerbated by data breaches. For example, in one survey, over 93% of the public said they understood the meaning of a

data breach and cited identity theft and loss of personal information as their main concerns. (Karunakaran et al., 2018)

Healthcare providers may be reluctant to migrate from legacy systems to cloud-based systems due to the risks of using third-party companies to store and process sensitive data. (Shen, Guo & Yang, 2019)

Conversely, the COVID pandemic highlighted the need for a flexible system where healthcare can be moved directly to the patient's home. (Umair et al., 2021) Many governments are investing in infrastructure to support Smart Healthcare. For example, the UK has invested £330m in a Federated Data Platform for the NHS which joins separate health data sources together to help clinicians plan and deliver patient care more efficiently. However, this platform is controversial, and there are public concerns about data privacy. (Jessica Morley, Joe Zhang, 2023)

### 5.2 Improving Adoption and Marketing of the IoT System

Privacy and security are major challenges for this application. This could be improved by using stronger security mechanisms such as private Blockchain networks, which can authenticate transactions between IoT devices and users, ensuring patient data is kept private and confidential. The blockchain can also improve data sharing, leading to a more efficient integrated system. (Abu-elezz et al., 2020)

Furthermore, the system could be improved by providing an interactive application for patients, which they could use on their phone or wearable watch. This would provide them with access to analytical insights provided by the system, as well as recommendations from their doctor. This would increase transparency and enhance cooperation between patients and doctors, which are important factors for improving engagement in healthcare. (Bhatt, Chakraborty, 2021)

## Conclusion

This report evaluated an IoT application that remotely monitors heart patients from their homes. Various technologies could be used in the three-layer architecture to implement this solution, and different data analysis methods could be used to improve

the system. This report analysed relevant attacks that could impact security and privacy and evaluated countermeasures that could be taken. Finally, this report discussed barriers that may impact this application's adoption and how these could be overcome. Overall, this application could save lives and improve the efficiency of the entire healthcare system.

## References


A. N. Navaz, M. A. Serhani, H. T. El Kassabi, N. Al-Qirim & H. Ismail 2021, "Trends, Technologies, and Key Challenges in Smart and Connected Healthcare", *IEEE Access*, vol. 9, pp. 74044-74067.

Abu-elezz, I., Hassan, A., Nazeemudeen, A., Househ, M. & Abd-alrazaq, A. 2020, "The benefits and threats of blockchain technology in healthcare: A scoping review", *International journal of medical informatics*, vol. 142, pp. 104246.

Alaya, B., Laouamer, L. & Msilini, N. 2020, "Homomorphic encryption systems statement: Trends and challenges", *Computer Science Review*, vol. 36, pp. 100235.

Alf, H.O. & Keeping, S. 2010, "Bluetooth Low Energy: Wireless Connectivity for Medical Monitoring", *J Diabetes Sci Technol*, vol. 4, no. 2, pp. 457-463.

Atrial Fibrillation Institute 2023, *Atrial Fibrillation: A Guide to Wearable ECG Smart Watches*.

Bhatt, V. & Chakraborty, S. 2021, "Improving service engagement in healthcare through internet of things based healthcare systems", *Journal of Science and Technology Policy Management*, vol. 14, no. 1, pp. 53–73.

Chavva, S.R. & Sangam, R.S. 2019, "An energy-efficient multi-hop routing protocol for health monitoring in wireless body area networks", *Network Modeling Analysis in Health Informatics and Bioinformatics*, vol. 8, no. 1, pp. 21.

Dhillon, P. & Sadawarti, H. 2014, "A Review Paper on Zigbee (IEEE 802.15.4) Standard", *International journal of engineering research and technology*, vol. 3.

Duncan, A., Creese, S. & Goldsmith, M. 2015, "An overview of insider attacks in cloud computing", *Concurrency and Computation: Practice and Experience*, vol. 27, no. 12, pp. 2964-2981.

E. Mackensen, M. Lai & T. M. Wendt 2012, "Bluetooth Low Energy (BLE) based wireless sensors", *SENSORS, 2012 IEEE*, pp. 1.

Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A. & Hayajneh, T. 2018, "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring", *Journal of medical systems*, vol. 42, no. 7, pp. 130.

H. Pirayesh & H. Zeng 2022, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey", *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767-809.

Hasan, K., Biswas, K., Ahmed, K., Nafi, N.S. & Islam, M.S. 2019, "A comprehensive review of wireless body area network", *Journal of Network and Computer Applications*, vol. 143, pp. 178-198.

I. Yurtseven & S. Bagriyanik 2020, "A Review of Penetration Testing and Vulnerability Assessment in Cloud Environment", *2020 Turkish National Software Engineering Symposium (UYMS)*, pp. 1.

Isakadze, N. & Martin, S.S. 2020, "How useful is the smartwatch ECG?", *Trends in cardiovascular medicine*, vol. 30, no. 7, pp. 442-448.

Jamil, F., Ahmad, S., Iqbal, N. & Kim, D. 2020, "Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals", *Sensors*, vol. 20, no. 8.

Jessica Morley & Joe Zhang 2023, "A controversial new federated data platform for the NHS in England", *BMJ*, vol. 383, pp. p2776.

Kakria, P., Tripathi, N.K. & Kitipawang, P. 2015, "A Real-Time Health Monitoring System for Remote Cardiac Patients Using Smartphone and Wearable Sensors", *International Journal of Telemedicine and Applications*, vol. 2015, pp. 373474.

Kapil, D. & Mishra, P. 2021, "Virtual Machine Introspection in Virtualization: A Security Perspective", *Proceedings of the 2021 Thirteenth International Conference on Contemporary Computing*Association for Computing Machinery, New York, NY, USA.

Karunakaran, S., Thomas, K., Bursztein, E. & Comanescu, O. 2018, "Data Breaches: User Comprehension, Expectations, and Concerns with Handling Exposed Data", *SOUPS @ USENIX Security Symposium*.

Kelly, J.T., Campbell, K.L., Gong, E. & Scuffham, P. 2020, "The Internet of Things: Impact and Implications for Health Care Delivery", *J Med Internet Res*, vol. 22, no. 11, pp. e20135.

L. Alhenaki, A. Alwatban, B. Alamri & N. Alarifi 2019, "A Survey on the Security of Cloud Computing", *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, pp. 1.

M. Bansal & B. Gandhi 2019, "IoT & Big Data in Smart Healthcare (ECG Monitoring)", *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, pp. 390.

Madona, P., Basti, R.I. & Zain, M.M. 2021, "PQRST wave detection on ECG signals", *Gaceta Sanitaria*, vol. 35, pp. S364-S369.

Nadeem Al Hassan, A. & Alghamdi, T. 2018, "Detection Algorithm for Sinkhole Attack in Body Area Sensor Networks using local information", *International Journal of Network Security*, vol. 20.

Nancy, A.A., Ravindran, D., Vincent, D.R., Srinivasan, K. & Chang, C. 2023, "Fog-Based Smart Cardiovascular Disease Prediction System Powered by Modified Gated Recurrent Unit", *Diagnostics (Basel, Switzerland)*, vol. 13, no. 12, pp. 2071. doi: 10.3390/diagnostics13122071.

Nemati, E., Deen, M.J. & Mondal, T. 2012, "A Wireless Wearable ECG Sensor for Long-Term Applications", *IEEE Communications Magazine*, vol. 50, pp. 36-43.

NHS England 2022, , *NHS England » Evolving to meet a changing world*. Available: https://www.england.nhs.uk/future-of-human-resources-and-organisational-development/the-future-of-nhs-human-resources-and-organisational-development-report/evolving-to-meet-a-changing-world/.

R. G. Tiwari, A. Misra, A. K. Agarwal & V. Khullar 2021, "Communication Jamming in Body Sensor Network: A Review", *2021 10th International Conference on System Modeling & Advancement in Research Trends (SMART)*, pp. 135.

Raghupathi, W. & Raghupathi, V. 2014, "Big data analytics in healthcare: promise and potential", *Health Information Science and Systems*, vol. 2, no. 1, pp. 3.

Rahaman, M., Shamrat, F.M., Kashem, M., Akter, M., Chakraborty, S., Ahmed, M. & Mustary, S. 2022, "Internet of things based electrocardiogram monitoring system using machine learning algorithm", *International Journal of Electrical and Computer Engineering*, vol. 12, pp. 3739-3751.

Rahmani, A.M., Gia, T.N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M. & Liljeberg, P. 2018, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach", *Future Generation Computer Systems*, vol. 78, pp. 641-658.

Rayes, A. & Salam, S. 2022, *Internet of Things From Hype to Reality : The Road to Digitization*, Springer, S.l.].

S. Majumder, L. Chen, O. Marinov, C. -H. Chen, T. Mondal & M. J. Deen 2018, "Noncontact Wearable Wireless ECG Systems for Long-Term Monitoring", *IEEE Reviews in Biomedical Engineering*, vol. 11, pp. 306-321.

S. Menaga, R. Vanithamani & P. Hema 2022, "A Comprehensive Review on Wireless Body Area Network - Technologies, Challenges, Application and Energy Saving Techniques", *2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC)*, pp. 541.

S. Saadatnejad, M. Oveisi & M. Hashemi 2020, "LSTM-Based ECG Classification for Continuous Monitoring on Personal Wearable Devices", *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 2, pp. 515-523.

Salim, M.M., Kim, I., Doniyor, U., Lee, C. & Park, J.H. 2021, "Homomorphic Encryption Based Privacy-Preservation for IoMT", *Applied Sciences*, vol. 11, no. 18.

Samol, A., Bischof, K., Luani, B., Pascut, D., Wiemer, M. & Kaese, S. 2019, "Single-Lead ECG Recordings Including Einthoven and Wilson Leads by a Smartwatch: A New Era of Patient Directed Early ECG Differential Diagnosis of Cardiac Diseases?", *Sensors*, vol. 19, no. 20.

Sharma, K. 2022, "Internet of healthcare things security vulnerabilities and jamming attack analysis", *Expert Systems*, vol. 39, no. 3, pp. e12853.

Shen, B., Guo, J. & Yang, Y. 2019, "MedChain: Efficient Healthcare Data Sharing via Blockchain", *Applied Sciences*, vol. 9, no. 6.

T. Floyd, M. Grieco & E. F. Reid 2016, "Mining hospital data breach records: Cyber threats to U.S. hospitals", *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, pp. 43.

Touati, F., Ochirkhand Erdene-Ochir, Mehmood, W., Hassan, A., Adel, B.M., Gaabab, B., Mohd Fadlee A. Rasid & Khriji, L. 2015, "An Experimental Performance Evaluation and Compatibility Study of the Bluetooth Low Energy Based Platform for ECG Monitoring in WBANs", *International Journal of Distributed Sensor Networks*, vol. 11, no. 9, pp. 645781.

Tukur, Y.M., Thakker, D. & Awan, I. 2021, "Edge-based blockchain enabled anomaly detection for insider attack prevention in Internet of Things", *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, pp. e4158.

Umair, M., Cheema, M.A., Cheema, O., Li, H. & Lu, H. 2021, "Impact of COVID-19 on IoT Adoption in Healthcare, Smart Homes, Smart Buildings, Smart Cities, Transportation and Industrial IoT", *Sensors*, vol. 21, no. 11.

William Smart 2018, *Lessons learned review of the WannaCry Ransomware Cyber Attack*, NHS England.