System Architectures

Assignment 3

OLLSCOIL TEICNEOLAÍOCHTA BHAILE ÁTHA CLIATH
DUBLIN
TECHNOLOGICAL UNIVERSITY DUBLIN

Saul Burgess

C19349793

07/05/2024

Contents

Contents **I**

1 Wereables and Health Monitoring **1**

1.1 AI and ML in Wearables 1

1.2 Event Detection 2

1.3 Predictive Analytics 2

1.4 Diagnostic Accuracy 2

1.5 Challenges in Implementation 2

1.5.1 Data Security and Privacy 2

1.5.2 Sensor Accuracy and Algorithm Reliability 3

1.5.3 Regulatory Compliance 3

2 System Architecture **4**

2.1 Smartphones as Edge Computing Nodes 5

2.2 Processing Server and Database 5

2.3 Load Balancer for Data Ingress 5

2.4 Document Management System Integration 6

2.5 Security and Compliance Measures 6

2.6 Scalability and Maintenance 6

3 System Performance **7**

3.1 System Performance 7

3.2 System Reliability 8

3.3 Scalability of Data Storage Requirements 8

4 Cloud Services **9**

4.1 Negative Examples 9

4.1.1 Data Breaches and Unauthorized Access 9

4.1.2 Compliance and Data Sovereignty Issues 9

4.2 Positive Example 10

4.2.1 Scalability and Accessibility 10

4.3 Conclusion 10

5 Internet of Things **11**

5.1 Internet of Things and Wearable Technologies in Health Monitoring . . . 11

5.1.1 Enhanced Data Collection and Integration 11

5.1.2 Proactive Health Management 12

5.1.3 Personalized Healthcare Experiences 12

5.1.4 Challenges and Considerations 12

Bibliography **13**

Chapter 1

Wereables and Health Monitoring

The proliferation of wearable technology has introduced a new approach to health monitoring. Devices such as smartwatches and fitness bands, equipped with multiple sensors, gather continuous information on physiological metrics. These devices facilitate a high degree of real-time health monitoring and have important implications for preventative healthcare. [1]

1.1 AI and ML in Wearables

AI and ML technologies enhance the functionality of wearable devices through advanced data analysis techniques. These technologies are essential in deciphering complex patterns from the continuous stream of information generated by the sensors of wearable devices. The main utility of integrating AI with wearables lies in its capacity to distinguish emergent health issues from physiological data indicators, thereby facilitating timely medical interventions. [2]

1.2 Event Detection

ML algorithms are applied to find specific patterns that suggest possible health threats such as falls or significant changes in vitals like heart rate and blood pressure. These algorithms are trained on extensive datasets to enhance their predictive accuracy and reliability. [3]

1.3 Predictive Analytics

AI algorithms are instrumental in predicting possible health deterioration before they become critical, enabling preemptive medical advice and interventions. This capability is facilitated by the analysis of historical information gathered by the wearable devices, allowing for a personalized and proactive approach to health management. [3]

1.4 Diagnostic Accuracy

Continuous improvements in AI and ML models assist in refining the algorithms over time, thereby enhancing their diagnostic precision. This iterative learning procedure is critical in reducing the occurrence of false positives and negatives, which are important for the reliability of health monitoring wearables. [4]

1.5 Challenges in Implementation

Despite their potential, several challenges hinder the widespread acceptance of AI-enhanced wearable health technologies:

1.5.1 Data Security and Privacy

The sensitive nature of health information necessitates stringent cybersecurity measures to guard against unauthorized access and breaches. [5]

1.5.2 Sensor Accuracy and Algorithm Reliability

The effectiveness of wearable health monitors heavily relies on the accuracy of their sensors and the reliability of the algorithms. Ensuring these can mitigate the risk associated with misdiagnoses or overlooking dangerous health conditions. [1]

1.5.3 Regulatory Compliance

Wearable technologies that cover health information must comply with the General Data Protection Regulation (GDPR) in the European Union. GDPR impose strict requirements on the processing of personal data and ensures that information handling practices are transparent and secure. Compliance with GDPR is vital to safeguard the privacy of individuals and preserve the integrity of health information gathered by wearable devices. This includes obtaining explicit consent from users before information collection, ensuring information minimization, and providing users with access to their data. Adherence to these regulations is necessary not just for legal compliance but also to guarantee the safety and efficacy of the device in health monitoring. [6]

Chapter 2

System Architecture

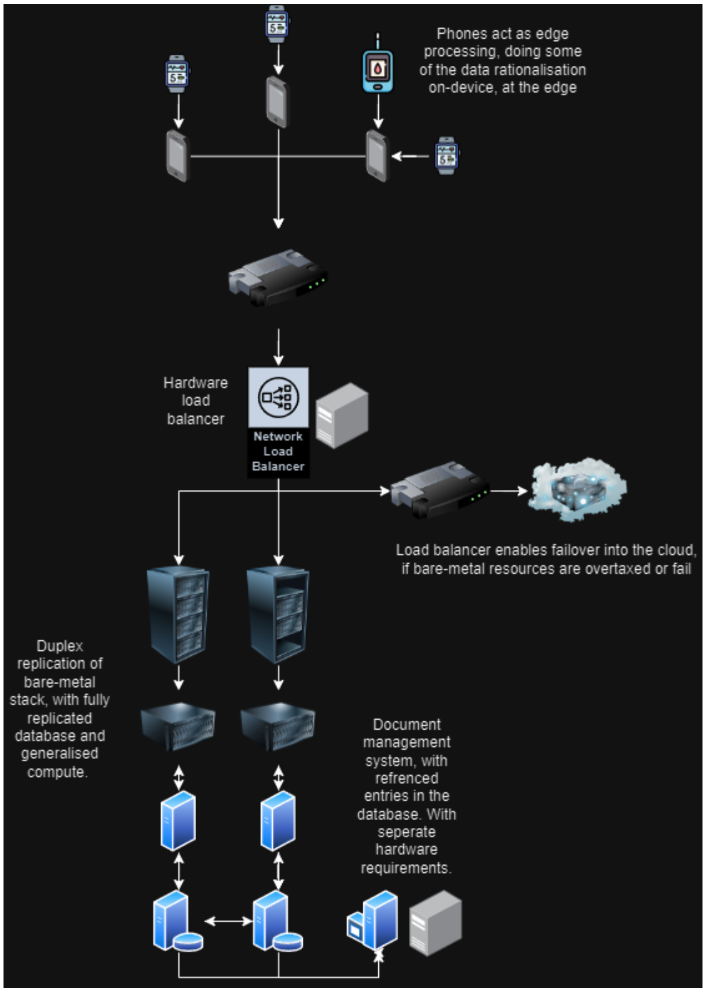
Phones act as edge processing, doing some of the data rationalisation on-device, at the edge
Hardware load balancer
Network Load Balancer
Load balancer enables failover into the cloud, if bare-metal resources are overtaxed or fail
Duplex replication of bare-metal stack, with fully replicated database and generalised compute.
Document management system, with refrenced entries in the database. With seperate hardware requirements.

Figure 2.1: System Diagram

2.1 Smartphones as Edge Computing Nodes

Smartphones are utilized as edge compute nodes due to their advanced processing capability and sensors.They preprocess information gathered from wearables by performing information filtering, initial analysis, and significance assessment. This not only enhances the quality of information sent to the central server but also reduces the bandwidth needed for information transmission. [7]

2.2 Processing Server and Database

The central processing server performs detailed data analysis and complex processing tasks. It is distinct yet closely integrated with the database to facilitate seamless information flow between processing and storage components. The server handles tasks such as:

- Further analysis of preprocessed information from smartphones
- Application of machine learning algorithms
- Generation of actionable insights and reports

The database is seperatly hosted. This separation ensures dedicated resources are available for process and storage functions, this seperation allows for more specialised hardware to be used for the database, which can be optimised for read and write operations. [8]

2.3 Load Balancer for Data Ingress

A load balancer is employed to handle data incoming from multiple smartphone edge nodes efficiently. This setup ensures that incoming information is spread equally across available server resources, preventing server overload.

2.4 Document Management System Integration

The Document Management System is integrated with the database to facilitate structured storage, retrieval, and management of documents. This integration allows the system to manage large volumes of documents efficiently, providing fast data retrieval and compliance with document retention policies and regulations.

2.5 Security and Compliance Measures

Comprehensive security measures are integral to the architecture, including:

- End-to-end encryption of information in transit and at rest
- Secure authentication mechanisms
- Rigorous access control

Compliance with data security laws such as GDPR is meticulously maintained to ensure the system respects and protects user privacy throughout all operations.

2.6 Scalability and Maintenance

The architecture is designed to be scalable to accommodate an increased amount of users and high data volumes. Regular updates and maintenance are planned to enhance system functionality, address security vulnerabilities, and assure sustained performance and reliability.

Chapter 3

System Performance

3.1 System Performance

The proposed architecture leverages smartphones as edge compute nodes, which significantly enhance system performance through these key aspects:

- **Reduced Latency:** By processing information locally on smartphones, the system minimizes the need to send large volumes of sensitive information to the central server. This local preprocessing speed up response time as only relevant information is forwarded for further processing. [7]
- **Load Distribution:** Incorporating a load balancer ensures efficient distribution of information across multiple servers instances, preventing any one server from becoming a bottleneck and enhancing overall response time and information handling capabilities.
- **Optimized Data Handling:** Separating the process and storage functionalities allow each to be optimized for their particular tasks, allowing for fast processing for real-time analytics and efficient storage for information persistence—improving both speed and efficiency. [8]

3.2 System Reliability

Several mechanisms are employed within the architecture to guarantee high reliability:

- **Fault Tolerance:** The use of a load balancer improves system reliability by rerouting traffic away from servers that are failing or are overburdened, maintaining continuous service and allowing for maintenance without downtime.
- **Data Redundancy:** Configuring the database system for redundancy protects against data loss in the case of hardware failure and allows for recovery without data corruption.
- **Robust Security Measures:** Implementing security features such as end-to-end encryption, strong authentication, and rigorous access control prevents unauthorized access and data breaches, enhancing system reliability. [9]

3.3 Scalability of Data Storage Requirements

The scalability of the architecture is addressed through various features:

- **Modular Design:** The architecture's modular design allows for the addition of more smartphones as edge client and server instances as needed. This horizontal scalability supports an increased amount of users and high information processing demands.
- **Cloud Integration Possibility:** Although the current setup is non-cloud, the architecture is designed for easy integration with cloud services if needed, providing almost unlimited scalability by leveraging cloud resources for additional processing and storage capacity.
- **Efficient Data Management:** Integrating a Document Management A system with a database ensures effective organization and management of data, supporting scalability with features like indexing and fast recovery capabilities as data volume grows.

Chapter 4

Cloud Services

4.1 Negative Examples

4.1.1 Data Breaches and Unauthorized Access

Cloud systems are open to a broader attack surface due to their internet accessibility. For an AT passport system handling sensitive health data, this exposure increases the chance of data breaches. For example, Amazon Web Services has experienced several significant breaches affecting many personal records. [10] In the context of health monitoring, such a breach could reveal extremely sensitive health information, and lead to serious privacy violations and possible abuse of personal health data.

4.1.2 Compliance and Data Sovereignty Issues

Cloud services frequently require data centres located in multiple jurisdictions, which can complicate compliance with stringent health data protection regulations such as HIPAA or GDPR. [6] If information from a European citizen is stored outside the EU, it may not be protected under GDPR, leading to possible legal and compliance risks. This scenario can result in fines and sanctions against healthcare providers or entities managing the AT passport system, alongside the danger of losing public trust. [6]

4.2 Positive Example

4.2.1 Scalability and Accessibility

Despite security concerns, cloud services provide unmatched scalability and accessibility, which is vital for the efficient deployment of an AT passport system. Cloud platforms can dynamically allocate resources to manage increasing data and user access requests without significant upfront investment in physical infrastructure. For example, during the COVID-19 pandemic, healthcare providers rapidly scaled up their telehealth service using cloud solutions to match the sudden surge in demand for remote healthcare, ensure that patient continue to have necessary health monitoring. [11]

4.3 Conclusion

While the benefits of cloud services, especially their scalability and accessibility, are undeniable, the threat to privacy and security, particularly concerning sensitive health data, is important and often outweigh the benefits. Data breaches and compliance issues not only present danger to individual privacy but also threaten the legal and operational standing of entities managing health data. Decisions to apply cloud services in the setting of health monitoring systems must be accompanied by robust security measures, rigorous compliance checks, and transparent information handling practices to mitigate these risks effectively.

Chapter 5

Internet of Things

5.1 Internet of Things and Wearable Technologies in Health Monitoring

The Internet of Things refers to the network of physical objects embedded with sensors and other technologies to connect and exchanging information with other devices and systems over the internet. These objects, or "things," can range from ordinary household items to advanced industrial tools. In the context of health monitoring, IoT technology enhances the functionality and effectiveness of wearable devices.

5.1.1 Enhanced Data Collection and Integration

IoT-enabled wearables can collect a broad array of health information in real-time, from heart rate and blood pressure to more complex metrics like blood oxygen level and electrocardiogram readings. These devices incorporated within the AT passport system, can transfer collected information to smartphones or directly to centralized servers for processing. For example, continuous glucose monitor devices that use IoT connectivity can transmit real-time glucose levels to a patient’s smartphone, which processes the information to offer insights and send alerts if intervention is needed.

5.1.2 Proactive Health Management

The integration of IoT in wearables facilitates not just the monitoring but also the proactive management of health conditions.[1] By continuously analyzing the information collected, the organization can identify possible health issues before they get critical. For instance, IoT-enabled wearables can detect irregular heartbeat indicative of atrial fibrillation and automatically alert healthcare providers, enabling early treatment and potentially preventing severe health events.[1]

5.1.3 Personalized Healthcare Experiences

IoT technology contributes to personalized medicine by allowing wearables to conform to the individual's particular health needs. Based on the analysis of accumulated data, wearables can indicate lifestyle changes, medication adjustments, or recommend consultations with healthcare providers. This level of personalization ensures that each user receives care that is tailored to their unique health profile, making health interventions more effective.[2]

5.1.4 Challenges and Considerations

Despite the numerous benefits, the integration of IoT in health monitoring systems raises important privacy and security concerns. The transmission of sensitive health information over a network exposes users to possible data breaches and unauthorized access. For example, if protection measures are not adequately enforced, personal health data could be intercepted during transmission from wearables to servers. Moreover, ensuring the accuracy and reliability of IoT devices remains crucial, as faulty data could lead to improper health interventions. Regulatory compliance, particularly concerning data security standards like GDPR, must be strictly adhered to, to protect user privacy and maintain confidence in the technology. While IoT technology enhances the capabilities of wearable technology in health monitoring, careful consideration must be given to privacy and security to fully realize its benefits in systems like the AT passport.

Bibliography

[1] S. Huhn, M. Axt, H.-C. Gunga, M. A. Maggioni, S. Munga, D. Obor, A. Sié, V. Boudo, A. Bunker, R. Sauerborn, *et al.*, "The impact of wearable technologies in health research: scoping review," *JMIR mHealth and uHealth*, vol. 10, no. 1, p. e34384, 2022.

[2] C. Y. Jin, "A review of ai technologies for wearable devices," in *IOP Conference Series: Materials Science and Engineering*, vol. 688, p. 044072, IOP Publishing, 2019.

[3] G. P. Buddha and R. Pulimamidi, "The future of healthcare: Artificial intelligence's role in smart hospitals and wearable health devices," *Tuijin Jishu/Journal of Propulsion Technology*, vol. 44, no. 5, pp. 2498–2504, 2023.

[4] S. B. Junaid, A. A. Imam, M. Abdulkarim, Y. A. Surakat, A. O. Balogun, G. Kumar, A. N. Shuaibu, A. Garba, Y. Sahalu, A. Mohammed, *et al.*, "Recent advances in artificial intelligence and wearable sensors in healthcare delivery," *Applied Sciences*, vol. 12, no. 20, p. 10271, 2022.

[5] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technology and Health Care*, vol. 25, no. 1, pp. 1–10, 2017.

[6] "Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (gen-

eral data protection regulation).” https://eur-lex.europa.eu/eli/reg/2016/679/oj, 2016. Accessed: [02/05/2024].

[7] Z. Ning, P. Dong, X. Wang, X. Hu, L. Guo, B. Hu, Y. Guo, T. Qiu, and R. Y. Kwok, “Mobile edge computing enabled 5g health monitoring for internet of medical things: A decentralized game theoretic approach,” *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 463–478, 2020.

[8] K. Liu, H. Tong, Z. Sun, Z. Ren, G. Huang, H. Zhu, L. Liu, Q. Lin, and C. Zhang, “Integrating fpga-based hardware acceleration with relational databases,” *Parallel Computing*, p. 103064, 2024.

[9] J. Pool, S. Akhlaghpour, F. Fatehi, and A. Burton-Jones, “A systematic analysis of failures in protecting personal health data: a scoping review,” *International Journal of Information Management*, vol. 74, p. 102719, 2024.

[10] M. Heiligenstein, “Microsoft data breaches: Full timeline through 2023,” *Firewall Times*, 2022.

[11] S. M. Wood, K. White, R. Peebles, J. Pickel, M. Alausa, J. Mehringer, and N. Dowshen, “Outcomes of a rapid adolescent telehealth scale-up during the covid-19 pandemic,” *Journal of Adolescent Health*, vol. 67, no. 2, pp. 172–178, 2020.